

---

# Encyclopedia of Cryptography, Security and Privacy

---

Sushil Jajodia • Pierangela Samarati •  
Moti Yung  
Editors

# Encyclopedia of Cryptography, Security and Privacy

Third Edition

With 459 Figures and 100 Tables

 Springer

*Editors*

Sushil Jajodia  
Center for Secure Information Systems  
George Mason University  
Fairfax, VA, USA

Pierangela Samarati  
Università degli Studi di Milano  
Milan, Italy

Moti Yung  
Google LLC and Columbia University  
New York, NY, USA

ISBN 978-3-030-71520-5      ISBN 978-3-030-71522-9 (eBook)  
<https://doi.org/10.1007/978-3-030-71522-9>

© Springer Nature Switzerland AG 2005, 2011, 2025

This work is subject to copyright. All rights are solely and exclusively licensed 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

If disposing of this product, please recycle the paper.

---

## Preface

A rich stream of papers and many good books have been written on cryptography, security, and privacy, but most of them assume a scholarly reader who has the time to start at the beginning and work their way through the entire text. The goal of the *Encyclopedia of Cryptography, Security, and Privacy, Third Edition* is to make important notions of cryptography, security, and privacy accessible to readers who have an interest in particular concepts related to these areas, but lack the time to study one of the many books in these areas or prefer a guided introduction to a particular subject.

The third edition is intended as a replacement of *Encyclopedia of Cryptography and Security, Second Edition* that was edited by Henk van Tilborg and Sushil Jajodia and published by Springer in 2011. The goal of the third edition is to enhance the earlier edition in several important and interesting ways. First, as noticeable already from the title of the encyclopedia, coverage has been expanded with special emphasis to the area of privacy. Second, entries of the second edition have been updated when needed to keep pace with the advancement of the state of the art. Third, considering the fast pace at which information and communication technology is evolving and has evolved drastically since the second edition, new entries have been introduced to provide an extensive view and include coverage of several newer topics. This third edition provides a comprehensive reference to 1067 topics in the broad field of cryptography, security, and privacy; compared to the second edition where the reader can find 750 new (either revised or newly added) entries.

This *Encyclopedia* is available not only as a printed volume but as an online reference work as well. The print publication includes an index of subjects and of authors. This *Encyclopedia* has a home page at Encyclopedia of Cryptography, Security and Privacy |SpringerLink where it is available online. The online edition is an XML e-Reference searchable version that allows cross-references. Moreover, the online edition will also allow us to make regular updates as new trends and terms arise.

Fairfax, USA  
Milan, Italy  
New York, USA  
November 2024

Sushil Jajodia  
Pierangela Samarati  
Moti Yung  
Editors

---

## Acknowledgments

We would like to acknowledge several individuals who made this *Encyclopedia* possible. First and foremost, we would like to extend our sincerest thanks to the members of the editorial board and all the authors for their hard work. We are grateful to Daniel Diwakar of Springer Nature India who assisted us with every aspect of preparing this *Encyclopedia*, from collection of entries to dealing with editors and authors and various format-related issues in preparation of the printed volume. Last, but certainly not the least, thanks are due to our publisher, Susan Lagerstrom-Fife of Springer Nature, for her enthusiasm and support for this project. Thank you very much, all of you!

---

## About the Editors



**Sushil Jajodia** is currently Distinguished University Professor, BDM International Professor, and the Director of the Center for Secure Information Systems, George Mason University, Fairfax, Virginia. Prior to joining George Mason, he held permanent positions at the National Science Foundation, Naval Research Laboratory, and the University of Missouri-Columbia. He has also been a Visiting Professor at the University of Milan, Sapienza University of Rome, Cambridge University, King's College, Paris Dauphine University, and Imperial College. Dr. Jajodia received his BS and MS from the Southern Illinois University, Carbondale, and PhD from the University of Oregon, Eugene, all in Mathematics.

Dr. Jajodia has sustained a highly active research agenda spanning database and distributed systems, and cyber security for over 30 years. He has authored or coauthored 7 books, edited 52 books and conference proceedings, and published more than 500 technical articles in refereed journals and conference proceedings. He is also a holder of 29 patents, 18 of which have been licensed by successful startups. Dr. Jajodia has supervised 27 doctoral dissertations; 13 of these graduates hold academic positions while rest are in successful industrial positions.

Dr. Jajodia has served in different capacities for various journals and conferences. He was the founding editor-in-chief of the *Journal of Computer Security* and has served as the editor of several journals including *IEEE Transactions on Computers*, *ACM Transactions on Privacy and Security*, and *IEEE Transactions on Knowledge and Data Engineering*.

Dr. Jajodia is a fellow of Association for Computing Machinery (ACM), Institute of Electrical and Electronics Engineers (IEEE), and International Federation for Information Processing (IFIP), and recipient of numerous awards including the IEEE Computer Society W. Wallace McDowell Award. According to Google Scholar, he has over 55,000 citations, and his h-index is 116 (See: <https://csis.gmu.edu/jajodia>).



**Pierangela Samarati** is a Professor at the Department of Computer Science of the Università degli Studi di Milano, Italy. Her main research interests are on data and applications security and privacy, especially in emerging scenarios. She has participated in several EU-funded projects involving different aspects of information protection, also serving as project coordinator. She has published more than 300 peer-reviewed articles in international journals, conference proceedings, and book chapters. She has been Computer Scientist in the Computer Science Laboratory at SRI, CA (USA). She has been a visiting researcher at the Computer Science Department of Stanford University, CA (USA), and at the Center for Secure Information Systems of George Mason University, VA (USA). She is the chair of the IEEE Systems Council Technical Committee on Security and Privacy in Complex Information Systems (TCSPCIS), of the ERCIM Security and Trust Management Working Group (STM), and of the ACM Workshop on Privacy in the Electronic Society (WPES). She is a member of several steering committees. She has served as Program Chair and General Chair of several international conferences and in the editorial board of several journals. She is an IEEE Fellow (2012), ACM Fellow (2021), and IFIP Fellow (2021). She has received the ESORICS Outstanding Research Award (2018), the IEEE Computer Society Technical Achievement Award (2016), and the IFIP WG 11.3 Outstanding Research Award (2012) (See: <https://samarati.di.unimi.it>).



**Moti Yung** is a Distinguished Security and Privacy Research Scientist with Google. He received his PhD from Columbia University in 1988. Previously, he was with IBM Research, Certco (Bankers Trust), RSA Laboratories (EMC), and Snap. He has also been an adjunct senior research faculty at Columbia University (for over 30 years), where he has co-advised and worked with PhD students.

Yung is a fellow of the IEEE, the Association for Computing Machinery (ACM), the International Association for Cryptologic Research (IACR), and the European Association for Theoretical Computer Science (EATCS). In 2010 he gave the IACR Distinguished Lecture. He is the recipient of the 2014 ACM's Special Interest Group on Security, Audit and Control (SIGSAC) Outstanding Innovation award, the 2014 ESORICS (European Symposium on Research in Computer Security) Outstanding Research award, an IBM Outstanding Innovation award, a Google OC award, and a Google founders' award. In 2018 he received the IEEE-CS W. Wallace McDowell Award and in 2020 he received the IEEE-CS Computer Pioneer Award. In 2020 he received the test-of-time award for a paper predicting ransomware co-authored in 1996 in IEEE's Symposium on Security and Privacy; also in 2020 he received the IACR's Public Key Cryptography (PKC) conference test-of-time award for a paper he co-authored in 1998; in 2024 he received the Eurocrypt test-of-time award for a paper he co-authored in 2009. Yung is a member of the American Academy of Arts and Sciences.

Yung's contributions to research and development treat science and technology holistically: from the theoretical mathematical foundations, via conceptual mechanisms, to applied cryptography, and to participation in developing actual industrial products. His work has been predicting future needs of secure systems, and analyzing coming threats. These led to basic innovative theoretical notions, central applied concepts, and concrete industrial systems (See: <https://dblp.org/pid/y/MotiYung.html> [https://en.wikipedia.org/wiki/Moti\\_Yung](https://en.wikipedia.org/wiki/Moti_Yung)).

---

## Section Editors



**Carlisle Adams**

School of Electrical Engineering and  
Computer Science  
University of Ottawa  
Ottawa, ON, Canada



**Charu C. Aggarwal**

IBM T. J. Watson Research  
Center  
Yorktown Heights, NY, USA



**Massimiliano Albanese**

Center for Secure Information  
Systems  
George Mason University  
Fairfax, VA, USA



**Carlo Blundo**  
Dipartimento di Scienze  
Aziendali – Management and Innovation  
Systems  
Università degli Studi di Salerno  
Fisciano (SA), Italy



**Dan Boneh**  
Stanford University  
Stanford, CA, USA



**Reza Curtmola**  
Computer Science  
New Jersey Institute of Technology  
Newark, NJ, USA



**Ernesto Damiani**  
Computer Science Department  
Università degli Studi di Milano  
Milano, Italy



**Sabrina De Capitani di Vimercati**  
Computer Science Department  
Università degli Studi di Milano  
Milano, Italy



**Robert Deng**  
School of Computing and Information  
Systems  
Singapore Management University  
Singapore, Singapore



**Yvo Desmedt**  
Computer Science  
The University of Texas at Dallas  
Richardson, TX, USA



**Roberto Di Pietro**  
CEMSE  
King Abdullah University of  
Science and Technology  
Jeddah, Saudi Arabia



**David Eckhoff**  
TUMCREATE  
Singapore, Singapore



**Caroline Fontaine**  
CNRS/Lab-STICC/CID and Telecom Bretagne  
Lab-STICC/CID and Telecom Bretagne/ITI  
Brest Cedex 3, France



**Sara Foresti**  
Dipartimento di Informatica  
Università degli Studi di Milano  
Milano, Italy



**Steven Furnell**  
School of Computer Science  
University of Nottingham  
Nottingham, UK



**Yufei Han**  
PIRAT team  
INRIA Center at University of Rennes  
Rennes, France



**Murat Kantarcioglu**  
Computer Science Department  
University of Texas at Dallas  
Richardson, TX, USA



**Ramesh Karri**  
Tandon School of Engineering  
Polytechnic Institute  
New York University  
Brooklyn, NY, USA



**Sokratis K. Katsikas**  
Department of Information Security and  
Communication Technology  
Norwegian University of Science and  
Technology – NTNU  
Gjøvik, Norway



**Aggelos Kiayias**  
School of Informatics  
University of Edinburgh and IOG  
Edinburgh, UK



**Tanja Lange**  
Department of Mathematics and  
Computer Science  
Coding Theory and Cryptology  
Eindhoven Institute for  
the Protection of Systems  
and Information  
Technische Universiteit Eindhoven  
Eindhoven, The Netherlands



**Javier Lopez**  
Computer Science  
University of Malaga  
Malaga, Spain



**Luigi V. Mancini**  
Dipartimento di Informatica  
Università di Roma “La Sapienza”  
Rome, Italy



**Catherine Meadows**  
US Naval Research Laboratory  
Washington, DC, USA

Mantua Drive  
Fairfax VA, USA



**Alfred Menezes**  
Department of Combinatorics and  
Optimization  
University of Waterloo  
Waterloo, ON, Canada



**David Naccache**  
Computer Science Department  
Ecole normale supérieure  
Paris, France



**Suku Nair**  
Vice Provost for Research and  
Chief Innovation Officer  
Director of AT&T Center for Virtualization  
University Distinguished Professor, SMU  
Dallas, TX, USA



**Christof Paar**  
Max Planck Institute for  
Security and Privacy  
Bochum, Germany



**Pankaj Pandey**  
Department of Information  
Security and Communication  
Technology  
Norwegian University of Science  
and Technology  
Gjøvik, Norway



**Stefano Paraboschi**  
DIGIP  
Università degli Studi di Bergamo  
Bergamo, Italy



**Gerardo Pelosi**  
Politecnico di Milano  
Department of Electronics  
Information and Bioengineering – DEIB  
Milan, Italy

**Guenther Pernul**

Department of Information Systems  
Fakultät für Informatik und Data Science  
Universität Regensburg  
Regensburg, Germany

**Pierluigi Perri**

Department “Cesare Beccaria”  
University of Milan  
Milan, Italy

**Giuseppe Persiano**

Dipartimento di Scienze Aziendali  
Università di Salerno  
Fisciano (SA), Italy

**Vincenzo Piuri**

Department of Computer Science  
Università degli Studi di Milano  
Milano, Italy

**Michalis Polychronakis**

Computer Science  
Stony Brook University  
Stony Brook, NY, USA

**Bart Preneel**

Department of Electrical  
Engineering ESAT/COSIC  
KU Leuven  
Leuven, Belgium

**Kazue Sako**

Department of Computer Science and Engineering  
Waseda University  
Tokyo, Japan

**Berry Schoenmakers**

Mathematics and Computer Science  
TU Eindhoven  
Eindhoven, Netherlands



**Fabio Scotti**  
Department of Computer Science  
Università degli Studi di Milano  
Milano (MI), Italy



**François-Xavier Standaert**  
Université Catholique de Louvain  
Louvain-la-Neuve, Belgium



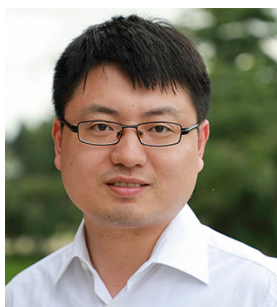
**Jaideep Vaidya**  
Management Science and Information  
Systems  
Rutgers University  
Newark, NJ, USA



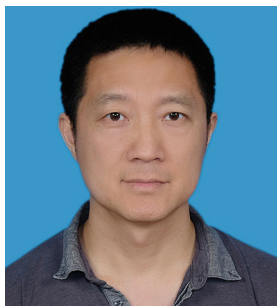
**Venkat Venkatakrisnan**  
Computer Science  
University of Illinois at Chicago and Discovery  
Partners Institute  
Chicago, IL, USA

**Isabel Wagner**

Department of Mathematics and Computer  
Science  
University of Basel  
Basel, Switzerland

**Suhang Wang**

College of Information Sciences and Technology  
The Pennsylvania State University  
University Park  
PA, USA

**Ting Yu**

Computer Science  
Mohamed bin Zayed University of Artificial  
Intelligence (MBZUAI)  
Abu Dhabi, United Arab Emirates

---

## List of Contributors

**Andrea F. Abate** Department of Computer Science, University of Salerno, Fisciano, Italy

**Hanaa Abbas** ICT Division, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

**Saeed Abu-Nimeh** Damballa Inc, Atlanta, GA, USA

**Alessandro Acquisti** Carnegie Mellon University, Pittsburgh, PA, USA

**Gergely Acs** CrySyS Lab, Department of Networked Systems and Services, Budapest University of Technology and Economics (BME-HIT), Budapest, Hungary

**Nabil Adam** Department of Management Science and Information Systems, CIMIC, Rutgers, The State University of New Jersey, Newark, NJ, USA

**Carlisle Adams** School of Electrical Engineering and Computer Science (EECS), University of Ottawa, Ottawa, ON, Canada

**Charu C. Aggarwal** IBM T. J. Watson Research Center, Hawthorne, NY, USA

**Chuahdhy Mujeeb Ahmed** University of Strathclyde, Glasgow, UK

**Mohammad Abdullah Al Faruque** University of California, Irvine, CA, USA

**Khalil Al-Hussaeni** Department of Computer Science, Rochester Institute of Technology, Dubai, UAE

**Ehab Al-Shaer** Cyber Defense and Network Assurability (CyberDNA) Center, Department of Software and Information Systems College of Computing and Informatics, University of North Carolina Charlotte, Charlotte, NC, USA

**Massimiliano Albanese** Center for Secure Information Systems, George Mason University, Fairfax, VA, USA

**Cristina Alcaraz** Computer Science Department, University of Malaga Campus de Teatinos s/n, Malaga, Spain

**Mohammad E. Alim** The University of Alabama in Huntsville, Huntsville, AL, USA

**Vijay Alturi** Management Science and Information Systems Department,  
Center for Information Management, Integration and Connectivity, Rutgers  
University, Newark, NJ, USA

**Jim Alves-Foss** Department of Computer Science, University of Idaho,  
Moscow, ID, USA

**Ghous Amjad** Brown University, Providence, RI, USA

**Marios Anagnostopoulos** Department of Information Security and Com-  
munication Technology, Norwegian University of Science and Technology,  
Gjøvik, Norway

**Nicolas AnCIAUX** Inria Saclay Île-de-France, Palaiseau, France

**Sebastian Angel** Microsoft Research, Redmond, WA, USA

University of Pennsylvania, PA, USA

**Angelos Antonopoulos** The University of Texas at Dallas, Richardson, TX,  
USA

**Claudio A. Ardagna** Dipartimento di Informatica, Università degli Studi di  
Milano, Milan, Italy

**Hafiz Asif** Rutgers University, Newark, NJ, USA

**Michael Atighetchi** Raytheon BBN, Cambridge, MA, USA

**Maurizio Atzori** DMI, University of Cagliari, Cagliari, Italy

**Roberto Avanzi** ARM Germany GmbH, Grasbrunn, Germany  
ARM, Bochum, Germany

**Gildas Avoine** INSA Rennes, Univ Rennes, IRISA, CNRS, Rennes, France

**Mikel Awad** St. Petersburg, FL, USA

**Erman Ayday** Bilkent University, Ankara, Turkey

Case Western Reserve University, Cleveland, OH, USA

**Kimia Zamiri Azar** George Mason University, Fairfax, VA, USA

**Enrico Bacis** Google, Zurich, Switzerland

**Maria Bada** Department of Computer Science and Technology, Cambridge  
Cybercrime Centre, University of Cambridge, Cambridge, UK

**Ali Bagherzandi** University of California, Irvine, CA, USA

**Leila Bahri** Royal Institute of Technology, Stockholm, Sweden

**Harald Baier** Research Institute CODE, Universität der Bundeswehr  
München, Munich, Germany

**Spiridon Bakiras** College of Science and Engineering, Hamad Bin Khalifa  
University, Doha, Qatar

**Suman Banerjee** Department of Computer Sciences, University of Wisconsin at Madison, Madison, WI, USA

**Ankan Bansal** University of Maryland, College Park, MD, USA

**K. Suzanne Barber** Center for Identity, The University of Texas at Austin, Austin, TX, USA

**Alessandro Barenghi** Department of Electronics, Information and Bioengineering – DEIB, Politecnico di Milano, Milan, Italy

**Sergio Barezani** Dipartimento di Informatica, Università degli Studi di Milano, Milan, Italy

**Alexander Barg** Department of Electrical and Computer Engineering, University of Maryland, College Park, MD, USA

**Paulo S. L. Barreto** Department of Computer and Digital Systems Engineering (PCS), Escola Politécnica, University of São Paulo (USP), São Paulo, Brazil

**Anomadarsi Barua** University of California, Irvine, CA, USA

**Kanad Basu** Department of Electrical and Computer Engineering, University of Texas, Dallas, TX, USA

**Lejla Batina** Radboud University, Nijmegen, The Netherlands

**Gunjan Batra** Kennesaw State University, Kennesaw, GA, USA

**Friedrich L. Bauer** Nördliche Villenstrasse, Kottgeisering, Germany

**Steffen Becker** Max Planck Institute for Security and Privacy, Bochum, Germany

Ruhr University Bochum, Bochum, Germany

**Carly Beckerman** Institute of Hazard Risk and Resilience and the School of Government and International Affairs, University of Durham, Durham, UK

**Homayoon Beigi** Research, Recognition Technologies, Inc., South Salem, NY, USA

**Amos Beimel** Department of Computer Science, Ben Gurion University of the Negev, Beer-Sheva, Israel

**David Elliott Bell** Reston, VA, USA

**Marta Bellés-Muñoz** Universitat Pompeu Fabra, Barcelona, Spain

**Steven M. Bellovin** Department of Computer Science, Columbia University, New York, NY, USA

**Nicola Bena** Dipartimento di Informatica, Università degli Studi di Milano, Milan, Italy

**Olivier Benot** Ingenico, Région de Saint-Étienne, France

**Malek Ben Salem** Accenture, Arlington, VA, USA

**Daniel J. Bernstein** Department of Computer Science, University of Illinois at Chicago, Chicago, IL, USA

**Filippo Berto** Dipartimento di Informatica, Università degli Studi di Milano, Milan, Italy

**Claudio Bettini** Department of Computer Science, Università degli Studi di Milano, Milano, Italy

**Bhaveer Bhana** Department of Information Systems, Rhodes University, Grahamstown, South Africa

**Bhawani Shanker Bhati** TUMCREATE Ltd., Singapore, Singapore

**Swarup Bhunia** University of Florida, Gainesville, FL, USA

**Kaigui Bian** Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA, USA

**Gergely Biczók** CrySyS Lab, Department of Networked Systems and Services, Budapest University of Technology and Economics (BME-HIT), Budapest, Hungary

**Frdrique Biennier** LIESP, INSA de Lyon, Villeurbanne, France

**Eli Biham** Department of Computer Science, Technion—Israel Institute of Technology, Haifa, Israel

**Leyla Bilge** NortonLifeLock Research Group, Antibes, France

**Alex Biryukov** FDEF, Campus Limpertsberg, University of Luxembourg, Luxembourg City, Luxembourg

**Matt Bishop** Department of Computer Science, University of California at Davis, Davis, CA, USA

**Joachim Biskup** Fakultät für Informatik, Technische Universität Dortmund, Dortmund, Germany

**J. Black** Department of Computer Science, Boulder, CO, USA

**G. R. Blakley** Department of Mathematics, Texas A&M University, College Station, TX, USA

**Gerrit Bleumer** Research and Development, Francotyp Group, Birkenwerder bei Berlin, Germany

**Carlo Blundo** Dipartimento di Scienze Aziendali – Management and Innovation Systems, Università degli Studi di Salerno, Fisciano, Italy

**Jonas Böhler** SAP Security Research, SAP SE, Karlsruhe, Germany

**Fabian Böhm** Chair of Information Systems, University of Regensburg, Regensburg, Germany

**Alexandra Boldyreva** School of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA

**Piero A. Bonatti** Dipartimento di Ingegneria Elettrica e Tecnologie dell'Informazione, Università di Napoli Federico II, Napoli, Italy

**Emma Bond** University of Suffolk, Ipswich, UK

**Dan Boneh** Department of Computer Science, Stanford University, Stanford, CA, USA

**Surekha Borra** Department of ECE, K.S. Institute of Technology, Bangalore, Karnataka, India

**Antoon Bosselaers** Department of Electrical Engineering, Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium

**Luc Bouganim** Inria Saclay Île-de-France, Palaiseau, France

**Emilie Bout** Inria Lille Nord-Europe, Lille, France

**Brian M. Bowen** Department of Computer Science, Columbia University, New York, NY, USA

**Xavier Boyen** Queensland University of Technology, Brisbane, QLD, Australia

**Gilles Brassard** Department IRO, Université de Montréal, Montreal, QC, Canada

**Vladimir Briik** Department of Computer Sciences, University of Wisconsin at Madison, Madison, WI, USA

**Gerald Brose** Hype Softwaretechnik GmbH, Bonn, Germany

**David Brumley** Electrical and Computer Engineering Department, Department of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA

**Marco Bucci** Fondazione Ugo Bardoni, Rome, Italy

**Ileana Buhan** Radboud University, Nijmegen, The Netherlands

**Benedikt Büinz** New York University, New York, USA

**Diana L. Burley** American University, Washington, DC, USA

**Mike Burmester** Department of Computer Science, Florida State University, Tallahassee, FL, USA

**Kaliski Burt** Office of the CTO, EMC Corporation, Hopkinton, MA, USA

**Christoph Busch** Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

**Laurent Bussard** European Microsoft Innovation Center, Aachen, Germany

**Enrique Cabello** URJC, Madrid, Spain

**Christian Cachin** IBM Research – Zurich, Rüschlikon, Switzerland

**Tom Caddy** InfoGard Laboratories, San Luis Obispo, CA, USA

**Jon Callas** Indiana University, Bloomington, IN, USA

**Alessandro Campi** Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milan, Italy

**Patrizio Campisi** Section of Applied Electronics, Department of Engineering, Roma Tre University, Rome, Italy

Department of Applied Electronics, Università degli Studi Roma TRE, Rome, Italy

**G. Camurati** ETH Zurich, Zurich, Switzerland

**Ran Canetti** The Blavatnik School of Computer Sciences, Tel Aviv University, Tel Aviv, Israel

**Ebru Celikel Cankaya** Department of Computer Science, University of Texas at Dallas, Richardson, TX, USA

**Hakki C. Cankaya** Masergy Communications, Inc., Plano, TX, USA

**Anne Canteaut** Project-Team SECRET, INRIA Paris-Rocquencourt Le Chesnay, France

**Guohong Cao** The Pennsylvania State University, University Park, PA, USA

**Yang Cao** Kyoto University, Kyoto, Japan

**Srdjan Capkun** Department of Computer Science, System Security Group, ETH Zurich, Zürich, Switzerland

**Elias G. Carayannis** School of Business, George Washington University, Washington, DC, USA

**Alvaro A. Cardenas** University of California, Santa Cruz, CA, USA

**Jaime S. Cardoso** INESC TEC and Faculdade de Engenharia da Universidade do Porto, Porto, Portugal

**Claude Carlet** Département de mathématiques at LAGA, Université Paris 8, Saint-Denis Cedex, France

**Barbara Carminati** DISTA, Università degli Studi dell'Insubria, Varese, Italy

**William D. Casper** High Assurance Computing and Networking Labs (HACNet), Department of Computer Science and Engineering, Bobby B. Lyle School of Engineering, Southern Methodist University, Houston, TX, USA

**Gaëtan Cassiers** UCLouvain, Louvain-la-Neuve, Belgium

**Aniello Castiglione** Department of Science and Technology, University of Naples Parthenope, Naples, Italy

**Ebru Celikel Cankaya** Department of Computer Science and Engineering, University of North Texas, Denton, TX, USA

**Anrin Chakraborti** Stony Brook University, Stony Brook, NY, USA

**Abhishek Chakraborty** University of Maryland, College Park, MD, USA

**Rajat Subhra Chakraborty** Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India

**Manuel M. T. Chakravarty** IOG, Utrecht, The Netherlands

**David Challener** Applied Physics Laboratory, Johns Hopkins University, Laurel, MD, USA

**Pascale Charpin** INRIA, Rocquencourt, Le Chesnay Cedex, France

**Rama Chellappa** Johns Hopkins University, Baltimore, MD, USA

**Rongmao Chen** National University of Defense Technology, Changsha, China

**Bee-Chung Chen** Yahoo! Research, Mountain View, CA, USA

**Chen-Mou Cheng** Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan

**Mihai Chiroiu** Computer Science and Engineering Department, University POLITEHNICA of Bucharest, Bucharest, Romania

**Young B. Choi** Department of Natural Science, Mathematics and Technology, School of Undergraduate Studies, Regent University, Virginia Beach, VA, USA

**Hamid Choukri** Gemalto Compagny, Meudon, France

**Sherman S. M. Chow** Department of Information Engineering, Chinese University of Hong Kong, Shatin, Hong Kong

**Mihai Christodorescu** IBM T.J. Watson Research Center, Hawthorne, NY, USA

**Stelvio Cimato** Department of Computer Science, Università degli studi di Milano, Milan, Italy

**Cosmin Ciobanu** EU Agency for Cybersecurity (ENISA), Heraklion, Greece

**Andrew Clark** Information Security Institute, Queensland University of Technology, Brisbane, QLD, Australia

**Nathan Clarke** University of Plymouth, Plymouth, UK

**Jiska Classen** Secure Mobile Networking Lab, TU Darmstadt, Darmstadt, Germany

**Christopher W. Clifton** CS Department, Purdue University, West Lafayette, IN, USA

**Jeff Collins** Southern Methodist University, Dallas, TX, USA  
Ericsson, Plano, TX, USA

**Hiep Cong-Pham** RMIT University Vietnam, Ho Chi Minh City, Vietnam

**Mauro Conti** Department of Mathematics, University of Padua, Padua, Italy

- Scott Contini** Silverbrook Research, Balmain, NSW, Australia
- Debbie Cook** Telcordia Applied Research, Piscataway, NJ, USA
- Sandro Coretti** IOG, Zurich, Switzerland
- Scott E. Coull** RedJack, LLC, Silver Spring, MD, USA
- Lorrie Faith Cranor** School of Computer Science, Carnegie Mellon University, Pittsburgh, PA, USA
- Claude Crépeau** School of Computer Science, McGill University, Montreal, QC, Canada
- Stefano Cresci** Institute for Informatics and Telematics, National Research Council (IIT-CNR), Pisa, Italy
- Eric Cronin** CIS Department, University of Pennsylvania, Philadelphia, PA, USA
- Scott Crosby** Department of Computer Science, Rice University, Houston, TX, USA
- Mary J. Culnan** Information and Process Management Department, Bentley University, Waltham, MA, USA
- Frédéric Cuppens** Polytechnique Montreal, Montreal, Canada  
LUSSI Department, TELECOM Bretagne, Cesson Sévigné Cedex, France
- Nora Cuppens-Boulahia** Polytechnique Montreal, Montreal, Canada  
LUSSI Department, TELECOM Bretagne, Cesson Sévigné Cedex, France
- Reza Curtmola** Department of Computer Science, New Jersey Institute of Technology, Newark, NJ, USA
- Adam Czajka** Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, IN, USA
- Adèle da Veiga** School of Computing, University of South Africa (UNISA), Johannesburg, South Africa
- Italo Dacosta** Department of Computer Sciences, Georgia Institute of Technology, Atlanta, GA, USA
- Joan Daemen** STMicroelectronics, Zaventem, Belgium
- Savino Dambra** Eurecom, Sophia Antipolis, France
- Ernesto Damiani** Dipartimento di Informatica, Università degli Studi di Milano, Milan, Italy
- Antitza Dantcheva** Centre Inria d'Université Côte d'Azur, Sophia Antipolis, France
- Vanesa Daza** Universitat Pompeu Fabra, Barcelona, Spain
- Christophe De Cannière** Department of Electrical Engineering, Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium

**Sabrina De Capitani di Vimercati** Dipartimento di Informatica, Università degli Studi di Milano, Milano, Italy

**Danny De Cock** Department of Electrical Engineering-ESAT/COSIC, Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium

**Maria De Marsico** Department of Computer Science, Sapienza University of Rome, Rome, Italy

**Marijke De Soete** Security4Biz, Oostkamp, Belgium

**Răzvan Deaconescu** Computer Science and Engineering Department, University POLITEHNICA of Bucharest, Bucharest, Romania

**Hua Deng** College of Computer Science and Electronic Engineering, Hunan University, Changsha, China

**Alexander W. Dent** Information Security Group, Royal Holloway, University of London, Surrey, UK

**Luke Deshotels** TikTok, Culver City, CA, USA

**Yvo Desmedt** Department of Computer Science, The University of Texas at Dallas, Richardson, TX, USA

**Nilanjan Dey** Department of Computer Science and Engineering, JIS University, Kolkata, West Bengal, India

**Roberto Di Pietro** ICT Division, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

CEMSE, King Abdullah University of Science and Technology, Thuwal, Saudi Arabia

**Vasiliki Diamantopoulou** Department of Information and Communication Systems Engineering, University of the Aegean, Samos, Greece

**Claudia Diaz** KU Leuven, Leuven, Belgium

**Sarah Diesburg** University of Northern Iowa, Cedar Falls, IA, USA

**Christoph Dobraunig** Intel Labs, Intel Corporation, Hillsboro, OR, USA

**Yevgeniy Dodis** Department of Computer Science, New York University, New York, NY, USA

**Josep Domingo-Ferrer** Department of Computer Engineering and Mathematics, Universitat Rovira i Virgili, Tarragona, Spain

**Changyu Dong** School of Computing, Newcastle University, Newcastle Upon Tyne, UK

**Jing Dong** Google, San Francisco, CA, USA

Center for Research on Intelligent Perception and Computing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, People's Republic of China

**Ruggero Donida Labati** Department of Computer Science, Università degli Studi di Milano, Milan, Italy

**Nicola Dragoni** Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Kongens Lyngby, Denmark

**Glenn Durfee** San Francisco, CA, USA

**Edlira Dushku** DTU Compute, Technical University of Denmark (DTU), Kongens Lyngby, Denmark

Department of Applied Mathematics and Computer Science, Technical University of Denmark (DTU), Kongens Lyngby, Denmark

Department of Electronic Systems, Aalborg University, Copenhagen, Denmark

**Cynthia Dwork** Microsoft Research, Mountain View, CA, USA

**David Eckhoff** TUMCREATE Ltd., Singapore, Singapore

**Wesley M. Eddy** MTI Systems, Cleveland, OH, USA

**Pavlos S. Efrimidis** Department of Electrical and Computer Engineering, Democritus University of Thrace, Xanthi, Greece

**Thomas Eisenbarth** Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL, USA

**Omar El-Gayar** Dakota State University, Madison, SD, USA

**Carl M. Ellison** New York, NY, USA

**William Enck** Department of Computer Science, North Carolina State University, Raleigh, NC, USA

Department of Computer Science and Engineering, The Pennsylvania State University, University Park, PA, USA

**Paul England** Microsoft Corporation, Redmond, WA, USA

**Ludwig Englbrecht** Chair of Information Systems, University of Regensburg, Regensburg, Germany

**Aaron Estes** Department of Computer Science and Engineering, Lyle School of Engineering, Southern Methodist University, Dallas, TX, USA

**Martin Evison** Forensic Science Program, University of Toronto, Mississauga, ON, Canada

**Xenofon Fafoutis** Technical University of Denmark (DTU), Kgs. Lyngby, Denmark

**Aristeidis Farao** Department of Digital Systems, University of Piraeus, Piraeus, Greece

**Hannes Federrath** Distributed Systems Security, Computer Science Department, University of Hamburg, Hamburg, Germany

- Serge Fenet** LIRIS UMR 5205, Université Claude Bernard Lyon 1, Villeurbanne cedex, France
- David Ferraiolo** National Institute of Standards and Technology, Gaithersburg, MD, USA
- Elena Ferrari** DISTA, Università degli Studi dell'Insubria, Varese, Italy
- Julian Fierrez** Universidad Autonoma de Madrid, Madrid, Spain
- Matthieu Finiasz** ENSTA, Palaiseau, France
- Matthias Fitzi** IOG, Zurich, Switzerland
- Francesco Flammini** School of Innovation, Design and Engineering, Division of Product Realisation, Mälardalen University, Västerås, Sweden  
Linnaeus University, Växjö, Sweden
- Stephen Flowerday** Department of Information Systems, Rhodes University, Grahamstown, South Africa
- Caroline Fontaine** Lab-STICC/CID and Telecom Bretagne/ITI, CNRS/Lab-STICC/CID and Telecom Bretagne, Brest, France
- Sara Foresti** Dipartimento di Informatica, Università degli Studi di Milano, Milano, Italy
- Dario V. Forte** University of Milano, Crema, Italy
- A. Francillon** EURECOM, Sophia-Antipolis, France
- Benjamin C. M. Fung** School of Information Studies, McGill University, Montreal, QC, Canada
- Steven Furnell** School of Computer Science, University of Nottingham, Nottingham, UK
- Ernst M. Gabidulin** Department of Radio Engineering, Moscow Institute of Physics and Technology (State University), Zhukovsky, Russia
- Alban Gabillon** Laboratoire Gepasud, Université de la Polynésie Française, Tahiti, French Polynesia
- Philippe Gaborit** XLIM-DMI, University of Limoges, Limoges, France
- Rhonda Gaede** The University of Alabama in Huntsville, Huntsville, AL, USA
- Martin Gagné** Department of Computer Science, University of Calgary, Calgary, AB, Canada
- Clemente Galdi** Department of Political and Social Studies, University of Salerno, Fisciano (SA), Italy
- Vinod Ganapathy** Department of Computer Science, Rutgers, The State University of New Jersey, Piscataway, NJ, USA

**Juan A. Garay** Department of Computer Science and Engineering, Texas A&M University, College Station, TX, USA

**William C. Garrison III** Department of Computer Science, University of Pittsburgh, Pittsburgh, PA, USA

**Pierrick Gaudry** CNRS – INRIA, Université de Lorraine, Nancy, France

**Peter Gaži** IOG, Bratislava, Slovakia

**Johannes Gehrke** Microsoft Research, Redmond, WA, USA

**Sutanu Kumar Ghosh** University of Illinois Chicago, Chicago, IL, USA

**Thanassis Giannetsos** UBITECH ubiquitous solutions, Athens, Greece

**Rigel Gjomemo** University of Illinois Chicago, Chicago, IL, USA

**Vasileios Gkioulos** Department of Information Security and Communications Technology, Norwegian University of Science and Technology, Trondheim, Norway

**Marta Gomez-Barrero** Fakultät Wirtschaft, Hochschule Ansbach, Ansbach, Germany

**Dan Gordon** IDA Center for Communications Research, San Diego, CA, USA

**Elisa Gorla** Department of Mathematics, University of Basel, Basel, Switzerland

**Louis Goubin** Versailles St-Quentin-en-Yvelines University, Versailles, France

**Tyrone Grandison** Intelligent Information Systems, IBM Services Research, Hawthorne, NY, USA

**SueAnne Griffith** Center for Cybersecurity Research and Education, The University of Alabama in Huntsville, Huntsville, AL, USA

Department of Electrical and Computer Engineering, Auburn University, Auburn, AL, USA

**Evangelos Grigoroudis** School of Production Engineering and Management, Technical University of Crete, Chania, Greece

**Vincent Grosso** CNRS and Laboratoire Hubert Curien, Saint-Etienne, France

**Jens Groth** DFINITY, Zurich, Switzerland

**Daniel Gruss** Graz University of Technology, Graz, Austria

**Marco Gruteser** Wireless Information Network Laboratory, Department of Electrical and Computer Engineering, Rutgers University, North Brunswick, NJ, USA

**Guofei Gu** Department of Computer Science and Engineering, Texas A&M University, College Station, TX, USA

**Qijun Gu** Department of Computer Science, Texas State University-San Marcos, San Marcos, TX, USA

**Jorge Guajardo** Bosch Research and Technology Center North America, Pittsburgh, PA, USA

**Tim E. Güneysu** Department of Electrical Engineering and Information Technology, Ruhr-University Bochum, Bochum, Germany

**Fuchun Guo** Institute of Cybersecurity and Cryptology, School of Computing and Information Technology, University of Wollongong, Wollongong, NSW, Australia

**Yanli Guo** Inria Saclay Île-de-France, Palaiseau, France

**Stuart Haber** HP Labs, Princeton, NJ, USA

**Hakan Hacigümüş** Google, NEC Research Labs, Cupertino, CA, USA

**Jesse R. Hairston** The University of Alabama in Huntsville, Huntsville, AL, USA

**Xu Han** Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing, China

**Helena Handschuh** Computer Security and Industrial Cryptography Research Group, Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium

**Darrel Hankerson** Department of Mathematics, Auburn University, Auburn, AL, USA

**Michael A. Harper** St. Petersburg, FL, USA

**Kjell Hausken** Faculty of Science and Technology, University of Stavanger, Stavanger, Norway

**Karin Hedström** Informatics, CERIS, Örebro University School of Business, Örebro, Sweden

**Clemens Heinrich** Francotyp-Postalia GmbH, Birkenwerder, Germany

**Tor Helleseth** The Selmer Center, Department of Informatics, University of Bergen, Bergen, Norway

**Hemantha S. B. Herath** Goodman School of Business, Brock University, St. Catharines, ON, Canada

**Tejaswini C. Herath** Goodman School of Business, Brock University, St. Catharines, ON, Canada

**Christopher Hodson** CISO, Tanium, Reading, UK

**Jeff Hoffstein** Mathematics Department, Brown University, Providence, RI, USA

**Michael D. Hogan** Information Technology Laboratory (ITL), National Institute of Standards and Technology, Gaithersburg, MD, USA

**Matthias Hollick** Secure Mobile Networking Lab, TU Darmstadt, Darmstadt, Germany

**Justin Holmgren** NTT Research, Berkeley, CA, USA

**Bijit Hore** Donald Bren School of Computer Science, GarbleCloud, University of California, Irvine, CA, USA

**Dwight Horne** AT&T Center for Virtualization, Southern Methodist University, Dallas, TX, USA

**Russ Housley** Vigil Security, LLC, Herndon, VA, USA

**Jiankun Hu** School of Engineering and Information Technology, University of New South Wales, Canberra, ACT, Australia

**Xinyi Huang** Jinan University, Guangzhou, China

**Kévin Huguenin** University of Lausanne, Lausanne, Switzerland

**Mathias Humbert** Cyber-Defence Campus, armasuisse Science and Technology, Thun, Switzerland

**Michael T. Hunter** School of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA

**Omar Adel Ibrahim** ICT Division, College of Science and Engineering, Hamad Bin Khalifa University, Doha, Qatar

**Hideki Imai** Faculty of Science and Engineering, Chuo University, Bunkyo-ku, Tokyo, Japan

**Sebastiaan Indestege** Department of Electrical Engineering-ESAT/COSIC, Katholieke Universiteit Leuven and IBBT, Leuven-Heverlee, Belgium

**Christos Ioannidis** Aston Business School, Aston University, Birmingham, UK

**John Ioannidis** Google, Inc, New York, NY, USA

**Yuval Ishai** Technion, Haifa, Israel

**Arun Iyengar** IBM Research Division, Thomas J. Watson Research Center, Yorktown Heights, NY, USA

**Collin Jackson** CyLab, Department of Electrical and Computer Engineering, Carnegie Mellon University, Moffett Field, CA, USA

**Nina Jacobsen** University of Maryland, College Park, MD, USA

**Trent Jaeger** Systems and Internet Infrastructure Security Lab, Pennsylvania State University, University Park, PA, USA

**Goce Jakimoski** NIKSUN Inc, Princeton, NJ, USA

**David Jao** Department of Combinatorics & Optimization, University of Waterloo, Waterloo, ON, Canada

- Yousra Javed** School of Information Technology, Illinois State University, Normal, IL, USA
- Martin Johns** SAP Research CEC Karlsruhe, SAP AG, Karlsruhe, Germany
- Jim Jones** George Mason University, Fairfax, VA, USA
- Antoine Joux** Laboratoire Prism, Universit de Versailles Saint-Quentin-en-Yvelines, Versailles Cedex, France
- Marc Joye** Zama, Paris, France
- Ari Juels** Cornell Tech and Initiative for CryptoCurrencies and Contracts (IC3), New York City, NY, USA
- Mike Just** Department of Computer Science, Heriot-Watt University, Edinburgh, UK
- Glasgow Caledonian University, Glasgow, UK
- Charanjit Jutla** IBM T. J. Watson Research Center, Yorktown Heights, NY, USA
- Gregory Kabatiansky** Dobrushin Mathematical Lab, Institute for Information Transmission Problems RAS, Moscow, Russia
- Severin Kacianka** Technical University of Munich, Munich, Germany
- Burt Kaliski** Office of the CTO, EMC Corporation, Hopkinton, MA, USA
- Hadi Mardani Kamali** George Mason University, Fairfax, VA, USA
- Seny Kamara** Brown University, Providence, RI, USA
- Brent Byung Hoon Kang** Department of Applied Information Technology and Centre for Secure Information Systems, The Volgenau School of Engineering, George Mason University, Fairfax, VA, USA
- Vivek Kanhangad** Department of Electrical Engineering, Indian Institute of Technology Indore, Indore, India
- Mohan Kankanhalli** National University of Singapore, Singapore, Singapore
- Sreeram Kannan** University of Washington at Seattle, Seattle, WA, USA
- Murat Kantarcioglu** University of Texas at Dallas, Richardson, TX, USA
- Frank Kargl** Institute of Distributed Systems, Ulm University, Ulm, Germany
- Naghmeh Karimi** Department of Computer Science and Electrical Engineering, University of Maryland Baltimore County, Baltimore, MD, USA
- Fredrik Karlsson** Informatics, CERIS, Örebro University School of Business, Örebro, Sweden
- Maria Karyda** Department of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, Samos, Greece

**Timo Kasper** Horst Görst Institute for IT Security, Ruhr University Bochum, Bochum, Germany

**Polinpapilinho F. Katina** Department of Informatics and Engineering Systems, University of South Carolina Upstate, Spartanburg, SC, USA

**Vasilios Katos** Bournemouth University, Bournemouth, UK

**Sokratis K. Katsikas** Norwegian Centre for Cybersecurity in Critical Sectors (NORCICS), Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

**Basel Katt** Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

**Stefan Katzenbeisser** Security Engineering Group, Technische Universität Darmstadt, Darmstadt, Germany

**Joakim Kävrestad** School of Informatics, University of Skövde, Skövde, Sweden

**Christodoulos Keliris** KIOS Research and Innovation Center of Excellence and Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus

**Angelos D. Keromytis** School of Electrical and Computer Engineering, Georgia Institute of Technology, Atlanta, GA, USA

**Florian Kerschbaum** Cheriton School of Computer Science, University of Waterloo, Waterloo, ON, Canada

**George Kesidis** Computer Science & Engineering and Electrical Engineering Departments, Pennsylvania State University, University Park, PA, USA

**Youssef Khazbak** The Pennsylvania State University, University Park, PA, USA

**Aggelos Kiayias** School of Informatics, University of Edinburgh and IOG, Edinburgh, UK

Department of Computer Science Engineering, University of Connecticut, Storrs, CT, USA

**Daniel Kifer** Department of Computer Science and Engineering, Penn State University, University Park, PA, USA

**Johannes Kinder** Formal Methods in Systems Engineering, Technische Universität Darmstadt, Darmstadt, Germany

**Michel A. Kinsy** Department of Electrical and Computer Engineering, Adaptive and Secure Computing Systems (ASCS) Laboratory, Texas A&M University, College Station, TX, USA

**Engin Kirda** Institut Eurecom, Sophia Antipolis, France

**Amit Klein** Trusteer, Tel Aviv, Israel

**Lars R. Knudsen** Department of Mathematics, Technical University of Denmark, Lyngby, Denmark

**Çetin Kaya Koç** Department of Computer Science, University California Santa Barbara, Santa Barbara, CA, USA

College of Engineering and Natural Sciences, Istanbul Sehir University, Istanbul, Turkey

**François Koeune** Crypto Group, ICTEAM Institute, UCLouvain, Louvain-la-Neuve, Belgium

Microelectronics Laboratory, Université catholique de Louvain, Louvain-la-Neuve, Belgium

**Spyros Kokolakis** Department of Information & Communication Systems Engineering, University of the Aegean, Karlovassi, Greece

**Stefan Köpsell** Department of Computer Science, Institute of Systems Architecture, Technische Universität, Dresden, Germany

**Maciej Korczyński** University Grenoble Alpes, CNRS, Grenoble INP, LIG, Grenoble, France

**Sokol Kosta** Department of Electronic Systems, Aalborg University, Copenhagen, Denmark

**Stewart Kowalski** Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway

**Hugo Krawczyk** Algorand Foundation, NY, USA

**Hennie Kruger** School of Computer Science and Information Systems, North-West University, Potchefstroom, South Africa

**Alexander Kruppa** Projet CACAO, LORIA, Villers-lès-Nancy Cedex, France

**Markus G. Kuhn** Department of Computer Science and Technology, University of Cambridge, Cambridge, UK

**Kaoru Kurosawa** National Institute of Advanced Industrial Science and Technology and Research and Development Initiative, Chuo University, Tokyo, Japan

**Klaus Kursawe** Vega Protocol, London, UK

Vega Project, Geneva, Switzerland

**Junzuo Lai** Jinan University, Guangzhou, China

**Russell W. F. Lai** Department of Computer Science, Aalto University, Espoo, Finland

**Peter Landrock** Cryptomathic Ltd, Cambridge, UK

**Jean-Louis Lanet** Department of Mathematics and Computer Science, University of Limoges, Limoges, France

**Tanja Lange** Coding Theory and Cryptology, Eindhoven Institute for the Protection of Systems and Information, Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, Eindhoven, The Netherlands

**Andreas Lanitis** Visual Media Computing Lab, Department of Multimedia and Graphic Arts, Cyprus University of Technology & Research Centre on Interactive Media and Emerging Technologies, Limassol, Cyprus

**Chun Pong Lau** Johns Hopkins University, Baltimore, MD, USA

**Gregor Leander** Department of Mathematics, Technical University of Denmark, Lyngby, Denmark

**Adam J. Lee** Department of Computer Science, University of Pittsburgh, Pittsburgh, PA, USA

**Kristen LeFevre** Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, MI, USA

**Arjen K. Lenstra** Laboratory for cryptologic algorithms – LACAL, School of Computer and Communication Sciences, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland

**Reynald Lercier** Institut de recherche mathématique de Rennes, Université de Rennes 1, Rennes Cedex, France

**Szilvia Lestyán** CrySyS Lab, Department of Networked Systems and Services, Budapest University of Technology and Economics (BME-HIT), Budapest, Hungary

**Paul Leyland** Brnikat Limited, Little Shelford, Cambridge, UK

**Na Li** Department of Computer Science, Prairie View A&M University, Prairie View, TX, USA

**Ninghui Li** Purdue University, West Lafayette, IN, USA

**Ming Li** Department of ECE, University of Arizona, Tucson, AZ, USA

**Stan Z. Li** Center for Biometrics and Security Research, Institute of Automation, Chinese Academy of Sciences, Beijing, People's Republic of China

**Yang Li** The University of Electro-Communications, Tokyo, Japan

**Xu Liang** Shenzhen Institute of Artificial Intelligence and Robotics for Society, Shenzhen, China

Bio-Computing Research Center, Harbin Institute of Technology, Shenzhen, China

**Xueqin Liang** State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an, China

Department of Communications and Networking, Aalto University, Espoo, Finland

**Benoît Libert** Microelectronics Laboratory, Université catholique de Louvain, Louvain-la-Neuve, Belgium

**Shinyoung Lim** School of Health and Rehabilitation Services, University of Pittsburgh, Pittsburgh, PA, USA

**Moses Liskov** Department of Computer Science, The College of William and Mary, Williamsburg, VA, USA

**Bo Liu** School of Computer Science, University of Technology Sydney, Sydney, NSW, Australia

**Yuntao Liu** University of Maryland, College Park, MD, USA

**Zongyi Liu** Amazon.com, Seattle, WA, USA

**Peng Liu** The Pennsylvania State University, University Park, PA, USA

**Donggang Liu** Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX, USA

**Giovanni Livraga** Computer Science Department, Università degli Studi di Milano, Milano, Italy

**Steve Lloyd** Steve Lloyd Consulting Inc., Ottawa, ON, Canada

**Michael E. Locasto** Department of Computer Science, George Mason University, Fairfax, VA, USA

**Flavio Lombardi** IAC-CNR, Rome, Italy

**Valeria Loscri** Inria Lille Nord-Europe, Lille, France

**Wenjing Lou** Department of Computer Science, Virginia Tech, Falls Church, VA, USA

**Haibing Lu** Department of Management Science and Information Systems, CIMIC, Rutgers, The State University of New Jersey, Newark, NJ, USA

**Ashwin Machanavaajhala** Department of Computer Science, Duke University, Durham, NC, USA

**Roel Maes** Intrinsic ID, Eindhoven, The Netherlands

TU Eindhoven, Eindhoven, The Netherlands

**Sasan Mahmoodi** Department of Electronics and Computer Science, University of Southampton, Southampton, UK

**Emanuele Maiorana** Section of Applied Electronics, Department of Engineering, Roma Tre University, Rome, Italy

Department of Applied Electronics, Università degli Studi Roma TRE, Rome, Italy

**Yiorgos Makris** The University of Texas at Dallas, Richardson, TX, USA

**Aakarsh Malhotra** IIIT-Delhi, New Delhi, India

**Nikos Mamoulis** Department of Computer Science and Engineering, University of Ioannina, Ioannina, Greece

**William Mansky** University of Illinois Chicago, Chicago, IL, USA

**Heiko Mantel** Department of Computer Science, TU Darmstadt, Darmstadt, Germany

**Letizia Marchegiani** University of Parma, Parma, Italy

**Eduard Marin** Telefonica Research, Barcelona, Spain

**Fabio Martinelli** Consiglio Nazionale delle Ricerche, Rome, Italy

**Davide Martinenghi** Dipartimento di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, Milano, Italy

**Ivan Martinovic** Department of Computer Science, University of Oxford, Oxford, UK

**Henri Massias** University of Limoges, Limoges, France

**Lee D. McFearnin** Department of Computer Science and Engineering, Southern Methodist University, Dallas, TX, USA

**David McGrew** Poolesville, MD, USA

**Catherine Meadows** U.S. Naval Research Laboratory, Washington, DC, USA

**Marcel Medwed** NXP Semiconductors, Gratkorn, Austria

**Sharad Mehrotra** Department of Computer Science, New Jersey Institute of Technology, Irvine, NJ, USA

**Ricardo Mendes** Huawei Technologies Düsseldorf GmbH, Düsseldorf, Germany

**Alfred Menezes** Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON, Canada

**Di Meng** Department of Electronics and Computer Science, University of Southampton, Southampton, UK

**Weizhi Meng** DTU Compute, Technical University of Denmark, Copenhagen, Denmark

**Yinbin Miao** School of Cyber Engineering, Xidian University, Xi'an, China

- Daniele Micciancio** Department of Computer Science & Engineering, University of California, San Diego, CA, USA
- Evangelia Micheli-Tzanakou** Department of Biomedical Engineering, Rutgers University, Piscataway, NJ, USA
- Jonathan K. Millen** The MITRE Corporation, Bedford, MA, USA
- Jelena Mirkovic** Information Sciences Institute, University of Southern California, Marina del Rey, CA, USA
- Nimish Mishra** Indian Institute of Technology, Kharagpur, India
- Tarik Moataz** MongoDB, New York, NY, USA
- Alip Mohammed** School of Information Studies, McGill University, Montreal, QC, Canada
- Bodo Möller** Google Switzerland GmbH, Zürich, Switzerland
- Refik Molva** EURECOM, Biot Sophia Antipolis, France
- Ankit Mondal** University of Maryland, College Park, MD, USA
- Amir Moradi** Implementation Security Group, Ruhr-University Bochum, Bochum, Germany
- François Morain** Laboratoire d'informatique (LIX), Palaiseau, France
- Aythami Morales** Universidad Autonoma de Madrid, Madrid, Spain
- Emilio Mordini** University of Haifa, Haifa, Israel
- Noria-Onlus, San Vito al Tagliamento, Italy
- Thomas H. Morris** Center for Cybersecurity Research and Education, The University of Alabama in Huntsville, Huntsville, AL, USA
- Department of Electrical and Computer Engineering, Mississippi State University, Mississippi State, MS, USA
- Harold Mouchère** Polytech Nantes, Université de Nantes, IRCCyN, Nantes, France
- Nicky Mouha** Department of Electrical Engineering, Katholieke Universiteit Leuven, Leuven-Heverlee, Belgium
- Tamer Mour** Weizmann Institute of Science, Rehovot, Israel
- Rijoy Mukherjee** Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India
- Debdeep Mukhopadhyay** Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, Kharagpur, India
- Michael Mundt** Esri Deutschland GmbH, Bonn, Germany
- David Naccache** Département d'informatique, Groupe de cryptographie, École normale supérieure Paris, France

**Adwait Nadkarni** William & Mary, Williamsburg, VA, USA

**Elham Naghizade** School of Computing Technologies, RMIT University, Melbourne, VIC, Australia

**Daniel Nagy** Department of Computer Science, ELTECRYPT Research Group Eötvös Loránd University, Budapest, Hungary

**Padmaraj M. V. Nair** Southern Methodist University, Dallas, TX, USA

Department of Computer Science and Engineering, School of Engineering, Southern Methodist University, Dallas, TX, USA

**Dalit Naor** Department of Computer Science and Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel

**Michele Nappi** Department of Computer Science, University of Salerno, Fisciano, Italy

**Fabio Narducci** Department of Computer Science, University of Salerno, Salerno, Italy

**George Necula** Electrical Engineering and Computer Science, University of California, Berkeley, CA, USA

**Mehmet Ercan Nergiz** Idea Teknoloji Cozumleri, Eclipse Maslak, Istanbul, Turkey

**Alessandro Neri** Department of Applied Electronics, Università degli Studi Roma TRE, Rome, Italy

**Kim Nguyen** Bundesdruckerei GmbH, Berlin, Germany

**Phong Nguyen** Département d'informatique, Ecole normale supérieure, Paris, Cedex 05, France

**Jianting Ning** Fujian Normal University, Fuzhou, China

Singapore Management University, Singapore, Singapore

**Peng Ning** Department of Computer Science, North Carolina State University, Raleigh, NC, USA

**Cristina Nita-Rotaru** Northeastern University, Boston, MA, USA

**Mark S. Nixon** Department of Electronics and Computer Science, University of Southampton, Southampton, UK

**Steven Noel** The MITRE Corporation, McLean, VA, USA

**Marcus Nohlberg** School of Informatics, University of Skövde, Skövde, Sweden

**Arman Noroozian** Delft University of Technology, Delft, The Netherlands

**Aria Nosratinia** The University of Texas at Dallas, Richardson, TX, USA

**Yevheniya Nosyk** University Grenoble Alpes, CNRS, Grenoble INP, LIG, Grenoble, France

- Guevara Noubir** Northeastern University, Boston, MA, USA
- Jason R. C. Nurse** School of Computing, University of Kent, Kent, UK
- Anita Ochiano** Visa International, Foster City, CA, USA
- Tae Oh** School of Informatics, Rochester Institute of Technology, Rochester, NY, USA
- Olga Ohrimenko** The University of Melbourne, Melbourne, VIC, Australia
- Hamed Okhravi** MIT Lincoln Laboratory, Lexington, MA, USA
- Gabriele Oligeri** Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar
- Raphael F. B. Oliveira** The University of Alabama in Huntsville, Huntsville, AL, USA
- Helder C. R. Oliveira** Biometric Technologies Laboratory, Department of Electrical and Software Engineering, University of Calgary, Calgary, AB, Canada
- Melek Önen** EURECOM, Biot Sophia Antipolis, France
- Yossi Oren** Ben Gurion University, Beer Sheva, Israel
- Alessandro Orso** College of Computing – School of Computer Science, Georgia Institute of Technology, Atlanta, GA, USA
- David Ortega del Campo** URJC, Madrid, Spain
- Javier Ortega-Garcia** Universidad Autonoma de Madrid, Madrid, Spain
- Arkadiusz Orłowski** Institute of Physics, Polish Academy of Sciences, Warsaw, Poland
- Department of Informatics, Warsaw, Poland
- Oleksii Osliaik** Consiglio Nazionale delle Ricerche, Rome, Italy
- Akira Otsuka** Research Center for Information Security, National Institute of Advanced Industrial Science and Technology, Tokyo, Japan
- Harald Øverby** NTNU Norwegian University of Science and Technology, Trondheim, Norway
- Christof Paar** Max Planck Institute for Security and Privacy, Bochum, Germany
- Lehrstuhl Embedded Security, Ruhr-Universität Bochum, Bochum, Germany
- Pascal Paillier** CryptoExperts, Paris, France
- Ranjan Pal** Department of EECS, University of Michigan Ann Arbor, Ann Arbor, MI, USA
- Partha Pal** Raytheon BBN, Cambridge, MA, USA

**Giorgos Panagiotakos** Department of Informatics and Telecommunications, National and Kapodistrian University of Athens, Athens, Greece

**Emmanouil Panaousis** School of Computing and Mathematical Sciences, University of Greenwich, London, UK

**Sakshyam Panda** Department of Computer Science, University of Surrey, Guildford, UK

**Pankaj Pandey** Norwegian University of Science and Technology, Gjøvik, Norway

University of Agder, Kristiansand, Norway

**Stephen M. Papa** High Assurance Computing and Networking Labs (HAC-Net), Department of Computer Science and Engineering, Bobby B. Lyle School of Engineering, Southern Methodist University, Houston, TX, USA

**Panos Papadimitratos** Networked Systems Security group, KTH Royal Institute of Technology, Kista, Stockholm, Sweden

**Thanos Papaioannou** Department of Informatics, Ionian University, Corfu, Greece

PDM&FC, Lisbon, Portugal

**Stephen M. Papa MSEE** High Assurance Computing and Networking Labs (HACNet), Department of Computer Science and Engineering, Bobby B. Lyle School of Engineering, Southern Methodist University, Houston, TX, USA

**Nicolas Papernot** University of Toronto and Vector Institute, Toronto, ON, Canada

**Stefano Paraboschi** Dipartimento di Ingegneria Gestionale, dell'Informazione e della Produzione, Università degli Studi di Bergamo, Bergamo, Italy

**Anthony Pardini** Masergy Communications, Inc., Plano, TX, USA

**Federica Pascucci** Engineering Department, Università degli Studi Roma Tre, Roma, Italy

**Ignazio Passero** Department of Computer Science, University of Salerno, Fisciano, Italy

**Jacques Patarin** Versailles St-Quentin-en-Yvelines University, Versailles, France

**Sarvar Patel** Google LLC, Menlo Park, CA, USA

**Malcolm Pattinson** The University of Adelaide, Adelaide, South Australia, Australia

**Bryan D. Payne** Information Systems Analysis, Sandia National Laboratories, Albuquerque, NM, USA

**Torben Pedersen** Cryptomathic, rhus, Denmark

Cryptomathic, Århus, Denmark

**Gerardo Pelosi** Politecnico di Milano, Department of Electronics, Information and Bioengineering – DEIB, Milan, Italy

**Bo Peng** Center for Research on Intelligent Perception and Computing, National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Beijing, People’s Republic of China

**Diego Perino** Telefonica Research, Barcelona, Spain

**Günther Pernul** Department of Information Systems, University of Regensburg, Regensburg, Germany

**Chiara Pero** Department of Computer Science, University of Salerno, Salerno, Italy

**Giuseppe Persiano** Università di Salerno, Salerno, Italy

**Enoch Peserico** Università degli Studi di Padova, Padua, Italy

**Christiane Peters** Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, Eindhoven, The Netherlands

**Jonathan Petit** Qualcomm Technologies Inc., Boxborough, MA, USA

**Christophe Petit** Département d’informatique, Université libre de Bruxelles, Bruxelles, Belgium

School of Computer Science, University of Birmingham, Birmingham, UK

**Fabien A. P. Petitcolas** Smals Research, Brussels, Belgium

**Andy Phippen** Bournemouth University, Bournemouth, UK

**Benny Pinkas** Department of Computer Science, University of Haifa, Haifa, Israel

**João Ribeiro Pinto** INESC TEC and Faculdade de Engenharia da Universidade do Porto, Porto, Portugal

**Vincenzo Piuri** Dipartimento di Information, Università, Degli Studi di Milano, Milano, Italy

**Konstantinos N. Plataniotis** The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON, Canada

**Angelika Plate** AEXIS Security Consultants, Bonn, Germany

**Emanuela Podda** Security, Privacy and Data Protection Laboratory (SPDP Lab), Computer Science Department, Università degli Studi di Milano, Milan, Italy

**Christian Poellabauer** Department of Computer Science and Engineering, University of Notre Dame, Notre Dame, IN, USA

**Norman Poh** Faculty of ICT, University of Malta, MSD, Malta

Trust Stamp, Atlanta, GA, USA

**David Pointcheval** Computer Science Department, Ecole normale supérieure, Paris, France

**Marios M. Polycarpou** KIOS Research and Innovation Center of Excellence and Department of Electrical and Computer Engineering, University of Cyprus, Nicosia, Cyprus

**Michalis Polychronakis** Department of Computer Science, Network Security Lab, Columbia University, New York, NY, USA

**Denis V. Popel** Algorithms Research Corporation, Charlottesville, VA, USA

**Christina Pöpper** Computer Science, New York University Abu Dhabi (NYUAD), Abu Dhabi, United Arab Emirates

**Thomas Poufinas** Department of Economics, Democritus University of Thrace, Komotini, Greece

**Romain Poussier** Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Paris, France

**Bart Preneel** Department of Electrical Engineering-ESAT/COSIC, University of Leuven, Heverlee, Belgium

**Alexander Pretschner** Technical University of Munich, Munich, Germany

**Davy Preuveneers** imec-DistriNet, KU Leuven, Heverlee, Belgium

**Emmanuel Prouff** CNRS, INRIA Laboratoire d'Informatique, Equipe Pol-Sys, Sorbonne Université, Paris Cedex 05, France

**Niels Provos** Google INC, Mountain View, CA, USA

**Baodong Qin** School of Cyberspace Security, Xi'an University of Posts & Telecommunications, Xi'an, P.R. China

**Jean-Jacques Quisquater** ICTEAM, UCLouvain, Louvain-la-Neuve, Belgium

Intel Corporation, Santa Clara, CA, USA

Microelectronics Laboratory, Université catholique de Louvain, Louvain-la-Neuve, Belgium

**Radmilo Racic** Department of Computer Science, University of California, Davis, CA, USA

**Alberto Pedro Ruez Liria** CNP, Madrid, Spain

**Md Moshir Rahman** University of Florida, Gainesville, FL, USA

**Kiran Raja** Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

**Raghavendra Ramachandra** Norwegian University of Science and Technology (NTNU), Gjøvik, Norway

**Ranvir Rana** University of Illinois at Urbana-Champaign, Urbana, IL, USA

**Silvio Ranise** Università di Trento and Fondazione Bruno Kessler, Trento, Italy

**Simone Raponi** Division of Information and Computing Technology, College of Science and Engineering, Hamad Bin Khalifa University, Qatar Foundation, Doha, Qatar

**Awais Rashid** Computer Science, University of Bristol, Bristol, UK

**Christian Rathgeb** Secunet Security Networks AG, Essen, Germany

**Ajita Rattani** Electrical Engineering and Computer Science, Wichita State University, Wichita, KS, USA

**Mohamed Omar Rayes** Department of Computer Science and Engineering, Bobby B. Lyle School of Engineering Southern Methodist University, Dallas, TX, USA

**Francesco Regazzoni** University of Amsterdam, Amsterdam, The Netherlands

Universtità della Svizzera italiana, Lugano, Switzerland

**Delphine Reinhardt** Institute of Computer Science, University of Göttingen, Göttingen, Germany

**Nathan Reitering** Department of Computer Science, University of Maryland, College Park, MD, USA

**Kui Ren** School of Cyber Science and Technology, Zhejiang University, Hangzhou, China

**Ling Ren** University of Illinois at Urbana-Champaign, Urbana, IL, USA

**Karen Renaud** Department of Computer and Information Sciences, University of Strathclyde, Glasgow, UK

Department of Information Systems, Rhodes University, Grahamstown, South Africa

**Moritz Riesner** Department of Information Systems, University of Regensburg, Regensburg, Germany

**Vincent Rijmen** Department of Electrical Engineering/ESAT, Katholieke Universiteit Leuven, Heverlee, Belgium

**Ruben Rios** Network, Information and Computer Security Lab, Universidad de Málaga, Málaga, Spain

ITIS Software, Universidad de Málaga, Málaga, Spain

**Matthieu Rivain** CryptoExperts, Paris, France

**Ronald L. Rivest** Department of Electrical Engineering and Computer Science, Massachusetts Institute of Technology, Cambridge, MA, USA

**Matthew J. B. Robshaw** Orange Labs, Issy Moulineaux, France

**Marco Rosa** SAP Security Research, Mougins, France

**Arnon Rosenthal** The MITRE Corporation, Bedford, MA, USA

**Arun Ross** Department of Computer Science and Engineering, Michigan State University, East Lansing, MI, USA

Department of Computer Science and Electrical Engineering, West Virginia University, Morgantown, WV, USA

**Scott A. Rotondo** Oracle Corporation, Redwood Shores, CA, USA

**Neil C. Rowe** U.S. Naval Postgraduate School, Monterey, CA, USA

**Julian Rrushi** School of Computer Science and Engineering, Oakland University, Rochester Hills, MI, USA

**Juan E. Rubio** Department of Computer Science, University of Malaga, Malaga, Spain

**Jungwoo Ryoo** Division of Business and Engineering, Penn State Altoona, Altoona, PA, USA

**Sayandeep Saha** Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, Kharagpur, India

**Kazuo Sakiyama** The University of Electro-Communications, Tokyo, Japan

**Kazue Sako** Department of Computer Science and Engineering, Waseda University, Tokyo, Japan

NEC, Kawasaki, Japan

**Malek Ben Salem** Department of Computer Science, Columbia University, New York, NY, USA

**Paolo Salvaneschi** Department of Information Technology and Mathematical Methods, University of Bergamo, Dalmine, BG, Italy

**Guido Salvaneschi** University of St. Gallen, St. Gallen, Switzerland

**Pierangela Samarati** Dipartimento di Informatica, Università degli Studi di Milano, Milano, Italy

**David Samyde** Intel Corporation, Santa Clara, CA, USA

**Sudeep Sarkar** Computer Science and Engineering, University of South Florida, Tampa, FL, USA

**Avesta Sasan** George Mason University, Fairfax, VA, USA

**Roberto Sassi** Department of Computer Science, Università degli studi di Milano, Milan, Italy

- Daniel Schlette** Chair of Information Systems, University of Regensburg, Regensburg, Germany
- Bruce Schneier** BT, London, UK
- Berry Schoenmakers** Department of Mathematics and Computer Science, Technische Universiteit Eindhoven, Eindhoven, The Netherlands
- Matthias Schunter** Intel Labs Europe, Munich, Germany
- Jörg Schwenk** Horst Görtz Institute for IT Security, Ruhr University Bochum, Bochum, Germany
- Savio Sciancalepore** Eindhoven University of Technology (TU/e), Eindhoven, The Netherlands
- Edward Sciore** Computer Science Department, Boston College, Chestnut Hill, MA, USA
- Fabio Scotti** Department of Computer Science, Università degli studi di Milano, Milan, Italy
- Nicolas Sendrier** Project-Team SECRET, INRIA Paris-Rocquencourt, Le Chesnay, France
- Basit Shafiq** CIMIC, Rutgers, The State University of New Jersey, Newark, NJ, USA
- Adi Shamir** The Paul and Marlene Borman Professor of Applied Mathematics, Weizmann Institute of Science, Rehovot, Israel
- Shantanu Sharma** Department of Computer Science, New Jersey Institute of Technology, Newark, NJ, USA
- Mohamed Shehab** College of Computing and Informatics, University of North Carolina Charlotte, Charlotte, NC, USA
- Micah Sherr** Department of Computer Science, Georgetown University, Washington, DC, USA
- R. Simon Sherratt** Department of Biomedical Engineering, University of Reading, Reading, UK
- Vlad Shmerko** Biometric Technologies Laboratory, Department of Electrical and Software Engineering, University of Calgary, Calgary, AB, Canada
- Igor Shparlinski** Department of Computing Faculty of Science, Macquarie University, Sydney, Australia
- Robert Silverman** Chelmsford, MA, USA
- Richard T. Simon** Harvard Medical School, Center for Biomedical Informatics, Cambridge, MA, USA
- Greg Sinclair** The Volgenau School of Engineering and IT, Centre for Secure Information Systems, George Mason University, Fairfax, VA, USA

**Gautam Singaraju** The Volgenau School of Engineering and IT, George Mason University Ask.com, Fairfax, VA, USA

**Richa Singh** IIT Jodhpur, Jodhpur, India

**Anoop Singhal** National Institute of Standards and Technology, Gaithersburg, MD, USA

**Radu Sion** National Security Institute, Stony Brook University, Stony Brook, NY, USA

**Jack Smalligan** The Georgia Institute of Technology, Atlanta, Georgia

**Ben Smeets** Department of Information Technology, Lund University, Lund, Sweden

**Matthew Smith** Department of Computer Science, University of Oxford, Oxford, UK

**Alan D. Smith** Department of Marketing, Robert Morris University, Moon Township (Pittsburgh), PA, USA

**Sean W. Smith** Department of Computer Science, Dartmouth College, Hanover, NH, USA

**Dirk Snyman** School of Computer Science and Information Systems, North-West University, Potchefstroom, South Africa

**Agusti Solanas** Universitat Rovira i Virgili, Tarragona, Catalonia, Spain

**Jerome A. Solinas** National Security Agency, Ft Meade, Savage, MD, USA

**Christoph Sommer** TU Dresden, Dresden, Germany

**Claudio Soriente** NEC Labs Europe, Heidelberg, Germany

**Pantelis Sotirelis** School of Production Engineering and Management, Technical University of Crete, Chania, Greece

**Aikaterini Soumelidou** Department of Informatics, Ionian University, Corfu, Greece

**Angelo Spognardi** Computer Science Department, Sapienza University of Rome, Rome, Italy

**Ankur Srivastava** University of Maryland, College Park, MD, USA

**Anurag Srivastava** Department of Applied Information Technology and Centre for Secure Information Systems, The Volgenau School of Engineering, George Mason University, Fairfax, VA, USA

**Mudhakar Srivatsa** IBM Research Division, Thomas J. Watson Research Center, Yorktown Heights, NY, USA

**William Stallings** WilliamStallings.com, Brewster, MA, USA

**François-Xavier Standaert** Microelectronics Laboratory, Université Catholique de Louvain, Louvain-la-Neuve, Belgium

**Angelos Stavrou** Computer Science Department, School Information Technology and Engineering, George Mason University, Fairfax, VA, USA

**Mark Stephens** SMU HACNet Labs, School of Engineering, Southern Methodist University, Nacogdoches, TX, USA

**Anton Stiglic** Instant Logic, Montreal, QC, Canada

**Adrian Stoica** Jet Propulsion Laboratory, California Institute of Technology, Pasadena, CA, USA

**Salvatore J. Stolfo** Department of Computer Science, Columbia University, New York, NY, USA

**Scott D. Stoller** Department of Computer Science, Stony Brook University, Stony Brook, NY, USA

**Martin Strohmeier** Cyber-Defence Campus, armasuisse Science and Technology, Zurich, Switzerland

Department of Computer Science, University of Oxford, Oxford, UK

**Kiruba Sankaran Subramani** The University of Texas at Dallas, Richardson, TX, USA

**Nary Subramanian** Department of Computer Science, The University of Texas at Tyler, Tyler, TX, USA

**Ravichandran Subramanian** Leidos Corporation, Tampa, FL, USA

**Kun Sun** Intelligent Automation, Inc, Rockville, MD, USA

**Berk Sunar** Department Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA, USA

**Laurent Sustek** Inside Secure France, Atmel, France

**Benjamin Tan** Center for Cybersecurity, New York University, New York, NY, USA

**Aimilia Tasidou** Telecom SudParis, Evry, France

**Pietro Tedeschi** Division of Information and Computing Technology (ICT), College of Science and Engineering (CSE), Hamad Bin Khalifa University (HBKU), Doha, Qatar

**Rahul Telang** Carnegie Mellon University, Pittsburgh, PA, USA

**Manolis Terrovitis** Information Management Systems Institute, Athena Research Center, Athens, Greece

**Edlyn Teske** Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON, Canada

**Nicolas Thériault** Universidad de Santiago de Chile, Santiago, Chile

**Emmanuel Thome** INRIA Lorraine Campus Scientifique, Villers-Lès-Nancy Cedex, France

**Kerry-Lynn Thomson** School of IT, Nelson Mandela University, Port Elizabeth, South Africa

**Mitchell A. Thornton** Darwin Deason Institute for Cyber Security, Department of Electrical and Computer Engineering, Lyle School of Engineering Southern Methodist University, Dallas, TX, USA

**Mehdi Tibouchi** Laboratoire d'informatique de l'ENS, École normale supérieure, Paris, France

**Nils Ole Tippenhauer** CISPA Helmholtz Center for Information Security, Saarbrücken, Germany

**Massimo Tistarelli** Computer Vision Laboratory, Department of Sciences and Information Technology, University of Sassari, Alghero, Sassari, Italy

**Genny Tortora** Department of Computer Science, University of Salerno, Fisciano, Italy

**Issa Traoré** Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, Canada

**Assia Tria** CEA-LETI, Grenoble, France

**Alberto Trombetta** Dipartimento di Scienze Teoriche e Applicate, Università degli Studi dell'Insubria, Varese, Italy

**Eran Tromer** Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology, Cambridge, MA, USA

**Aggeliki Tsohou** Department of Informatics, Ionian University, Corfu, Greece

**Michael Tunstall** Rambus Cryptography Research, San Francisco, CA, USA

**Sean Turner** sn3rd, LLC, Washington, DC, USA

**Federico Turrin** Department of Mathematics, University of Padua, Padua, Italy

**Andreas Uhl** Department of Computer Sciences, University of Salzburg, Salzburg, Austria

**Salil Vadhan** School of Engineering & Applied Sciences, Harvard University, Cambridge, MA, USA

**Jaideep Vaidya** Department of Management Science and Information Systems, CIMIC, Rutgers, The State University of New Jersey, Newark, NJ, USA

**Cédric Van Rompay** EURECOM, Biot Sophia Antipolis, France

**Henk C. A. van Tilborg** Department of Mathematics and Computing Science, Eindhoven University of Technology, Eindhoven, The Netherlands

**Peter Van Valkenburgh** Coin Center, Washington, DC, USA

- Mayank Varia** Computer Science and Artificial Intelligence Laboratory (CSAIL), Massachusetts Institute of Technology, Cambridge, MA, USA
- Matteo Varvello** Bell Labs, Nokia, Holmdel, NJ, USA
- Mayank Vatsa** IIT Jodhpur, Jodhpur, India
- Marc Vauclair** BU Identification, Center of Competence Systems Security, NXP Semiconductors, Leuven, Belgium
- Helmut Veith** Institute of Information Systems, Technische Universität Wien, Wien, Austria
- V. N. Venkatakrishnan** Department of Computer Science, University of Illinois at Chicago, Chicago, IL, USA
- Sridhar Venkatesan** Peraton Labs, Bernards, NJ, USA
- Sudip Vhaduri** Department of Computer and Information Science, Fordham University, Bronx, NY, USA
- Christian Viard-Gaudin** Polytech Nantes, Université de Nantes, IRCCyN, Nantes, France
- Marion Videau** Université Henri Poincaré, Nancy 1/LORIA and ANSSI, Paris, France
- Manfred Vielberth** Chair of Information Systems, University of Regensburg, Regensburg, Germany
- João P. Vilela** CISUC, CRACS/INESCTEC and Department of Computer Science, Faculty of Sciences, University of Porto, Porto, Portugal
- Sabrina De Capitani di Vimercati** Dipartimento di Informatica, Università degli Studi di Milano, Milano, Italy
- Pramod Viswanath** Princeton University, Princeton, NJ, USA
- Triet D. Vo-Huu** Northeastern University, Boston, MA, USA
- Nikolaos Vordonis** Department of Economics, Democritus University of Thrace, Komotini, Greece
- Spyros Voulgaris** Athens University of Economics and Business, Athens, Greece
- Isabel Wagner** De Montfort University, Leicester, UK
- Muhammad Waleed** Department of Electronic Systems, Aalborg University, Copenhagen, Denmark
- Dan Wallach** Department of Computer Science, Rice University, Houston, TX, USA
- Colin D. Walter** Information Security Group, Royal Holloway University of London, Surrey, UK
- Nana Wang** Jiangsu Normal University, Xuzhou, China

**Wei Wang** Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing, China

**Jiafan Wang** Department of Information Engineering, Chinese University of Hong Kong, Shatin, Hong Kong

**Lingyu Wang** Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC, Canada

**Xiao Wang** Department of Computer Science, Northwestern University, Evanston, IL, USA

**Xinyue Wang** Rutgers University, Newark, NJ, USA

**Yi Wang** National University of Defense Technology, Changsha, China

**XiaoFeng Wang** School of Informatics and Computing, Indiana University at Bloomington, Bloomington, IN, USA

**Michael Ward** Product Security Chip Centre of Excellence MasterCard Worldwide, Waterloo, Belgium

**Merrill Warkentin** Management & Information Systems, Mississippi State University, Mississippi State, MS, USA

**Nicholas C. Weaver** International Computer Science Institute, Berkeley, CA, USA

**Xiangyu Wei** Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing, China

**André Weimerskirch** Escrypt Inc., Ann Arbor, MI, USA

**Mor Weiss** Bar-Ilan University, Ramat Gan, Israel

**Jian Weng** Jinan University, Guangzhou, China

**William Whyte** Security Innovation, Wilmington, MA, USA

**Michael J. Wiener** Molecular Physiology and Biological Physics, University of Virginia, Charlottesville, VA, USA

**Jeffrey J. Wiley** Department of Computer Science and Engineering, Bobby B. Lyle School of Engineering, Southern Methodist University, Dallas, TX, USA

**Julian Williams** Julian Williams Institute of Hazard Risk and Resilience and the Durham University Business School, University of Durham, Durham, UK

**Tania Williams** The University of Alabama in Huntsville, Huntsville, AL, USA

**William E. Winkler** Statistical Research Division, U.S. Bureau of the Census, Washington, DC, USA

**Bruno Woltzenlogel Paleo** Piracicaba, Brazil

**Brian Wongchaowart** Department of Computer Science, University of Pittsburgh, Pittsburgh, PA, USA

**Damon L. Woodard** Florida Institute for Cybersecurity (FICS) Research, Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA

**Qianhong Wu** School of Cyber Science and Technology, Beihang University, Beijing, China

**Christos Xenakis** Department of Digital Systems, University of Piraeus, Piraeus, Greece

**Shan Xiao** Management & Information Systems, Mississippi State University, Mississippi State, MS, USA

**Xiaokui Xiao** School of Computer Engineering, Nanyang Technological University, Singapore, Singapore

**Daniel Xing** University of Maryland, College Park, MD, USA

**Li Xiong** Emory University, Atlanta, GA, USA

**Wenyuan Xu** College of Electrical Engineering, Zhejiang University, Hangzhou, China

**Asahiko Yamada** Cyber Physical Security Research Center, National Institute of Advanced Industrial Science and Technology, Tokyo, Japan

**Atsushi Yamagishi** IT Security Center, Information-Technology Promotion Agency, Bunkyo-ku, Tokyo, Japan

**Zheng Yan** State Key Laboratory on Integrated Services Networks, School of Cyber Engineering, Xidian University, Xi'an, China

Department of Communications and Networking, Aalto University, Espoo, Finland

**Bo-Yin Yang** Research Fellow, Taipei, Taiwan

**Qiushi Yang** Department of Computer Science, University College London, London, UK

**Xiaowei Yang** Department of Computer Science, Duke University, Durham, NC, USA

**Yang Yang** Singapore Management University, Singapore, Singapore

**Yi Yang** Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA

**Athanasios N. Yannacopoulos** Department of Statistics, Athens University of Economics and Business, Athens, Greece

**Svetlana Yanushkevich** Biometric Technologies Laboratory, Department of Electrical and Software Engineering, University of Calgary, Calgary, AB, Canada

**Svetlana N. Yanushkevich** Department of Electrical and Computer Engineering, Schulich School of Engineering, University of Calgary, Calgary, AB, Canada

**Bulent Yener** Department of Computer Science, Rensselaer Polytechnic Institute, Troy, NY, USA

**Kevin Yeo** Google LLC, Menlo Park, CA, USA

**Xuefei Yin** School of Engineering and Information Technology, University of New South Wales, Canberra, ACT, Australia

**Sachiko Yoshihama** IBM Research-Tokyo, Yamato, Kanagawa, Japan

**Cuilin Yu** Department of Supply Chain and Information Management, Hang Seng University of Hong Kong, Hong Kong, China

**Philip S. Yu** Department of Computer Science, University of Illinois at Chicago, Chicago, IL, USA

**Shucheng Yu** Department of Electrical and Computer Engineering, Stevens Institute of Technology, Hoboken, NJ, USA

**Yu Yu** Shanghai Jiao Tong University, Shanghai, China

**Feng Yue** Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong

School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China

**Moti Yung** Google Inc, New York, NY, USA

Columbia University, New York, NY, USA

**Matthew Zaber** Southern Methodist University, Dallas, TX, USA

**Razieh Nokhbeh Zaeem** Center for Identity, The University of Texas at Austin, Austin, TX, USA

**Yikui Zhai** Department of Intelligent Manufacturing, Wuyi University, Jiangmen, China

**David Zhang** School of Data Science, The Chinese University of Hong Kong, Shenzhen, China

Bio-Computing Research Center, Harbin Institute of Technology, Shenzhen, China

Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong

Shenzhen Institute of Artificial Intelligence and Robotics for Society, Shenzhen, China

**Ning Zhang** Washington University, St. Louis, MO, USA

**Menghuan Zhang** The Hong Kong Polytechnic University, Hong Kong, China

**Wensheng Zhang** Department of Computer Science, College of Liberal Arts and Sciences, Iowa State University Ames, IA, USA

**Yinghui Zhang** School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, P.R. China

School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an, Shaanxi, China

**Zonghua Zhang** IMT Lille Douai, Institut Mines-Télécom, Villeneuve d'Ascq, France

**Yongjun Zhao** Nanyang Technological University, Singapore, Singapore

**Zhen Zhao** School of Cyber Engineering, Xidian University, Xi'an, Shaanxi, China

**Jingxiao Zheng** University of Maryland, College Park, MD, USA

**Jianying Zhou** SUTD, Singapore, Singapore

**Wei Zhou** School of Computer and Information Security, Guilin University of Electronic Technology, Guilin, China

**Sencun Zhu** Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA

**Tianqing Zhu** School of Computer Science, University of Technology Sydney, Sydney, NSW, Australia

**Yanming Zhu** School of Engineering and Information Technology, University of New South Wales, Canberra, ACT, Australia

**Zhichao Zhu** Shape Security, San Francisco Bay Area, CA, USA

**Paul Zimmermann** Team Caramel, Bâtiment A, LORIA/INRIA, Villers-lès-Nancy Cedex, France

**Dionysis Zindros** Stanford University, Stanford, CA, USA

**Robert Zuccherato** Ajax, ON, Canada

**Wangmeng Zuo** Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Hong Kong

School of Computer Science and Technology, Harbin Institute of Technology, Harbin, China

**Mary Ellen Zurko** IBM Software Group Lotus Live Security Architecture and Strategy, Westford, MA, USA

**Michael Zuzak** University of Maryland, College Park, MD, USA