Guest Editors' Introduction to the Special Section on Special-Purpose Hardware for Cryptography and Cryptanalysis

Rainer Steinwandt, Willi Geiselmann, and Çetin Kaya Koç, *Fellow*, *IEEE*

DESIGNING and implementing cryptographic schemes in such a way that both security and efficiency needs are met is a notoriously challenging task. To cope with specific requirements of lightweight platforms or high-speed applications, special-purpose hardware has turned out to be an indispensable tool for designers and implementors of cryptographic systems. In addition, the sheer need to defend against threats on the implementation level motivates the use of nonstandard components: To counter cryptanalytic attacks building on the induction of faults or information obtained from side channels, algorithmic countermeasures are combined with the use of special-purpose hardware.

However, special-purpose hardware is of importance not only in building cryptographic systems: There are an increasing number of proposals for cryptanalytic attacks that make substantial use of nonstandard hardware. Attacks on both symmetric and asymmetric cryptographic schemes are explored here and the spectrum of cryptanalytic proposals ranges from architectures to speed up exhaustive key searches to designs that support algorithms for factoring large integers. While, for some of these proposals, no successful implementations have been reported, others have been implemented and tested successfully.

With this special section, we try to give an impression of recent advances in this research topic at the interface of computer science, mathematics, and electrical engineering. With the limited number of papers that can be fit into the space of this special section, we certainly cannot do justice to all aspects of special-purpose hardware in cryptography and cryptanalysis, but we hope that the subsequent pages help in getting an idea of the diverse and fascinating work that is being done in this area of research. In the call for papers for this special section, we encouraged submissions on all aspects of special-purpose hardware in cryptography and cryptanalyis, including

- cryptographic and cryptanalytic algorithms building on the use of unconventional architectures,
- design techniques and evaluation methodologies for architectures with cryptographic or cryptanalytic significance,
- fault tolerance in cryptographically or cryptanalytically relevant architectures, and
- integration of hardware and software for cryptographic or cryptanalytic applications.

In response to this call for papers, we received 47 submissions, each of which was evaluated by at least three reviewers. Eventually, eight manuscripts were selected to form this special section of the *IEEE Transactions on Computers*.

The (in alphabetic order of the authors) first paper, by Bijan Ansari and M. Anwar Hasan, reports on a "High-Performance Architecture of Elliptic Curve Scalar Multiplication" for finite fields in characteristic two, including a discussion of a specialized architecture for scalar multiplication. Another aspect of elliptic curves, more specifically of pairing-based cryptography, is addressed by Jean-Luc Beuchat, Nicolas Brisebarre, Jérémie Detrey, Eiji Okamoto, Masaaki Shirase, and Tsuyoshi Takagi. Their contribution, "Algorithms and Arithmetic Operators for Computing the η_T Pairing in Characteristic Three," reports on an efficient hardware implementation of a pairing computation. Another contribution drawing its tools from several scientific disciplines is "Provably Sublinear Point Multiplication on Koblitz Curves and Its Hardware Implementation" by Vassil S. Dimitrov, Kimmo U. Järvinen, Michael J. Jacobson Jr., Wai Fong Chan, and Zhun Huang. This paper integrates a number of different techniques with the aim of an efficient hardware implementation of elliptic curve arithmetic.

Sylvain Guilley, Laurent Sauvage, Philippe Hoogvorst, Renaud Pacalet, Guido Bertoni, and Sumanta Chaudhuri's paper on "Security Evaluation of WDDL and SecLib Countermeasures against Power Attacks" explores countermeasures at the logical and physical level to defend against side channel attacks. The paper reports on two power-constant logic styles and considers several different side-channel attacks. The work of Tim Güneysu, Timo Kasper, Martin Novotný, Christof Paar, and Andy Rupp, "Cryptanalysis with COPACOBANA," belongs to the cryptanalyic part of the spectrum of this special section. Their paper describes a parallel FPGA cluster that is optimized for cryptanalytic applications and this contribution gives an

- *R. Steinwandt is with the Department of Mathematical Sciences, Florida Atlantic University, Boca Raton, FL 33431. E-mail: rsteinwa@fau.edu.*
- *W. Geiselmann is with the Institut für Algorithmen und Kognitive Systeme, Universität Karlsruhe, 76131 Karlsruhe, Germany. E-mail: geiselma@ira.uka.de.*
- *Ç.K. Koç is with City University of Istanbul and the Department of Computer Science and the College of Creative Studies, University of California Santa Barbara, Santa Barbara, CA 93106. E-mail: koc@cryptocode.net.*

For information on obtaining reprints of this article, please send e-mail to: tc@computer.org.

idea of the current state-of-the-art in attacking cryptographic schemes by means of a special-purpose architecture.

The use of elliptic curve cryptography in a setting with rather strict efficiency constraints is discussed by Yong Ki Lee, Kazuo Sakiyama, Lejla Batina, and Ingrid Verbauwhede. Their paper, "Elliptic-Curve-Based Security Processor for RFID," looks at the implementation of public key cryptography on a platform with very limited resources. The problem of defending against fault induction attacks is addressed by the contribution of Paolo Maistri and Régis Leveugle. Their paper, "Double-Data-Rate Computation as a Countermeasure against Fault Analysis," discusses several types of fault attacks, including faults with a duration of more than just one clock cycle. The problem of defending against differential power analysis is addressed by Radu Muresan and Stefano Gregori. In their paper, "Protection Circuit against Differential Power Analysis Attacks for Smart Cards," a current flattening technique is explored that aims at improving the protection of smart cards.

In the end, less than 20 percent of the submissions could be included in the limited space available for this special section and we would like to express our sincere gratitude to all of the authors who submitted their work to this special section—independent of whether the paper could be accepted or not. We would also like to thank the anonymous reviewers for their invaluable help in evaluating and judging the submissions. Further on, it is our pleasure to thank Fabrizio Lombardi and Joyce Arnold for their continuous help and support with all our organizational questions in connection with this special section.

Rainer Steinwandt
Willi Geiselmann
Çetin Kaya Koç
Guest Editors

Rainer Steinwandt received the Dipl.-Inform. (1998) and Dr. rer. nat. (2000) degrees from the Fakultät für Informatik, Universität Karlsruhe, Germany. He is a professor in the Department of Mathematical Sciences at Florida Atlantic University and serves as associate director of the Center for Cryptology and Information Security at Florida Atlantic University.

Willi Geiselmann received the Dipl.-Math. degree from the Fakultät für Mathematik, Universität Konstanz, Germany, in 1987 and the Dr. rer. nat. degree from the Fakultät für Informatik, Universität Karlsruhe, Germany, in 1993. He is now with the Institut für Algorithmen und Kognitive Systeme, Fakultät für Informatik, Universität Karlsruhe, Germany. His main research interests are in algorithm engineering and cryptography.

Çetin Kaya Koç received the PhD degree in 1988 in electrical and computer engineering from the University of California, Santa Barbara. He worked as an assistant professor at the University of Houston (1988-1992) and as an assistant, associate, and full professor at Oregon State University (1992-2007). In 2001, he received an Award for Outstanding and Sustained Research Leadership at Oregon State University. Currently, he is with City University of Istanbul and the University of California, Santa Barbara. His research interests are in cryptographic engineering, information security, embedded systems, and computer arithmetic. He is a cofounder of the CHES (Cryptographic Hardware and Embedded Systems) and WAIFI (Arithmetic of Finite Fields) Workshops and served as a steering committee member, program chair, and publicity chair. He has been an associate editor and guest coeditor of the *IEEE Transactions on Computers* and *IEEE Transactions on Mobile Computing*. He has coauthored two books, *Cryptographic Algorithms in Reconfigurable Hardware*, published in 2007, and *Cryptographic Engineering*, to be published in 2008, both by Springer, coedited six CHES and WAIFI workshop proceedings (published in *Lecture Notes in Computer Science* by Springer). He has published 11 US patents (six issued and five pending) and more than 150 journal, conference, and book articles. In 2007, he was elected as an IEEE fellow with the citation "for contributions to cryptographic engineering."