Authors' Biographies

Çetin Kaya Koç

Çetin Kaya Koç received his Ph.D. in Electrical and Computer Engineering from University of California Santa Barbara in 1988. He was an assistant professor at University of Houston (1988–1992) and assistant, associate and full professor at Oregon State University (1992–2007). He established Information Security Laboratory at OSU and guided 14 Ph.D. students, 8 of who are currently professors. In September 2001, he received Oregon State University Research Award for outstanding and sustained research leadership.

His research interests are in algorithms and architectures for cryptography, computer arithmetic and embedded systems. He has co-founded *Workshop on Cryptographic Hardware and Embedded Systems* (chesworkshop.org) in 1999 and has been the program chair and proceedings editor from 1999 to 2003. He is now a permanent member of the steering committee of CHES. Recently, he has also co-founded a new conference, *International Workshop on the Arithmetic of Finite Fields* (waifi.org), which is a forum of engineers and mathematicians interested in efficient software and hardware realizations of finite fields. He has co-authored one book, *Cryptographic Algorithms on Reconfigurable Hardware*, published by Springer. He has been an associate editor of *IEEE Transactions on Computers* and *IEEE Transactions on Mobile Computing* and guest co-editor of two issues (April 2003 and November 2008) of *IEEE Transactions on Computers* on cryptographic and cryptanalytic hardware and embedded systems. Dr. Koç published more than 120 journal, conference and book articles, 7 US patents, and edited 5 books. He is an *IEEE Fellow* since 2007 *for contributions to cryptographic engineering*.

Dr. Koç is currently with City University of Istanbul and University of California Santa Barbara.

Onur Acıiçmez

Onur Acıiçmez holds a Ph.D. in Electrical Engineering and Computer Science from Oregon State University. During his Ph.D. research, he discovered several microarchitectural attacks, a number of security weaknesses in widely used cryptographic software, and participated in strengthening these systems against microarchitectural cryptanalysis. He received his B.S. degree in Computer Engineering and Information Science in July 2002 from Bilkent University in Ankara, Turkey, where he has received several awards and distinctions. He completed his Master's study focusing on high performance implementations of cryptographic algorithms in Electrical and Computer Engineering in May 2004 at Oregon State University. He has authored and co-authored 22 patent applications and several papers on side-channel analysis, microarchitectural cryptanalysis, and trusted computing. He is currently working on trusted computing as a research scientist at Samsung Information Systems America, an R&D center of Samsung Electronics.

Sandro Bartolini

Sandro Bartolini is an assistant professor at the Department of Information Engineering, University of Siena, Italy. He received his Ph.D. in Computer Engineering from the University of Pisa, Italy. He took part in various research and industrial projects on the following topics, which constitute his main research interests: embedded systems, cache and memory subsystems, compiler optimizations, link/post-link profile-driven tuning of applications, low-power techniques, advanced computer architecture, and special hardware for security and cryptography. He is a member of the European HiPEAC (High Performance and Embedded Architecture and Compilation) network of excellence and is currently working in the SARC FP6 integrated project on "scalable computer architecture". Dr. Bartolini is associate editor of the *EURASIP Journal on Embedded Systems* and was guest editor of *ACM Computer Architecture News* and of the *Journal of Embedded Computing*. He is coorganizer of the MEDEA International Workshop since 2002. He is a member of IEEE, IEEE Computer Society, and ACM.

Nigel Boston

Nigel Boston grew up in England and attended Cambridge and Harvard. His postdoctoral work in Paris and Berkeley was followed by 12 years at the University of Illinois, except for 6 months as Rosenbaum Fellow at the Newton Institute in Cambridge, UK, when he witnessed Wiles's announcement of a proof of Fermat's last theorem. In recent years he has moved toward engineering, becoming founding director of the Illinois Center for Cryptography and Information Protection. In 2002, he was hired by the University of Wisconsin-Madison as part of the computational sciences cluster, with joint appointments in Mathematics and Electrical and

Computer Engineering. In 2006–2007 he was Williams-Hedberg-Hedberg chair at the University of South Carolina. Beginning in September 2008 he will be Stokes professor of pure and applied algebra at University College Dublin, Ireland.

Debrup Chakraborty

Debrup Chakraborty received Bachelor of Mechanical Engineering degree from Jadavpur University, Kolkata, India, in 1997. He obtained M.Tech. and Ph.D. degrees in Computer Science from Indian Statistical Institute, Kolkata, India, in 1999 and 2005, respectively. Currently he is a postdoctoral researcher in the Computer Science Department of Centro de Investigaciones y Estudios Avanzados del IPN, Mexico City, Mexico. Dr. Chakraborty's current research interests include design and analysis of provably secure symmetric encryption schemes, efficient software/hardware implementations of cryptographic primitives, and pattern recognition.

Pawel Chodowiec

Pawel Chodowiec received the B.Sc. degree in Telecommunications from Warsaw University of Technology in Warsaw, Poland, and the M.Sc. degree in Electrical and Computer Engineering from George Mason University in Fairfax, VA, USA. During his research at George Mason University he cooperated with Dr. Kris Gaj on development of novel hardware implementations for cryptographic algorithms with emphasis on block ciphers. Currently he works at Mantaro Networks, Inc., as an FPGA engineer and consultant with specialization in high-speed network and security applications.

Matthew Darnall

Matthew Darnall is a Ph.D. student in Mathematics at the University of Wisconsin – Madison. He received his B.A. in Mathematics at Humboldt State University in Arcata, CA. His research interests are cryptography, number theory, and irregularities of distribution.

Serdar Süer Erdem

Serdar Süer Erdem received the B.S. degree from Boğaziçi University, Istanbul, Turkey, in 1992, the M.S. degree from the Pennsylvania State University in 1996, and the Ph.D. degree from the Oregon State University in 2002, all in Electrical and Computer Engineering. Currently, he is an assistant professor at the Electronics Engineering Department of Gebze Institute of Technology in Kocaeli, Turkey. His

research interests include computer arithmetic, cryptography and network security, embedded systems.

Kris Gaj

Kris Gaj received the M.Sc. and Ph.D. degrees in Electrical Engineering from Warsaw University of Technology in Warsaw, Poland. He was a founder of Enigma, a Polish company that generates practical software and hardware cryptographic applications used by major Polish banks. In 1998, he joined George Mason University, where he currently works as an associate professor, doing research and teaching courses in the area of cryptographic engineering and reconfigurable computing. His research projects center on novel hardware architectures for secret key ciphers, hash functions, public key cryptosystems, and factoring, as well as development of specialized libraries and application kernels for high-performance reconfigurable computers. He has been a member of the Program Committees of CHES, CryptArchi, and Quo Vadis Cryptology workshops, and a General Co-Chair of CHES 2008 in Washington, D.C. He is an author of a book on breaking German Enigma cipher used during World War II.

Roberto Giorgi

Roberto Giorgi is an associate professor at Department of Information Engineering, University of Siena, Italy. He was research associate at the University of Alabama in Huntsville, USA. He received his Ph.D. in Computer Engineering and his Master's in Electronics Engineering, magna cum laude both from University of Pisa, Italy. He is participating in the European projects HiPEAC (High Performance Embedded-system Architecture and Compiler) and SARC (Scalable ARChitectures) in the area of future and emerging technologies. He took part in ChARM project, developing software for performance evaluation of ARM processor-based embedded systems with cache memory, for VLSI Technologies Inc., San Jose. His current interests include computer architecture themes such as embedded systems, multiprocessors, memory system performance, workload characterization. He has been selected by the European Commission as an independent expert for evaluating the European project SHAPES (Scalable Software Hardware Architecture Platform for Embedded Systems). He is a member of ACM and a senior member of the IEEE, IEEE Computer Society.

Marc Joye

Marc Joye received his Ph.D. degree in applied sciences (cryptography) from the Université Catholique de Louvain, Belgium, in 1997. In 1998 and 1999, he was a postdoctoral fellow of the National Science Council, Republic of China. From 1999

to 2006, he was with the Card Security Group, Gemplus (now Gemalto), France. Since August 2006, he has been with the Security Laboratories, Thomson R&D, France. His research interests include cryptography, computer security, computational number theory, and smart card implementations. He is author and co-author of more than 80 scientific papers and holds several patents. He served in numerous program committees and was program chair for CT-RSA 2003, CHES 2004, and ACM-DRM 2008. He is a member of the IACR and co-founder of the UCL Crypto Group.

Enrico Martinelli

Formerly with the Italian National Research Council as a researcher at the Istituto di Elaborazione dell'Informazione, Pisa, presently Enrico Martinelli is a full professor of the University of Siena, where he teaches courses on logic design and information security and is the head of the Department of Information Engineering. His main research interests are focused on logic design of high performance digital structures for special applications as digital signal processing and cryptography.

Francisco Rodríguez-Hénriquez

Francisco Rodríguez-Hénriquez received his bachelor's degree in Electrical Engineering from the University of Puebla, Mexico, in 1988. He obtained M.Sc. degree in Electrical and Computer Engineering from the National Institute of Astrophysics, Optics and Electronics (INAOE), Mexico, in 1992 and he received Ph.D. degree in Electrical and Computer Engineering, Department of Oregon State University in 2000. Currently, he is an associate professor (CINVESTAV-3B researcher) at the Computer Science Department of CINVESTAV-IPN, in Mexico City, Mexico, which he joined in 2002. Dr. Rodríguez-Hénriquez's major research interests are in cryptography, finite field arithmetic, and hardware implementation of cryptographic algorithms.

Pankaj Rohatgi

Pankaj Rohatgi is a research staff member and the manager of the Internet Security Group at IBM's TJ Watson Research Center. He received a B.Tech degree in Computer Science and Engineering from IIT Delhi in 1988 and a Ph.D. in Computer Science from Cornell University in 1994. From 1993 to 1996 he worked at Thomson R&D Labs and at the Sun-Thomson Interactive Alliance as a security architect for the OpenTV operating system. In 1996, he joined the IBM TJ Watson

Research Center where he has contributed to products such as the IBM System S, the IBM 4758 crypto co-processor, and conducted research in the areas of applied cryptography, side-channel cryptanalysis, network and systems security, security for embedded systems, and security risk management. He has published over 35 scientific articles and holds 11 patents. He has given numerous invited talks in the area of side-channel cryptanalysis. He is currently serving as the program co-chair of the 2008 Workshop on Cryptographic Hardware and Embedded Systems (CHES).

Gökay Saldamlı

Gökay Saldamlı received his B.S. and M.Sc. degrees from the Mathematics Department of Middle East Technical University, Ankara, Turkey, in 1996 and 2000, respectively. He completed his Ph.D. degree in Electrical and Computer Engineering at Oregon State University in June 2005. He worked 2 years at Samsung Electronics, Giheung, South Korea, as a senior engineer. Currently, he is working at Eczacıbaşı Embedded Design Center, in Istanbul, Turkey, and leading various projects related to cryptography and information security. His research interests include cryptographic engineering, public-key cryptography, low-power cryptography, and computer arithmetic. He is a member of the IEEE Computer Society and the International Association of Cryptologic Research (IACR).

Erkay Savaş

Erkay Savaş received the B.S. (1990) and M.S. (1994) degrees in Electrical Engineering from the Electronics and Communications Engineering Department at Istanbul Technical University. He completed the Ph.D. degree in the Department of Electrical and Computer Engineering at Oregon State University in June 2000. He worked for various companies and research institutions before joining Sabanci University as an assistant professor in 2002. He is the director of the Cryptography and Information Security Group (CISec) of Sabanci University. His research interests include cryptography, data and communication security, privacy in biometrics, trusted computing, security and privacy in data mining applications, embedded systems security, and distributed systems. He is a member of IEEE, ACM, the IEEE Computer Society, and the International Association of Cryptologic Research (IACR).

Werner Schindler

Werner Schindler received his Diploma in Mathematics in 1989, his Ph.D. in Mathematics (Dr. rer. nat.) in 1991, and his postdoctoral lecture qualification (Habilitation) in 1998, all at Darmstadt University of Technology, Germany. Since 1993, he has been working as a federal civil servant at Bundesamt für Sicherheit in der Informationstechnik (BSI) in Bonn, Germany. He is also an adjunct professor of

mathematics (außerplanmäßiger professor) at Darmstadt University of Technology since 2005. His main fields of expertise are cryptographic algorithms and protocols, side-channel attacks on smart cards and software implementations, random number generators for cryptographic applications, electronic payment systems, stochastic simulations, measure and integration theory.

François-Xavier Standaert

François-Xavier Standaert was born in Brussels, Belgium, in 1978. He received the Electrical Engineering degree and Ph.D. degree from the Université Catholique de Louvain, respectively, in June 2001 and June 2004. In 2004–2005, he was a Fulbright visiting researcher at Columbia University, Department of Computer Science, Network Security Lab (September 04 to February 05), and at the MIT Medialab, Center for Bits and Atoms (February 05 to July 05). In March 2006, he was a founding member of IntoPIX s.a. He is now a postdoctoral researcher of the Belgian Fund for Scientific Research (FNSR) at the UCL Crypto Group. His research interest includes digital electronics and FPGAs, cryptographic hardware, design of symmetric cryptographic primitives, physical security issues, and side-channel analysis.

Berk Sunar

Berk Sunar received his B.Sc. degree in Electrical and Electronics Engineering from Middle East Technical University in 1995 and his Ph.D. degree in Electrical and Computer Engineering (ECE) from Oregon State University in December 1998. After briefly working as a member of the research faculty at Oregon State University, Sunar has joined Worcester Polytechnic Institute as an assistant professor. Since July 2006, he is serving as an associate professor. He is currently heading the Cryptography and Information Security Laboratory (CRIS). Sunar received the National Science Foundation CAREER award in 2002. He served as the co-editor of Cryptographic Hardware and Embedded Systems Workshop (CHES) 2005 and International Workshop on the Arithmetic of Finite Fields (WAIFI) 2007. His research interests include lightweight and tamper-resilient cryptography. Sunar is a member of the IEEE Computer Society, the ACM, and the International Association of Cryptologic Research (IACR) professional societies.

Colin Walter

Colin Walter is a senior member of the IEEE, a member of the IACR CHES steering committee, and head of cryptography at Comodo, one of the main certificate

authorities. He obtained his doctorate in algebraic number theory from Cambridge University and worked in academia prior to his current post. He helped design several cryptographic ASICs in the late 1980s. From this stemmed a series of papers on hardware arithmetic, particularly on Montgomery modular multiplication. Amongst these is the earliest design for a fully systolic modular multiplier with purely local connections. In the latter 1990s he was a consultant working on the Mondex purse to defeat timing and power attacks. This led to a number of papers on side-channel attacks, many of which assume standard blinding techniques and showing, paradoxically, that longer keys may be cryptographically weaker. His proposals for counter-measures include a randomized exponentiation algorithm.

Tuğrul Yanık

Tuğrul Yanık received a B.S. in Computer Engineering from the Aegean University in Izmir, Turkey, in 1996, an M.Sc. in Computer Science and Engineering from the Oregon Graduate Institute of Science and Technology in 1999, and a Ph.D. degree from the Oregon State University in 2002. He worked for 4 years as a software engineer at Mentor Graphics Corp. Currently he is an assistant professor at the Computer Engineering Department of Fatih University in Istanbul, Turkey. His research interests include computer arithmetic, cryptography, and network security focusing on VOIP security and security protocols. He is a member of IEEE.

Index