About the Authors of LNCS Volume 6650

2011

Oded Goldreich (`oded@wisdom.weizmann.ac.il`) is a Meyer W. Weisgal Professor at the Faculty of Mathematics and Computer Science of the Weizmann Institute of Science, Israel. Oded was born in 1957, and completed his graduate studies in 1983 under the supervision of Shimon Even. He was a post-doctoral fellow at MIT (1983-86), a faculty member at the Technion (1986-94), a visiting scientist at MIT (1995-98), and a Radcliffe fellow at Harvard (2003/04). Since 1995, he is a member of the Computer Science and Applied Mathematics Department of the Weizmann Institute. He is the author of the books "Modern Cryptography, Probabilistic Proofs and Pseudorandomness" (Springer, 1998), "Computational Complexity: A Conceptual Perspective" (Cambridge University Press, 2008), and the two-volume work "Foundations of Cryptography" (Cambridge University Press, 2001 and 2004).

Lidor Avigad (`avigadl@gmail.com`) works in HP software. He completed his master thesis at the Weizmann Institute of Science in 2009.

Mihir Bellare (`mihir@cs.ucsd.edu`) is a Professor at the Department of Computer Science and Engineering of the University of California San Diego, USA. Mihir got a BS from Caltech in 1986 and a Ph.D from MIT in 1991 under the supervision of Silvio Micali. He was a research staff member at IBM Research in New York from 1991 to 1995. He is a co-designer of the HMAC authentication algorithm (used to secure credit-card numbers in Internet shopping) and the OAEP encryption scheme (used for RSA-based encryption). He has received the 2009 ACM Paris Kanellakis Theory and Practice Award, the 2003 RSA Conference Award in Mathematics, and a 1996 David and Lucille Packard Fellowship in Science and Engineering.

Zvika Brakerski (`zvika.brakerski@weizmann.ac.il`) is currently a PhD student at the Weizmann Institute of Science, Israel.

Shafi Goldwasser (`shafi.goldwasser@gmail.com`) is a Professor at the computer science department of the Weizmann Institute of Science in Israel, and the Electrical Engineering and Computer Science department at MIT. Shafi was born in 1958 in New York city, received her B.S in applied mathematics from Carnegie Mellon University in 1979, and completed her graduate studies in 1983 at the computer science department of UC Berkeley under the supervision of Professor Manuel Blum. She joined the MIT faculty in 1984 and Weizmann faculty in 1994. Her research interests include cryptography, complexity theory, randomized algorithms, and computational number theory She is a member of American Academy of Arts and Science, the US national academy of science and the US national academy of engineering.

Shai Halevi (shaih@alum.mit.edu) is a Research Staff Member in IBM T.J. Watson Research Center. Shai Halevi has a PhD in Computer Science from MIT (1997). His research covers many aspects of cryptography, he is a board member of the International Association for Cryptologic Research and an editor in ACM TISSEC. Shai served as a program chair for CRYPTO 2009, a co-chair for TCC 2006, and as program committee member for many other conferences in cryptography.

Tali Kaufman (kaufmant@mit.edu) is a member of the Computer Science Department of Bar-Ilan university, Israel. She completed her graduate studies in 2006 under the supervision of Noga Alon and Michael Krivelevich and was a post-doc fellow at MIT and IAS (2006-2009) and in the Weizmann Institute (2010).

Leonid Levin (http://www.cs.bu.edu/∼lnd/) is a Professor of computer science at Boston University. He obtained his master degree in 1970 and a Ph.D. equivalent in 1972 at Moscow University, where he studied under Andrey Kolmogorov. After emigration to USA in 1978, he also received a PhD at MIT in 1979.

Noam Nisan (noam.nisan@gmail.com) is a Professor of Computer Science and a member of the Rationality Center at the Hebrew University of Jerusalem and a part-time research scientist in Google, Tel-Aviv. He got his Ph.D. in Computer Science from U.C. Berkeley in 1988. During the last ten years his research has focused on the border of Computer Science, Game theory, and economic theory. Previously he has worked on Computational Complexity, and in particular on Randomness in Computation.

Dana Ron (danar@eng.tau.ac.il) is a Professor at the School of Electrical Engineering in Tel Aviv University, Israel. Dana was born in 1964, and completed her graduate studies in 1995 under the supervision of Naftali Tishby. She was an NSF post-doctoral fellow at MIT (1995-97) and a science scholar at the Bunting Institute, Radcliffe (1997-98). She was also a Radcliffe fellow at Harvard (2003/04). Since 1998 she is a faculty member in Tel Aviv University.

Madhu Sudan (madhu@mit.edu) is a Principal Researcher at Microsoft Research, Cambridge, MA, USA and the Fujitsu Professor of Electrical Engineering and Computer Science at the Massachusetts Institute of Technology. Madhu received his Bachelor's degree in Computer Science from the Indian Institute of Technology in 1987 and his Ph.D. from the University of California at Berkeley, supervised by Umesh Vazirani, in 1992. From 1992 to 1997 he was a Research Staff Member at IBM's Thomas J. Watson Research Center. From 1997 he has been a member of the EECS department at MIT. In 2009 he took a leave of absence to join Microsoft Research at their New England Research Center. Madhu was also Adjunct Associate Professor at the Tata Institute of Fundamental Research in Mumbai, India from 1999 to 2002, and a Radcliffe fellow from 2003-2004. Madhu Sudan's principal interests are in Computational Complexity and Communication. He is best known for his works on Probabilistic Checking of Proofs and List Decoding. His current interests include Property Testing and Semantic Communication.

Luca Trevisan (trevisan@stanford.edu) is a professor of computer science at Stanford University. Luca received his Dottorato (PhD) in 1997, from the Sapienza University of Rome, working with Pierluigi Crescenzi. After graduating, Luca was a post-doc at MIT in 1997-98 and at DIMACS in 1998, he was an assistant professor at Columbia University in 1999-2000, and on the faculty of the University of California, Berkeley, from 2000 to 2010. He joined Stanford University in 2010. Luca received the STOC'97 Danny Lewin (best student paper) award, the 2000 Oberwolfach Prize, and the 2000 Sloan Fellowship. He was an invited speaker at the 2006 International Congress of Mathematicians in Madrid.

Salil Vadhan (`salil@seas.harvard.edu`) is the Vicky Joseph Professor of Computer Science and Applied Mathematics in the Harvard School of Engineering Applied Sciences. Salil was born in 1973, and completed his graduate studies in 1999 at MIT under the supervision of Shafi Goldwasser. He was a postdoctoral fellow at MIT (1999-2000) and the Institute for Advanced Study (2000-01), before joining the Harvard faculty in 2001. He has also been a fellow at the Radcliffe Institute for Advanced Study at Harvard University (2003-04) and a Miller Visiting Professor at UC Berkeley (2007-08). His main research areas are computational complexity and cryptography, with particular interests in zero-knowledge proofs, pseudorandomness, and data privacy.

Avi Wigderson (`avi@ias.edu`) is the Herbert Maass Professor at the School of Mathematics of the Institute for Advanced Study in Princeton. Avi was born in 1956, and completed his graduate studies in 1983 at Princeton University under the supervision of Dick Lipton. After postdoctoral positions at UC Berkeley, IBM labs at San Jose and at MSRI he became a faculty member at the Hebrew University at 1986. In 1999 he moved to the Institute for Advanced Study, where he is leading a program on theoretical computer science and discrete mathematics.

David Zuckerman (`diz@cs.utexas.edu`) holds an Endowed Professorship in the Computer Science Department at the University of Texas at Austin. David was born in 1965, and completed his graduate studies in 1991 under the supersion of Umesh Vazirani. He was an NSF Postdoctoral Fellow at MIT (1991-93), a Lady Davis Postdoctoral at the Hebrew University of Jerusalem (Fall 1993), a Visiting Scholar and Visiting MacKay Lecturer at UC Berkeley (1999-2000), and a Guggenheim Fellow and Radcliffe Fellow at Harvard (2004-05). Since 1994, he has been on the faculty of the Computer Science Department at the University of Texas at Austin. His research awards include a Guggenheim Fellowship, a David and Lucile Packard Fellowship for Science and Engineering, an Alfred P. Sloan Research Fellowship, and an NSF CAREER Award.