Special Session: Security on SoC

Organizers
Cathy Gebotys
University of Waterloo, Canada
Hiroto Yasuura
Kyushu University, Japan

Invited Talks
"Testing and Validation of MPC190",
Michael Torla, *Motorola, USA*
"Securing Wireless Data: System Architecture
Challenges," Srivaths Ravi, *NEC, USA*

Panel Discussion

Moderator:
Hiroto Yasuura, *Kyushu University, Japan*

Panelists:
Michael Torla, *Motorola, USA*
Srivaths Ravi, *NEC, USA*
Naofumi Takagi, *Nagoya University, Japan*
Cathy Gebotys, *University of Waterloo, Canada*

SoC is one of the important components of social and personal information systems, which directly influence with our life, property and privacy. Security technology is now embedded into various hardware and software of SoC and SoC designers should be concerned with security issues. Cryptography requires heavy computation and wireless communication requests architecture and protocols for security. In design process of SoC, choice of IP's and design data control also significantly affect on the security of the systems that uses the SoC. In this panel, we will have discussions on the security on SoC from various viewpoints. System architecture, circuit complexity, test and validation, energy consumption, security policy, and design methodology
are discussed for exploring research directions of secure system synthesis.

Position Statements

Michael Torla
Motorola, USA

Verification of cryptographic accelerator systems presents significant challenges to the design team. Parallelism must be addressed in a way that ensures that all parallel capabilities are exercised. BIST and SCAN techniques can ensure that the connections are manufactured correctly, but cannot verify proper functionality.

A multi-tiered approach, as outlined below, improves the likelihood of complete coverage of all functionality.

1. Unit-level testing. Each cryptographic accelerator core requires a suite of functional tests to ensure proper functionality, including compliance to standards. These tests should include all such compliance testing, and should also fully test the interface to the core.
2. System-level testing. The entire system must be integrated and tested to ensure proper operation. In a complex system, it will be nearly impossible to ensure proper testing of all possible accelerator core combinations through such a suite. The system-level suite should include all applicable unit-level tests, to ensure that the surrounding system does not mask any functionality that needs verifying.
3. Randomized testing: developing a method of specifying stimulus and expected response in a standard format (or template) permits stimulus reuse and encourages variability of other features. For example, in a system with multiple AES acceleration units, the same stimulus template allows verification of AES functionality using all acceleration units. This allows the focus then to be set on identifying and verifying different combinations of accelerator cores and other control units. Often, this can be achieved using randomizing techniques provided by verification tools. However, this relies on a good set of stimulus and expected response templates being written.

Focusing on the verification problem early ensures maximizing time available to verifying and debugging the design, thereby maximizing silicon functionality. Complex testbenches require non-trivial development time; such development needs to occur

Copyright is held by the author/owner(s).
ISSS'02, October 2-4, 2002, Kyoto, Japan.
Copyright 2002 ACM 1-58113-562-9/02/0010…$5.00.

in parallel with system design to minimize time-to-development.

Srivaths Ravi
NEC, USA

A large and increasing number of systems, and the SoCs they contain, need to deal with security in one form or the other - processors in PCs, PDAs, wireless handsets, and smart cards, ICs in network equipment such as routers, gateways, firewalls, storage and web servers, etc. While security has so far mostly been a concern of standards committees and software developers, there are several factors that will increasingly elevate security considerations during HW and system architecture design:

(i) Software solutions are not sufficient to keep up with the computational demands of security processing, due to increasing data rates and complexity of security protocols. These shortcomings are most felt in systems that need to process very high data rates or a large number of transactions (e.g., network routers, firewalls, web servers), and systems with modest processing resources (e.g., PDAs, wireless handsets and smartcards).

(ii) New techniques for breaking security, such as fault analysis, power analysis, etc., require that the system implementation itself be secure even when it can be physically accessed by malicious entities. Resistance to such attack techniques can be ensured only if built-in during system design.

(iii) In addition to the traditional security concerns such as privacy, authentication, and integrity, new issues such as denial of service and security of systems that execute dynamically downloaded third-party software (or hardware in the case of re-configurable systems), need to be addressed. Some of these problems require solutions that will be even more complex than the existing encryption techniques and security protocols.

(iv) As SoCs themselves begin to resemble complex systems that consist of components (IP) assembled from different sources, the responsibility of ensuring a "secure implementation" needs to be distributed across IP developers and system integrators.

We believe that advanced system architectures and design methodologies will be necessary to address the above challenges, and security issues in HW/SW system design will emerge as an important area of research and development.

Naofumi Takagi
Nagoya University, Japan

Demands on security are introducing much more computation for encryption/decryption on SoC. For example, long-bit multiplications in RSA algorithm and shuffle operations in AES consume a lot of chip area and large amount of energy. Hardware algorithms and architectures of basic operations for encryption/decryption significantly influence performance, cost, and energy consumption of SoC. IP's for encryption/decryption will be very important components for SoC design. For security on SoC, we have new questions in system design.

(1) What is a good system architecture from the viewpoint of security?

Are there any trade-off between security and area/performance/energy of a system?

(2) How can we design good hardware algorithms for security computation and verify their correctness?

(3) How can IP's for encryption/decryption be supplied without loss of security in design phase?

Hardware-software co-design, computational complexity analysis, verification methods and synthesis methods for security computation are also urgent technologies.

Cathy Gebotys
University of Waterloo, Canada

Security implementations are found everywhere, they are present in PDAs, smartcards, e-commerce, and other devices including battery authentication, postal networks, and more. Security not only involves (de)encrypting audio, video, and data, but cryptographic algorithms to generate keys, authenticate sites or authenticate communicating PDAs or components and support non-repudiation. However there are numerous problems with existing security implementations. Lessons learned from these problems are: 1) it is not sufficient to have protocols with security, but the implementation of these protocols must be secure (consider 802.11 security failure [2]); 2) although standards exist for security at the network layer, there must be security standards developed at the hardware or physical level (a "tamper resistant" smart card was broken in 1999 through power analysis [1]); 3) it is essential to chose the right (de)encryption/cryptographic algorithms in portable devices (for example, with equivalent security, an incorrect choice of standardized cryptographic algorithms, could be 1920 times worse in execution time[3], and more in energy dissipation); 4) there is a growing market for illegal use of cryptography, thus security is receiving more attention with funding opportunities; 5) increased needs for security engineers; embedded systems designers trained in security.

Unfortunately within the systems synthesis and embedded design field, little research has been performed in developing methodologies which support security. Currently security research lies more in the mathematics domain with only a few emerging worshops, such as CHES, targeting implementation issues and hardware. This is largely due to the complex mathematical barrier involved in cryptographic work. Methodologies are a necessity in designing these embedded systems to tradeoff performance, energy dissipation, cost and security. Metrics are also a necessity for quantizing security at the hardware implementation level (ie. to quantize their resistance to EM or power analysis attacks) in addition to current software level security metrics (ie. key size). Technologies for security suggested so far range from new devices (which dissipate equivalent power for 0-1 and 1-0 switching), to high speed security processor engines [6], key-specific FPGA designs, DSP processor implementation, smartcard processor implementation, and general purpose processor implementation. From this group of technologies, DSP processor cores are most suitable for portable wireless applications providing lower cost alternative with lower energy dissipation than general purpose processors, and implementation security through highly parallel architectures supporting decorrelation of data. Furthermore DSP processors are highly suitable for (de)encryption and cryptographic applications, providing flexibility for supporting numerous standards. As an example consider the more complex yet efficient elliptic curve cryptography in prime fields[4], it demands a large number of integer multiplications (within multiprecision arithmetic algorithms), as well as high memory bandwidth, high speed shifting, and general arithmetic logic computations. It is not surprising that these key characteristics are also shared by DSP applications.In summary 1) with the proliferation of IP-enabled wireless communication devices there is a need for new methodologies and metrics which support security as a design objective in addition to performance, cost, energy dissipation, 2) it is believed that existing technology, specifically DSP processor cores, will play an important role in supporting secure software in portable devices maintaining flexibility to support numerous cryptographic applications, 3) design of secure cryptographic implementations on portable devices which are low energy dissipation, high performance will create new challenges for embedded system designers which must be trained in security.

REFERENCES

[1] P. Kocher, J. Jaffe, B. Jun, “Differential Power Analysis”, LNCS 1666, 1999.

[2] A. Stubblefield, J. Ioannidis, A.Rubin “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, AT&T Lab, Tech.Rept TD-4ZCPZZ, August 2001.

[3] A. Menezes, et al. “PGP in constrained wireless devices” Proc of 9th USENIX Sec. Symp. 2000.

[4] C. Gebotys, R. Gebotys, Secure Elliptic Curve Implementations: An analysis of resistance to power-attacks in a DSP processor, to appear CHES’ 02, LNCS 2002.

[5] M. Torla, “Testing and Validation of MPC190” in this proceeding