Guest Editors' Introduction to Security in Reconfigurable Systems Design

PATRICK R. SCHAUMONT
Virginia Polytechnic Institute and State University
ALEX K. JONES
University of Pittsburgh
and
STEVE TRIMBERGER
Xilinx Inc.

This special issue on Security in Reconfigurable Systems Design reports on recent research results in the design and implementation of trustworthy reconfigurable systems. Five articles cover topics including power-efficient implementation of public-key cryptography, side-channel analysis of electromagnetic radiation, side-channel resistant design, design of robust unclonable functions on an FPGA, and Trojan detection in an FPGA bitstream.

Categories and Subject Descriptors: C.1.3 [**Processor Architectures**]: Other Architecture Styles—*Adaptable architectures*; C.3.3 [**Processor Architectures**]: Special-purpose and Application-Based Systems—*Real-time and embedded systems*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms: Security, Reliability, Design

Additional Key Words and Phrases: Trustworthy design, side-channel resistant design, physically unclonable function, Trojan

ACM Reference Format:
Schaumont, P. R., Jones, A. K., and Trimberger, S. 2009. Guest editors' introduction to security in reconfigurable systems design. ACM Trans. Reconfig. Techn. Syst. 2, 1, Article 1 (March 2009) 6 pages. DOI = 10.1145/1502781.1502782. http://doi.acm.org/10.1145/1502781.1502782.

Patrick Schaumont is supported in part by grant 0644070 from the National Science Foundation.
Authors' addresses: P. Schaumont, Virginia Tech, Whittemore Hall 302, Blacksburg VA 24061; A. K. Jones, University of Pittsburgh, Benedum Hall 334, Pittsburgh, PA 15260; S. Trimberger, Xilinx Inc, 2100 Logic Drive, San Jose, CA 95124.

1. INTRODUCTION

The trustworthy operation of reconfigurable electronic systems is an important emerging area that is vital to us as security concerns are extending beyond the software information-processing domain into the hardware domain. Many researchers are exploring these opportunities within the area of reconfigurable computing. Indeed, the special role of reconfigurable hardware in the design of a trustworthy system is illustrated by the following examples.

—From a design perspective, security forms a separate dimension, next to constraints on area, performance, and power [Ravi et al. 2004]. It is well known that the best design from a power or performance perspective may not be the best one from a security perspective.

—Secure design emphasizes information leakage and dependable behavior. This leads to unique design techniques. Some examples include constant-power/constant-time design, design and implementation of boundaries for logical and physical protection, design of protected storage, and design of secure computing primitives, among others.

—In order to optimally defend a secure embedded system, there is need for isolation techniques that will partition security-critical parts from noncritical parts and that will minimize the use of expensive defenses.

Reconfigurable devices are uniquely positioned to tackle these requirements. By carefully considering security issues in the design of reconfigurable hardware, security becomes a basic property of the system implementation rather than being addressed as an afterthought. Additionally, the soft nature of design in reconfigurable devices provides an opportunity to address intellectual property issues in a detailed and novel manner. Security-related research efforts using reconfigurable devices have been presented at academic and industrial conferences on a regular basis, and these efforts fall into two broad categories: (1) secure design technology and architectures and (2) novel secure applications and secure application exploits. Secure design technology and architectures are able to treat security as a separate design dimension. This is illustrated in the following examples.

—The reconfigurable fabric supports innovative architectures. Examples include the physical partitioning of subsystems on a single die [Huffmire et al. 2007], the creation of device-unique identifiers for anti-counterfeiting and bit-stream authentication [Suh and Devadas 2007], and the design of side-channel resistant and fault-tolerant circuits [Standaert et al. 2006; Wollinger et al. 2004].

—Bitstream confidentiality and authentication is required to provide intellectual property protection in the field [Trimberger 2007]. This problem has a technological dimension (how to support confidentiality with a given reconfigurable fabric) as well as a methodological, protocol-oriented dimension [Gogniat et al. 2005; Drimer 2007].

—Methods are needed to quantify the trade-offs between security, performance, and power in reconfigurable circuits, in particular in the area of

cryptographic algorithms [Alrimeih and Rakhmatov 2007]. In addition, formally verifiable design automation techniques ensure that synthesis will maintain trust and security properties in the design [Hammarberg and Nadjm-Tehrani 2003].

—The implementation of physically unclonable functions [Guajardo et al. 2007] demonstrates how the uniqueness of a given reconfigurable technology can be used for authentication and anti-counterfeiting applications.

—Tracing, metering, and watermarking of intellectual property (IP) in the reconfigurable design flow is important because such design flows are heavily reliant on intellectual property components often provided through multiple parties [Lach et al. 1999]. Reconfigurable technology is particularly susceptible to IP theft because the IP is present in soft form, as bit-streams.

Reconfigurable platforms also enable novel secure applications and provide opportunities for new methods of attack.

—Modular arithmetic and extended word-length arithmetic can be supported efficiently on a fine-grain reconfigurable fabric, yielding significant speedups over equivalent software-based systems [Sakiyama et al. 2007; Suzuki 2007].

—Brute-force attacks on cryptographic algorithms can be significantly accelerated using reconfigurable devices [Kumar et al. 2006].

—New attack meethodologies require new countermeasures for security applications that execute on reconfigurable devices [Standaert et al. 2006; Wollinger et al. 2004].

—High-quality cryptographic primitives, including true random number generators, can be built using reconfigurable devices and standard logic design [Sunar et al. 2007; Dichtl and Golic 2007].

—Finally, trusted computing primitives including block ciphers, stream ciphers, hash functions and public-key ciphers are all excellent candidates for prototyping on a reconfigurable fabric [Eisenbarth et al. 2007; Bajracharya et al. 2004].

2. SPECIAL ISSUE OUTLINE

We received twenty-five submissions, each of which was reviewed by a minimum of three reviewers, according to standard ACM guidelines. Based on the reviewers' recommendations, we've selected five articles for publication in this special issue. These five articles cover topics from both major areas just discussed. The topics include low-power implementation of secure algorithms, new attack methods as well as new countermeasure methods for secure algorithms on a reconfigurable architecture, PUFs, and detection of design tampering. This issue provides an interesting snapshot of active research in security for reconfigurable devices.

A first important motivation to use reconfigurable logic in secure systems design is improved performance and energy efficiency. Indeed, architecture specialization will result in implementations with better efficiency, which has

an obvious benefit for compute-intensive algorithms such as public-key cryptography. The first article, *Elliptic Curve Cryptography on FPGA for Low Power Applications*, is by Maurice Keller, Andre Byrne and William Marnane. Their article illustrates the impact of the system design parameters of an elliptic-curve cryptoprocessor on the power and energy consumption of an FPGA. Such system parameters include, for example, the elliptic-curve coordinate system or the scalar multiplication methods. The authors conclude that the impact of the ECC system parameters on the execution time of the algorithm is larger than the impact on the power dissipation of the FPGA. Hence, for energy-constrained operations, the optimization of execution time is more important.

Intensely researched for over a decade, side-channel analysis exploits the information leakage of circuits through their power signature. This nonintrusive passive attack can be mitigated using side-channel resistant circuits, which either randomize or hide the circuits' power signature during active operation. The second article, *Isolated WDDL: A Hiding Countermeasure for Differential Power Analysis on FPGAs*, is by Robert McEvoy, Michael Tunstall, Colin Murphy and William Marnane. The authors present a side-channel resistant design technique based on wave dynamic differential logic. In the article, the authors show how to address the routing symmetry requirement that must be met in an FPGA when implementing WDDL logic.

Side-channel analysis can be performed on any implementation charateristic of a system. Recent developments have focused on electromagnetic (EM) radiation, emitted by a cryptocircuit as a result of switching digital gates. The third article, *Electromagnetic Radiations of FPGAs: High Spatial Resolution Cartography and Attack of a Cryptographic Module* by Laurent Sauvage, Sylvain Guilley, and Yves Mathieu describes such an EM-based attack on reconfigurable logic. By using small EM-probes, the authors can perform localized power measurements with an increased signal-to-noise ratio compared to global power measurements. The authors present measurement results and a successful attack on a commercial 130nm CMOS FPGA.

The fourth article addresses an important and new development in reconfigurable technology: the design of robust cryptographic hardware security primitives. By the nature of the manufacturing process variations, it is possible to distinguish one unique die from another one by building a physically unclonable function (PUF). These PUF have important applications as secure nonvolatile key storage and as components in intellectual property protection protocols. In *Techniques for Design and Implementation of Secure Reconfigurable PUFs*, Mehrdad Majzoobi, Farinaz Koushanfar and Miodrag Potkonjak describe methods to protect a PUF against reverse engineering and emulation attacks. The authors propose countermeasures that exploit the reconfigurability of the FPGA fabric.

A recent concern that has raised interest from DARPA and system houses is that of malicious tampering of the configuration data in reconfigurable circuits. These modifications are called Trojans and are intended to subvert a systems' correct operation after deployment. Trojans must be mitigated by detecting tampering in the reconfigurable design flow. The challenge is that

these malicious modifications cannot be predicted upfront. In the final article, *Trust-Based Design and Check of FPGA Circuits Using Two-Level Randomized ECC Structures*, Santanu Dutt and Li Li discuss techniques to detect Trojans inside of the reconfigurable logic of an FPGA. The detection techniques are designed so that the chance for a Trojan to bypass the detection circuitry becomes very small.

3. CONCLUSIONS

Security is an increasingly important aspect in reconfigurable systems design. A broad and rich design space is available to designers who need trustworthiness at the system level, architecture level or circuit level. The articles in this special issue document a few of the recent exciting developments. At the same time, large areas of the design - and research space have yet to be explored. This includes for example an end-to-end design flow to map a given specification into a secure and trustworthy implementation on a reconfigurable device. Hence, the guest editors would like to encourage researchers to investigate this novel area.

ACKNOWLEDGMENTS

The guest editors would like to thank all authors who submitted or contributed articles for this special issue on Security in Reconfigurable Systems Design. In addition, a large group of anonymous reviewers has contributed valuable research time to read and comment on the submissions. Their insights and dedication is essential to the quality of the journal and the progress of this research field. Finally, the guest editors thank Jason Bakos, the Information Director with this Transactions, for helping us manage the review process.

REFERENCES

ALRIMEIH, H. AND RAKHMATOV, D. 2007. Security-performance trade-offs in embedded systems using flexible ECC hardware. *IEEE Design Test Comput. 24*, 6, 556–569.

BAJRACHARYA, S., SHU, C., GAJ, K., AND EL-GHAZAWI, T. 2004. Implementation of elliptic curve cryptosystems over GF(2^n) in optimal normal basis on a reconfigurable computer. In *Proceedings of the 2004 ACM/SIGDA 12th International Symposium on Field Programmable Gate Arrays (FPGA'04)*. ACM, New York, NY, 259–259.

DICHTL, M. AND GOLIC, J. D. 2007. High-speed true random number generation with logic gates only. In *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. 45–62.

DRIMER, S. 2007. Authentication of FPGA bitstreams: Why and how. In *Proceedings of the International Workshop on Applied Reconfigurable Computing (ARC)*. 73–84.

EISENBARTH, T., GÜNEYSU, T., PAAR, C., SADEGHI, A.-R., SCHELLEKENS, D., AND WOLF, M. 2007. Reconfigurable trusted computing in hardware. In *Proceedings of the ACM Workshop on Scalable Trusted Computing (STC'07)*. ACM, New York, NY, 15–20.

GOGNIAT, G., WOLF, T., AND BURLESON, W. 2005. Reconfigurable security primitive for embedded systems. In *Proceedings of the International Symposium on System-on-Chip*. 23–28.

GUAJARDO, J., KUMAR, S. S., SCHRIJEN, G. J., AND TUYLS, P. 2007. FPGA intrinsic PUFs and their use for IP protection. In *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. 63–80.

HAMMARBERG, J. AND NADJM-TEHRANI, S. 2003. Development of safety-critical reconfigurable hardware with Esterel. In *Proceedings of the 8th International Workshop on Formal Methods for*

Industrial Critical Systems (FMICS'03). *Electronic Notes in Theoretical Computer Science 80*, 219–234.

HUFFMIRE, T., BROTHERTON, B., WANG, G., SHERWOOD, T., KASTNER, R., LEVIN, T., NGUYEN, T., AND IRVINE, C. 2007. Moats and drawbridges: An isolation primitive for reconfigurable hardware based systems. In *Proceedings of the IEEE Symposium on Security and Privacy (SP'07)*. IEEE Computer Society, Los Alamitos, CA, 281–295.

KUMAR, S., PAAR, C., PELZL, J., PFEIFFER, G., AND SCHIMMLER, M. 2006. COPACOBANA: A cost-optimized special-purpose hardware for code-breaking. In *Proceedings of the 14th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'06)*. IEEE Computer Society, Los Alamitos, CA, 311–312.

LACH, J., MANGIONE-SMITH, W. H., AND POTKONJAK, M. 1999. Robust FPGA intellectual property protection through multiple small watermarks. In *Proceedings of the 36th ACM/IEEE Conference on Design Automation (DAC'99)*. ACM, New York, NY, 831–836.

RAVI, S., RAGHUNATHAN, A., KOCHER, P., AND HATTANGADY, S. 2004. Security in embedded systems: Design challenges. *Trans. Embed. Comput. Syst. 3*, 3, 461–491.

SAKIYAMA, K., MENTENS, N., BATINA, L., PRENEEL, B., AND VERBAUWHEDE, I. 2007. Reconfigurable modular arithmetic logic unit supporting high-performance RSA and ECC over GF(p). *Int. J. Electron. 94*, 5, 501–514.

STANDAERT, F.-X., PEETERS, E., ROUVROY, G., AND QUISQUATER, J.-J. 2006. An overview of power analysis attacks against field programmable gate arrays. *Proc. IEEE 94*, 2, 383–394.

SUH, G. E. AND DEVADAS, S. 2007. Physical unclonable functions for device authentication and secret key generation. In *Proceedings of the 44th Annual Conference on Design Automation (DAC'07)*. ACM, New York, NY, 9–14.

SUNAR, B., MARTIN, W., AND STINSON, D. 2007. A provably secure true random number generator with built-in tolerance to active attacks. *Trans. Comput. IEEE 56*, 1, 109–119.

SUZUKI, D. 2007. How to maximize the potential of FPGA resources for modular exponentiation. In *Proceedings of the Workshop on Cryptographic Hardware and Embedded Systems (CHES)*. 272–288.

TRIMBERGER, S. 2007. Trusted design in FPGAs. In *Proceedings of the 44th Annual Conference on Design Automation (DAC'07)*. ACM, New York, NY, 5–8.

WOLLINGER, T., GUAJARDO, J., AND PAAR, C. 2004. Security on FPGAs: State-of-the-art implementations and attacks. *Trans. Embed. Comput. Syst. 3*, 3, 534–574.

Received January 2009; accepted January 2009