Guest Editors' Introduction to the Special Section on Cryptographic Hardware and Embedded Systems

Çetin K. Koç, *Senior Member*, *IEEE*, and Christof Paar, *Member*, *IEEE*

1 Introduction

Cryptography provides the necessary tools for accomplishing private and authenticated communication and for performing secure and authenticated transactions over the Internet as well as other open networks. It is highly probable that every single bit of information flowing through our networks will have to be either encrypted or signed and authenticated in a few years from now. This is not to imagine the world of Big Brother, but rather, carrying over the required, legal, and contractual certainty from our paper-based offices to our virtual offices existing in cyberspace. In such an environment, server and client computers, as well as handheld, portable, and wireless devices, will have to be capable of encrypting or decrypting and signing or verifying messages. That is to say, without exception, all computers and devices must have cryptographic layers implemented and must be able to access cryptographic functions. In this context, efficient (in terms of time, area, and power consumption) hardware structures will have to be designed, implemented, and deployed. Furthermore, general-purpose (platform-independent) as well as special-purpose software implementing cryptographic functions on embedded devices are needed. An additional challenge is that these implementations should be done in such a way as to resist cryptanalytic attacks launched against them by adversaries having access to primary (communication) and secondary (power, energy, electromagnetic) channels.

This special section of the *IEEE Transactions on Computers* arrives at an appropriate time to inform the readers about this growing area of technical challenges and opportunities. We announced this special issue early in 2001 with a paper deadline of 15 May 2002. Later, this deadline was extended one month. We received the first submission on 2 February 2002 and, by the deadline, we had 68 submissions. We had space for only 10 papers in this special section; therefore, many good quality papers had to be rejected. We have informed these authors and urged them to send their papers to a *regular* issue of this journal, with sincere apologies.

- *Ç.K. Koç is with the Information Security Laboratory, Department of Electrical and Computer Engineering, Oregon State University, Corvallis, OR 97331. E-mail: koc@ece.orst.edu.*
- *C. Paar is with the Lehrstuhll Kommunikationssicherheit, Ruhr-Universitaet Bochum, Universitaetsstrasse 150, 44780 Bochum, Germany. E-mail: cpaar@crypto.ruhu-uni-bochum.de.*

For information on obtaining reprints of this article, please send e-mail to: tc@computer.org, and reference IEEECS Log Number 117875.

The call for papers for the special section announced 10 key areas in which we have sought papers; these were

- computer architectures for secret-key and public-key cryptography,
- reconfigurable computing and applications in cryptography,
- cryptographic processors and coprocessors,
- modular and Galois field arithmetic architectures,
- tamper resistance on chip and board level,
- smart card attacks and architectures,
- efficient algorithms for embedded processors,
- special-purpose hardware for cryptanalysis,
- true and pseudorandom number generators,
- cryptography in wireless applications.

We accepted one paper on true/pseudorandom number generators, which is the first paper in this issue, written by M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanouovo.

The second paper is by P. Sarkar and S. Maitra and shows how to implement large Boolean functions, which has its applications in both secret-key and public-key cryptography.

The remaining four papers are in the general area of algorithms and computer architectures for public-key cryptography. They address issues such as low-complexity finite field multiplications (the paper by R. Katti and J. Brennan and the paper by A. Reyhani-Masoleh and M.A. Hasan). On the other hand, the paper by C. O'Rourke and B. Sunar addresses NTRU implementations using Montgomery multiplication and the paper by A. Satoh and K. Takano describes a scalable, dual-field (unified) elliptic curve cryptographic processor.

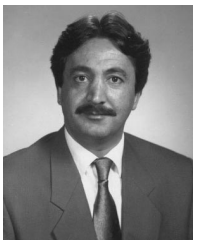
Another issue in the design of algorithm and architectures for cryptography is to come up with designs which are immune to (or resistant against) certain attacks, for example, power attacks, side-channel attacks, or hardware fault attacks. The paper by S.-M. Yen, S. Kim, S. Lim, and S. Moon addresses RSA implementations using the CRT against hardware fault attacks.

Finally, we have three papers on secret-key cryptographic algorithms. The first one is by G. Rouvroy, F.-X. Standaert, J.-J. Quisquater, and J.-D. Legat which discusses the uses of FPGAs on DES implementations. The remaining two papers describe AES (Advanced Encryption Standard) implementations, the first one of which is a

regular and scalable implementation of AES by S. Mangard, M. Aigner, and S. Dominikus. The second paper, i.e., the last paper of the special section, is by G. Bertoni, L. Breveglieri, I. Koren, P. Maistri, and V. Piuri, which describes error analysis and detection procedures for hardware implementations of AES.

The guest editors thank the office of the IEEE Computer Society, the reviewers from all over the world, and also the authors for giving us an opportunity to introduce a synopsis of work on cryptographic hardware and embedded system design to the scientific and engineering community.

Çetin K. Koç
Christof Paar
Guest Editors



Çetin K. Koç received the PhD (1988) and MS (1985) degrees in electrical and computer engineering from the University of California at Santa Barbara and the MS (1982) and BS (1980, summa cum laude) degrees in electrical engineering from Istanbul Technical University. He is a full professor in the Department of Electrical and Computer Engineering at Oregon State University, which he joined in 1992. He is the founder and director of the Information Security Laboratory at Oregon State University. In 2001, he received the OSU College of Engineering Research Award for Outstanding and Sustained Research Leadership. Between 1988 and 1992, he was on the faculty of the University of Houston. Professor Koç's research interests are in security, cryptography, computer arithmetic, finite fields, and high-speed computing. He is the cofounder (together with Christof Paar) of the Workshop on Cryptographic Hardware and Embedded Systems (CHES). He is an associate editor of the *IEEE Transactions on Mobile Computing*. He has been working as a consulting engineer with research and development interests in cryptography and high-speed computing in constrained environments for several organizations and companies, including Intel and RSA Security. He is a senior member of the IEEE and a member of the IEEE Computer Society, IEEE Information Theory Society, and International Association for Cryptologic Research (IACR).

Christof Paar received his first degrees in electrical engineering from the Fachhochschule of Cologne and the University of Siegen, Germany, in 1988 and 1991, respectively. In 1994, he received the PhD degree in engineering from the Institute for Experimental Mathematics at the University of Essen, Germany. From 1995-2001, he was first an assistant and later an associate professor in the Electrical and Computer Engineering Department at Worcester Polytechnic Institute (WPI). At WPI, he headed the Cryptography and Informations Security Group and received a US National Science Foundation CAREER award for investigating cryptographic algorithms on FPGAs. Since 2001, he has held an endowed chair for communication security at the University of Bochum, Germany. He is one of the two founding members of the EUROBITS Center of Excellence for IT Security in Bochum. In 1999, he cofounded, together with Çetin Koç, the Cryptographic Hardware and Embedded Systems (CHES) Workshop series. His research interests include computer architectures for asymmetric and symmetric ciphers, reconfigurable hardware, side channel attacks, and security in ad hoc networks. He is a member of the IEEE, ACM, and IACR.