Back to Contents

What is Hardware Security?

Farinaz Koushanfar, ECE, Rice University
Miodrag Potkonjak, CS, University of California at Los Angeles

Historically, the dominant technological and application trends have had a direct impact on the key integrated circuits design metrics. In the 70s, the silicon area was a scarce and expensive commodity. Therefore, development of techniques such as hardware sharing and design simplification was of prime importance. In the 80s, the premier design metrics was the speed of computation while in the 90s, the quest for power and energy optimization emerged. Initially, the emphasis was on minimizing the switching power but the focus has gradually moved towards minimizing the leakage energy.

The first decade of this century was marked by development of techniques for simulation and optimization in presence of (process variation) for deep submicron technologies. In the past few years, the two relevant topics of reliability and security started to attract a great deal of research attention. The scope of security research is already very wide and unceasingly broadening. Security today encompasses not just traditional notions of data communication and storage protection and privacy but also notions of privacy of actions, trust, digital rights management and many others. The leading-edge applications including data centers, mobile communication and embedded devices, and sensor networks are often exposed to side channels, physical, and software attacks. Operation in potentially hostile environments renders traditional and even emerging cryptographic techniques of limited effectiveness [1][11].

A novel suit of security and trust solutions based on process variation, design variability, and unique integrated circuits signatures is emerging [2-11]. The new methods are elegant yet practical, while they also provide low power and low cost security solutions. The variability itself has many aspects including but not limited to fluctuations in IC timing, power, temperature profile, substrate noise, and aging. Aside from CMOS, other device technologies including but not limited to photonic fibers, nano- technologies, plasmonics, and RF interconnects show variability. Therefore, security and trust techniques based on variability can be easily adapted to new and emerging technologies.

The famous physicist Richard Feynman once said: .There's Plenty of Room at the Bottom.. Perhaps we can add to the quote that there is also plenty of randomness, uniqueness, and unpredictability down there. As usual, any coin has two sides. The intrinsic variability is an ideal platform to build new generation of security protocols based on the uniqueness of each device. But at the same time, it tremendously complicates the detection of new types of attacks such as addition of malicious circuitry either by foundry or by untrusted tools [1][12].

Hardware-based system and application security encompasses rapidly increasing number of research directions. Among them, the most popular (if not the most

relevant) are hardware Trojan detection [5][6][10][11], trusted synthesis using untrusted tools [12], new security primitives [3][4], novel synthesis techniques integrating IC and architectural components with security primitives, preventing piracy and over-building of integrated circuits [2], and hardware-based security protocols [3][4][7][8]. Hardware Trojans refer to modifications, alterations, or insertions to the original IC for adversarial purposes. Although to date only a limited number of Trojan attacks were reported in industrial practice, hardware Trojans are probably one of the most popular contemporary research topics. Depending on the assumptions and models, the Trojan detection task may be straightforward or highly intractable. Most often, a hardware Trojan consists of one or more added gates and wires embedded somewhere in design by malicious party in such a way that standard structural and functional tests are ineffective for detecting the change [5][10]. If one assumes no process variations, all what is needed is to measure for example switching or leaking power for short sequences of input and compare them against a golden simulation model. However, process variation greatly complicates hardware Trojan detection. In particular, the Trojans are hard to detect if they are placed in an intelligent way off the critical paths or if their output is correlated with the existing gates. In such situations, the structural or side channel tests are of limited effectiveness for detection.

For example, it has been shown that the Trojan detection objective function can be written in a submodular way, such that for a certain given set of Trojan test vectors, no algorithm can found a better solution within 63% of the optimal detection [6]. Any Trojan outside this bound would stay undetected by the detections that use the set of given test vectors. Interestingly, new measurement methods that can go beyond traditional test vector limitations, such as the recent thermal conditioning techniques provide starting points for a more effective and scalable hardware Trojan detection [11]. In addition, new testing methods can be used for diagnosis and masking of malicious circuitry. The scope of hardware Trojans is currently restricted to addition of few gates but one can envision hardware Trojans that include gate sizing alternations or clock tree malicious modifications [1][5][10][12]. We believe that in particular, it is important to develop techniques that prevent CAD and compilation tools to alter designs in unwanted ways.

Another important variability-based hardware security research topic and direction are physical unclonable functions (PUF) [4][7][8]. PUF is a revolutionary concept with a large practical potential. A PUF provides a unique and unclonable chip-dependent mapping from a set of inputs (challenges) to a set of outputs (responses). The dependency map is such that it is difficult to reverse-engineer (predictive model) using numeric and/or statistical techniques. In addition, the mapping on each chip should not be predictable. A great variety of technologically different and architecturally unique PUFs have been proposed and implemented. Unfortunately, many of the existing PUF solutions are shown not to be secure because of the limited number of possible challenge responses, or because of the linearity or low level of nonlinearity of the structure, or susceptibility to statistical characterization and other reverse-engineering attacks [9].

It is important to emphasize that PUFs are by no means the only hardware

variability-based security primitive. For example, the very important classes of silicon identifiers and true random number generators can also be built upon process and random fluctuations. The common PUF structures also present a number of limitations including but not limited to the exponential size of challenge/response database [4]. Public PUFs (PPUF) are a special class of PUFs where reverse engineering is simple and feasible. PPUFs enable a novel class of asymmetric key (public key) cryptography system. In an asymmetric cryptography, the key used for encryptying messages is not the same as the decrypting key. For example, each user can encrypt by a publicly published key (public key), and only the owner of a matching secret key (private key) can decrypt the message. The private key cannot be found from the knowledge of a public key in a polynomial time.

The structural details of a PPUF are publicly published, allowing everybody to find the response to a given challenge by simulation that can be used as a public key [3]. Even though everybody can find the challenge/response by simulations the response cannot be found within a given time-bound by entities other than the authentic device. In other words, no simulation or parallelization reaching a bound of the original device computation time can be found [7]. The asymmetry in computation time between the original PPUF device and other entities can be used for creation of lightweight public key cryptography protocols. The PPUF-based security protocols are intrinsically resilient against side channel and physical attacks. In addition, they can potentially serve as the basic blocks for trusted design.

Hardware-based security protocols can be used to solve many seemingly impossible problems such as remote sensing, remote IC enabling and disabling, and trusted computations by the third party in a simple and elegant way. In many cases, there is a need that security primitives like PUFs or PPUFs are tightly integrated with the native device.s circuitry. This integration can be accomplished in several ways ranging from FSM boosting to their overlap of security primitives [2].

Hardware-based security systems and applications are in early stages of research where many false starts may be made. At the same time, there are tremendous, surprising and high impact research potentials and already very promising results. The field has a natural connection to reliability and testing, but often the problems are both conceptually and computationally much more difficult. Many challenges are yet to be addressed to ensure a long-term industrial impact for hardware-based security systems. There are already strong signs that the connections among security, reliability, testing, and ensuring proper functionality under differing operational conditions and environmental variations will have significant research and industrial impacts.

Bibliography

[1] S. Adee, The hunt for the kill switch. IEEE Spectrum, 45 (5), 34.39, 2008.

[2] Y. M. Alkabani, and F. Koushanfar, Active hardware metering for intellectual property protection and security. USENIX Security Symposium, 1-16, 2007.

[3] N. Beckmann, M. Potkonjak, Hardware-Based Public-Key Cryptography with Public Physically Unclonable Functions. Information Hiding Conference, 206-220, 2009.

[4] B. Gassend, D. Clarke, M. van Dijk, and S. Devadas, Silicon physical random functions. ACM Conference on Computer and Communications Security, 148.160, 2002.

[5] R. Karri, J. Rajendran, K. Rosenfeld, and M. Tehranipoor, Roadmap for Trusted Hardware - Part I: Hardware Trojan Taxonomy and Design. IEEE Computer Magazine, 2010.

[6] F. Koushanfar, A. Mirhoseini, and Y. Alkabani, A Unified Submodular Framework for Multimodal IC Trojan Detection. Information Hiding Conference, 2010.

[7] M. Majzoobi, A. Elnably, and F. Koushanfar, FPGA Time-bounded Unclonable Authentication. Information Hiding Conference, 2010

[8] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, Physical One-Way Functions. Science 297, 2026-2030, 2002.

[9] U. Ruhrmair, J. Solter, and F. Sehnke, On the Foundations of Physical Unclonable Functions, Cryptology ePrint Archive, 2009.

[10] M. Tehranipoor, and F. Koushanfar, A Survey of Hardware Trojan Taxonomy and Detection. IEEE Design and Test 27, 1 (Jan), 10-25, 2010.

[11] S. Wei, S. Meguerdichian, and M. Potkonjak. Gate-Level Characterization: Foundations and Hardware Security Applications. Design Automation Conference, 2010.

[12] Defense Science Board (DSB) study on high performance microchip supply in 2005: http://www.acq.osd.mil/dsb/reports/2005-02-hpms_report_final.pdf.

Back to Contents

Paper Submission Deadlines

DATE'11 - Design Automation and Test in Europe (sponsored by SIGDA)
Grenoble, France
Mar 14-18, 2011
Deadline: Sep 5, 2010
http://www.date-conference.com/

ISSCC'11 - Int'l Solid-State Circuits Conference
San Francisco, CA
Feb 20-24, 2011
Deadline: Sep 13, 2010
http://isscc.org/