

MONET Special Issue on Next Generation Hardware Architectures for Secure Mobile Computing

Nicolas Sklavos · Máire McLoone · Xinmiao Zhang

Received: 15 August 2007 / Accepted: 15 August 2007 / Published online: 28 September 2007
© Springer Science + Business Media, LLC 2007

Security is of paramount importance to the design of modern communication systems and in particular, to wireless networks. Wireless devices are becoming commonplace in both the office and home environment and therefore, the need for strong secure transport protocols is one of the most important issues in mobile standards. Cryptography is the foremost method for providing communication security and is a mathematically intensive process which, to date, has mainly been implemented in software. However, such methods are slow and cannot cope with the demands of rapidly growing real-time wireless communication systems. Encryption of digital information in real-time holds the key to the successful growth of applications such as wireless hand-held devices and high performance mobile communications. The innovative mapping of complex cryptographic operations onto hardware architectures with consideration for throughput, area and power issues has emerged as a viable solution. This special

issue aims to present recent advances in cryptographic hardware architectures for secure mobile computing. The majority of the accepted papers focus on the challenge of designing high-speed asymmetric cryptographic hardware architectures for mobile applications. Asymmetric techniques are, in general, more complex than symmetric cryptographic methods and as such, it is inevitably more difficult to design efficient low resource, high-speed asymmetric architectures. The most common and best known asymmetric scheme is the RSA algorithm, but hardware implementations of RSA can require tens of thousands of gates. A much more promising asymmetric security solution is elliptic curve cryptography (ECC). ECC is viewed as a low-cost alternative to RSA and provides similar security strengths using much shorter key lengths. The research described in the contributions to this special issue illustrate the possibilities of using ECC to provide strong security for mobile computing applications.

The first paper, ‘A Survey of Cryptographic Primitives and Implementations for Hardware-Constrained Sensor Network Nodes’, by Roman, Alcaraz and Lopez surveys existing research into hardware and software cryptographic implementations for wireless sensor networks. They conclude that while existing sensor nodes can support software security implementations, next generation sensor nodes will be able to support hardware security architectures of more complex asymmetric cryptographic algorithms.

The next three papers describe high-speed ECC processor architectures. Sakiyama, Batina, Preneel and Verbauwhede’s paper, ‘High-Performance Public-Key Cryptoprocessor for Wireless Mobile Applications’, presents an ECC processor hardware architecture that exploits parallel processing of the modular operations in the arithmetic logic unit, in addition to instruction-level parallelism to achieve a high overall

N. Sklavos (✉)
University of Patras,
Patras, Achaia 26500, Greece
e-mail: nsklavos@ieee.org

M. McLoone
ECIT Institute, Queen’s University Belfast,
Queen’s Road, Queen’s Island,
Belfast BT3 9DT, UK
e-mail: m.mcloone@ecit.qub.ac.uk

X. Zhang
Case Western Reserve University,
Cleveland, OH, USA
e-mail: xinmiao.zhang@case.edu

performance. In the paper, ‘A State-of-the-art Elliptic Curve Cryptographic Processor Operating in the Frequency Domain’, Baktir, Kumar, Paar and Sunar outline a novel ECC processor hardware architecture that performs all of the finite field operations required in elliptic curve computations in the discrete Fourier domain. The architecture achieves a high throughput and is area efficient, thus making it suitable for secure mobile computing applications. The paper, ‘Hardware Organisation to achieve High-Speed Elliptic Curve Cryptography for Mobile Devices’, by Liu, King and Wang describes a novel lookup-table-based sharing scheme which reduces the computation involved in ECC when implemented using the Lopez-Dahab projective co-ordinate system. Their design results in a reduction in the execution time of elliptic curve scalar multiplication.

In the final paper, ‘New and Improved Architectures for Montgomery Modular Multiplication’, Sudhakar, Kamala and Srinivas present an improved Montgomery multiplier architecture, which utilises four-to-two carry save adders and pre-computed input values to reduce the overall critical path delay. The resulting high-speed modular multiplier is applicable to both RSA and ECC asymmetric cryptography.

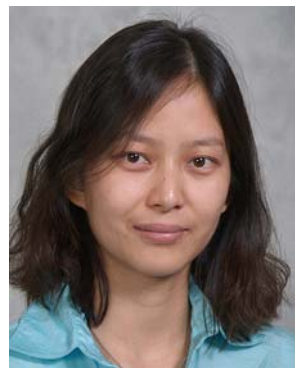
The guest editors would like to thank the authors for their valuable contributions to this special issue and all of the reviewers, who provided constructive suggestions and thorough reviews during the paper selection process. The help and support of the MONET editorial team was also greatly appreciated.



Nicolas Sklavos received a Ph.D. Degree in Electrical & Computer Engineering, and a Diploma in Electrical & Computer Engineering, in 2004 and in 2000 respectively, both from the Electrical & Computer Engineering Dept., University of Patras, Greece. His research interests include Cryptography, Wireless Communications Security, Computer Networks and VLSI Design. He holds an award for his PhD thesis on “VLSI Designs of Wireless Communications Security Systems,” from IFIP VLSI SOC 2003. He was the conference general chair of MobiMedia’07. He has participated in numerous international journal and conference organization, as Program Committee Member and Guest Editor. Dr. N. Sklavos is a member of the ACM, IEEE, IET, the Technical Chamber of Greece, and the Greek Electrical Engineering Society. He has authored or co-authored up to 90 scientific articles, books chapters, tutorials and reports in the areas of his research.



Máire McLoone obtained a Master of Engineering with distinction in Electrical and Electronic Engineering from Queen’s University Belfast in 1999 and was awarded a Ph.D. in Digital Signal Processing from Queen’s in 2002. In 2004 she was presented with the Vodafone award for her work in high-speed data security at the Britain’s Younger Engineers event held at the House of Commons, London. She was awarded the Women’s Engineering Society (WES) prize at the 2006 IET Young Woman Engineer of the Year awards. In 2007 she was named British Female Inventor of the Year at the British Female Inventors & Innovators Network (BFIIN) awards ceremony. She is currently in her final year of a 5-year UK Royal Academy of Engineering research fellowship conducting research into cryptographic algorithms and architectures for system-on-chip. Dr McLoone has authored a research book on ‘System-on-Chip Architectures and Implementations for Private-Key Data Encryption,’ Kluwer Academic Press, 2003. She was a guest editor of the launch issue of the IET proceedings on Information Security published in October 2005. She has over 40 peer-reviewed conference and journal publications. In 2005 she was selected as a European Commission expert evaluator for Framework Programme 6 Marie Curie schemes. Dr McLoone leads the SoC Cryptographic research group at the ECIT Institute, Queen’s University Belfast and her research interests include generic silicon architectures for symmetric and asymmetric cryptographic algorithms, security for wireless and ad hoc networks, hardware/software cryptographic system-on-chip architectures and cryptography for constrained environments. She is a fellow of the HEA and a member of the IET, IEEE and IACR.



Xinmiao Zhang received the B.S. and M.S. degrees in Electrical Engineering from Tianjin University, Tianjin, China, in 1997 and 2000, respectively. She received her Ph.D. degree in Electrical Engineering from the University of Minnesota-Twin Cities, in 2005. Since then, she has been with Case Western Reserve University, where she is currently a Timothy E. and Allison L. Schroeder Assistant Professor in the department of Electrical Engineering and Computer Science. Her research interests include efficient VLSI architecture design for communications, cryptosystems, and digital signal processing. Ms. Zhang is the recipient of the Best Paper Award at ACM Great Lake Symposium on VLSI 2004. She is a member of IEEE.