Guest Editors' Introduction: Special Section on Fault Diagnosis and Tolerance in Cryptography

Luca Breveglieri and Israel Koren, *Fellow*, *IEEE*

VARIOUS information technology disciplines such as telecommunication, networking, data base systems, and mobile applications have developed increasingly strict security requirements over the years, leading to a surge of research and development activity in the field of applied cryptography.

Crypto-systems are inherently computationally complex: In order to satisfy the high throughput requirements of many applications, they are often implemented by means of either VLSI devices or highly optimized software routines. The high complexity of such implementations makes reliability a challenge. Moreover, attacks on crypto-systems based on malicious injection of faults (for the purpose of extracting the secret key) have unfortunately proven to be very successful, making their own security another challenge. New methodologies are therefore needed in designing robust cryptographic systems, both hardware and software, in order to protect them against both accidental and malicious faults.

The objective of this special section is to present some of the state-of-the-art developments in the analysis of fault attacks and the techniques to protect crypto-systems from such attacks. The papers included in this special section were selected from 12 manuscripts submitted in response to the call for papers. Submissions were also solicited from the authors of papers presented at the Workshop on Fault Diagnosis and Tolerance in Cryptography (FDTC '04), held in Florence, Italy, in June 2004. This workshop has, since then, become an annual meeting with FDTC '05 in Edinburgh, UK, in September 2005 and the next one, FDTC '06, to be held in Yokohama, Japan on 10 October 2006 (http://www.elet.polimi.it/conferences/FDTC06/).

As a result of the review process, five papers were selected to be included in this special section. Two of these papers are extensions of papers presented at FDTC '04 and the rest have originated from the open call for papers.

The first paper in this special section, "A Fault Attack on Pairing-Based Cryptography" by D. Page and F. Vercauteren, deals with Tate pairing, a new cryptographic primitive that allows the design of public-key systems that do not use certificates, a desirable characteristic for mobile systems. The authors analyze the mathematical foundation of Tate pairing algorithms, identify the vulnerabilities of these algorithms to fault attacks and propose some countermeasures. This paper demonstrates the mathematical complexity of studying fault attacks on cryptographic systems.

The second paper, "Combining Crypto with Biometrics Effectively" by F. Hao, R. Anderson, and J. Daugman, does not deal with malicious faults, but, instead, with the unavoidable errors due to the measurement procedure for an iris scan. The authors combine error diagnosis and correction techniques with cryptography in order to be able to derive a key from given biometric data. The paper also discusses the technological difficulties one faces when implementing the proposed technique in a secure way.

The third paper, "Fault Detection Architectures for Field Multiplication Using Polynomial Bases" by A. Reyhani-Masoleh and M.A. Hasan, focuses on one of the basic building blocks of most cryptographic devices: the finite field multiplier. The authors describe techniques based on error detecting codes for detecting faults in these frequently used circuits.

The fourth paper, "Designing Resistant Circuits against Malicious Faults Injection Using Asynchronous Logic" by Y. Monnet, M. Renaudin, and R. Leveugle, deals with circuit techniques that are available for protection against fault injection-based attacks, namely, the use of dual-rail logic. This is an alternative to implementing countermeasures at a higher, algorithmic level. The authors present methods for analyzing the sensitivity to faults of cryptographic devices and use them to evaluate (through simulation) the efficiency of dual-rail logic for preventing fault-based attacks. The analysis results are then compared to real fault injection experiments where laser pulses are used to inject temporary faults into a DES device.

Finally, the Brief Contribution, "An RSA Implementation Resistant to Fault Attacks and to Simple Power Analysis" by C. Giraud, focuses on the classical public-key RSA cryptosystem. The practical importance of RSA justifies a careful analysis of its already known and new fault attacks and their corresponding countermeasures. This paper demonstrates that, even for established and extensively studied systems, it is possible to find new aspects which require reexamination and new designs.

The papers included in this special section illustrate the interaction among classical fault diagnosis techniques, cryptography and fault injection-based attacks. The interested reader may wish to refer to a recently published survey paper: "The Sorcerer's Apprentice Guide to Fault

- *L. Breveglieri is with the Department of Electronics and Information Technology, Politecnico di Milano, Milano, Italy. E-mail: brevegli@elet.polimi.it.*
- *I. Koren is with the Department of Electrical and Computer Engineering, University of Massachusetts, Amherst, MA 01003. E-mail: koren@ecs.umass.edu.*

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

Attacks" by H. Bar-El, H. Choukri, D. Naccache, M. Tunstall, and C. Whelan (*Proceedings of the IEEE*, vol. 94, no. 2, pp. 370-382, Feb. 2006) that provides an excellent introduction to the main methods and techniques for carrying out successful fault attacks on cryptographic devices.

We would like to thank the authors of all of the submitted papers, including the authors of papers that could not be included in this special issue due to extensive revision requests made by the referees. We also want to express our personal thanks to the referees, whose names will be included with the reviewers list for 2006. We greatly appreciate their time and effort, especially because of the short turn-around times required. Special thanks are due to the Editor-in-Chief, Professor Viktor Prasanna, for hosting this special section, and to Ms. Joyce Arnold for her support during the editorial process.

Luca Breveglieri
Israel Koren
Guest Editors

Luca Breveglieri received both the MSc degree in electronic engineering and the DSc degree in electronic engineering of information technology and systems from the Politecnico di Milano, Italy, in 1986 and 1992, respectively. From 1991 to 1998, he was a computer technician and a part-time researcher. Since 1998, he has been an associate professor of computer science at the Politecnico di Milano. He has more than 60 publications in refereed journals and conferences. His current research interests include architectures of computing systems, application specific VLSI synthesis, computer arithmetic and cryptography, and formal languages theory.

Israel Koren (S'72-M'76-SM'87-F'91) received the BSc, MSc, and DSc degrees from the Technion—Israel Institute of Technology, Haifa, in 1967, 1970, and 1975, respectively, all in electrical engineering. He is currently a professor of electrical and computer engineering at the University of Massachusetts, Amherst. Previously, he was with the Technion and also held visiting positions with the University of California at Berkeley, University of Southern California, Los Angeles, and University of California, Santa Barbara. He has been a consultant to several companies, including IBM, Intel, Analog Devices, AMD, Digital Equipment Corp. and National Semiconductors. Dr. Koren's current research interests include fault-tolerant techniques with a focus on cryptographic systems, VLSI yield and reliability, and computer arithmetic. He has published extensively and has more than 200 publications in refereed journals and conferences. He was a co-guest editor for the *IEEE Transactions on Computers*, special issue on high yield VLSI systems, April 1989, and a special issue on computer arithmetic, July 2000. He served on the editorial board of the *IEEE Transactions on Computers* between 1992 and 1997 and has served on the editorial board of the *IEEE Transactions on VLSI Systems* since 2001. He also served as general chair, program chair, and program committee member for numerous conferences. He is the author of the textbook *Computer Arithmetic Algorithms*, second edition (A.K. Peters, Ltd. 2002) and a coauthor of a forthcoming textbook *Fault Tolerant Systems* (Morgan Kaufman, 2007). He is a fellow of the IEEE.