

Guest Editors' Introduction to the Special Issue on Security of Computers and Networks

The rapid growth of secure transmission is a critical point nowadays. An essential aspect of secure communication over any type of network is cryptography. Cryptography algorithms fulfill specific information security requirements such as authentication, confidentiality, integrity and non-repudiation. We have to exchange data securely at very high data rates. Efficient solutions have to be hardware implemented and flexible in order to evolve with the permanent changes in norms. In addition, applications with strict requirements concerning performance, power consumption, or side-channel leakage are, in practice, usually implemented by dedicated hardware.

On the other hand, including network control, the various services are provided through home gateway. The possession of service framework with scalable is essential to continually provide these various services and upgrades. The security problems in existing gateways are authentication for mobility and connectivity with other networks, re-authentication and consistency about security, integrated authentication on various devices. Also, the configuration of security scheme and the insufficient support for integrated authentication services are major problems that need re-enhancements. In addition, in traditional computing environments, users actively choose to interact with computers. On the contrary, pervasive computing applications are embedded in the users' physical environments and integrate seamlessly with their everyday tasks.

This special issue of *Computers and Electrical Engineering: An International Journal* is on Security of Computers and Networks. The papers were peerly reviewed by outstanding researchers in this field. We are very grateful to them for their valuable comments and suggestions. The call for papers for the special issue announced the mainly nine areas in which we have sought papers; these were

- Security for mobile devices and 3G applications
- Reconfigurable processors in cryptography
- Public-key cryptosystems
- Embedded Systems Aspects
- Embedded Systems Security and Forensics
- Crypto-Processors for wireless networks
- Pervasive computing security (e.g. RFID, WiFi, WiMedia)
- Cryptography and cryptanalysis
- Network security

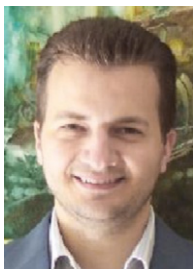
The contribution of each of the selected papers is summarised as follows. First, in a paper entitled *HW/SW Co-design for Public-Key Cryptosystems on the 8051 Micro-controller* by K. Sakiyama, L. Batina, B. Preneel and I. Verbauwhede. The authors presents a HW/SW co-design solution for RSA and Elliptic Curve Cryptography (ECC) over $GF(p)$ on a 12 MHz 8-bit 8051 micro-controller. The second paper entitled *Applying Systolic Multiplication-Inversion Architectures Based on Modified Extended Euclidean Algorithm for $GF(2^k)$*

in *Elliptic Curve Cryptography* by A. Fournaris and O. Koufopavlou mainly propose an optimized inversion algorithm that can be applied very well in hardware avoiding well known inversion problems. Then, in a paper by G. Elias, A. Miri, and T.-H. Yeap, entitled *On Efficient Implementation of FPGA-Based Hyperelliptic Curve Cryptosystems*, presents an efficient design of a high-performance Hyperelliptic Curve Cryptosystem for a Field Programmable Gate Array which is well suited for embedded systems having limited resources. Subsequently, in a paper entitled *Differential Power and Electromagnetic Attacks on a FPGA Implementation of Elliptic Curve Cryptosystems*, the authors (E. De Mulder, B. ORS, B. Preneel, I. Verbauwhede) describe a differential power and electromagnetical analysis attacks performed on a hardware implementation of an elliptic curve cryptosystem. After, in a paper entitled *Compact Modular Exponentiation Accelerator for Modern FPGA Devices* by T. Alho, P. Hämäläinen, present a compact FPGA implementation of a modular exponentiation accelerator suited for cryptographic applications. Thereafter, in a paper entitled *Hardware architectures for the Tate pairing over $GF(2^m)$* , by M. Keller, R. Ronan, W.P. Marnane, and C. Murphy, present two different approaches to the design of a reconfigurable Tate pairing hardware accelerator. Afterward, in a paper by A. Ashkenazi and D. Akselrod entitled *Platform Independent Overall Security Architecture in Multi-processor System-on-chip Integrated Circuits for Use in Mobile Phones and Handheld Devices* show an architecture provides an enhanced security protection scheme for use in smartphones, PDA's, as well as other similar wireless systems. The remaining two papers are in the general area of computer and network security. The first one entitled *Security Aspects in IPv6 Networks – Implementation and Testing* by D. Žagar, K. Grgić, and S. Rimac-Drlje deals the security improvements and extensions in the IPv6 protocol. The second one, by Z. Banković, D. Stepanović, S. Bojanić, O. N.-Taladriz entitled *Improving Network Security using Genetic Algorithm Approach* realizes a misuse detection system based on Genetic Algorithm (GA) approach.

The guest editors thank the office of the *Computers and Electrical Engineering: An International Journal* and also the authors for giving us an opportunity to introduce a synopsis of work on Security of Computers and Networks to the scientific and engineering community.



Dr. Paris Kitsos received the B.Sc. degree in Physics in 1999 and a Ph.D. in 2004 from the Department of Electrical and Computer Engineering, both at the University of Patras. Currently is research fellow with the Digital Systems and Media Computing Laboratory, School of Science and Technology, Hellenic Open University (HOU). His research interests include VLSI design, hardware implementations of cryptographic algorithms and security protocols for wireless communication systems. Dr. Kitsos has published more than 60 scientific articles, edited books, books chapters and technical reports, as well as is reviewing manuscripts for International Journals and Conferences/Workshops in the areas of his research. Also, is a member of the Institute of Electrical and Electronics Engineers (IEEE) and Institution of Electrical Engineers (IEE).



Dr. Nicolas Sklavos received the Ph.D. Degree in Electrical and Computer Engineering, and the Diploma in Electrical and Computer Engineering, in 2004 and in 2000 respectively, both from the Electrical and Computer Engineering Department, University of Patras, Greece. His research interests include Cryptography, Wireless Communications Security, Computer Networks and VLSI Design. He holds an award for his Ph.D. thesis on “VLSI Designs of Wireless Communications Security Systems”, from IFIP VLSI SOC 2003. He was conference Co-Chair of MobiMedia'07. He has participated to international journals and conferences organization, as Program Committee Member and Guest Editor. Dr. N. Sklavos is a member of the ACM, IEEE, IEE, the Technical Chamber of Greece, and the Greek Electrical Engineering Society. He has authored or co-authored more than 80 scientific articles, books chapters, tutorials and reports, in the areas of his research.

Guest Editors
Paris Kitsos

*Computer Science, Hellenic Open University,
Patras, Greece*

E-mail address: pkitsos@eap.gr

Nicolas Sklavos

University of Patras, Greece
E-mail address: nsklavos@ieee.org

Available online 29 June 2007