Journal of Computers

Special Issue on Computer Arithmetic and Cryptography

FOREWORD

Computer arithmetic is fundamental to the design of general-purpose and application-specific processors. For cryptographic applications such as elliptic curve cryptosystems, the finite field arithmetic is a foundational principle to realize efficient hardware implementations and the high-speed or leak-resistant software for embedded systems, like smart cards. Since side channel attack is a very powerful technique to break cryptographic keys, several research works have been addressed concurrent error detection for digital electronic circuits during the last few decades. The design of efficient finite field arithmetic with concurrent error detection/correction feature is highly desirable to have a reliable operation of cryptographic hardware. Therefore, we need a forum for researcher to share their experiences in computer arithmetic and to further foster research in these areas.

The objective of this special issue is to present the novel researches and developments in various aspects of computer arithmetic and cryptography. We hope that this special issue would promote the interested computer scientists in finite field arithmetic research area. After a very careful reviewing process, the editorial committee accepts five outstanding papers to be included in this special issue. The first paper, by Prof. Meher from Institute for Infocomm Research in Singapore, presents an efficient systolic multiplier for all-one polynomial in GF(2^m). The second paper, a work by Prof. Liang and his research team from National Taipei University of Technology, Taiwan, employs the concept of REcomputing with Shift Operands to develop a concurrent error detection architecture in finite field multiplier for trinomials. The third paper, by Prof. Chiou and his research team from Ching Yun University, Taiwan, proposes a new self-checking alternating logic approach to detecting errors in a systolic polynomial basis multiplier. The fourth paper, by Prof. Lee from Lunghwa University of Science and Technology, Taiwan, develops a fault detection multiplier using linear code approaches. The final paper, by Prof. Chen from St. John's University, Taiwan, reports the realization of RFID Data Security and Privacy based on XOR operations. On behalf of the editorial committee, we would like to express my sincere thanks to all authors and reviewers for their great contribution to this special issue. We would also like to thank the editorial committee members for their excellent helps. Finally, we are grateful to Professor Chin-Chen Chang, the Editor-in-Chief, and the editorial staffs, for their kind helps. Without all of their great contribution and help, it is impossible to have this special issue.

Chiou-Yng Lee Guest Co-Editor
Professor
Department of Computer Information and Network Engineering, Lunghwa University of Science and Technology, Taoyuan County 333, Taiwan, R.O.C.
E-mail: PP010@mail.lhu.edu.tw

Che-Wun Chiou Guest Co-Editor
Professor
Department of Computer Science and Information Engineering, Ching Yun University, Chung-Li 320, Taiwan, R.O.C.
E-mail: cwchiou@cyu.edu.tw