09282 Executive Summary
Foundations for Forgery-Resilient Cryptographic Hardware
— Dagstuhl Seminar —

Jorge Guajardo[1], Bart Preneel[2], Ahmad-Reza Sadeghi[3] and Pim Tuyls[4]

[1] Philips Research - Eindhoven, NL
jorge.guajardo@philips.com
[2] Katholieke Universiteit Leuven, BE
Bart.Preneel@esat.kuleuven.be
[3] Ruhr-Universität Bochum, DE
ahmad.sadeghi@trust.rub.de
[4] Intrinsic-ID - Mol, BE
Pim.Tuyls@INTRINSIC-ID.COM

Abstract. From 05.07 to 08.07.2009, the Dagstuhl Seminar 09282 "Foundations for Forgery-Resilient Cryptographic Hardware" was held in Schloss Dagstuhl – Leibniz Center for Informatics. During the seminar, several participants presented their current research, and ongoing work and open problems were discussed. This paper provides a summary of the motivation for the seminar and the importance of the research area, a list of the participants and the program of talks given during the seminar.

Keywords. Foundations, PUF models, PUF applications, anti-counterfeiting, forgery resilience, side-channel attack models

1 Motivation

The rapid expansion of global connectivity, distributed applications and digital services over open networks and across organizational domains requires secure IT systems that adhere to well-defined policies. Cryptography and technical IT security mechanisms support the establishment of secure channels and authorized access. However, many of today's IT applications demand sophisticated security and privacy mechanisms in both software and hardware that go beyond secure channels and authorization and include truly secure liaisons: Enterprises or manufacturers outsource their computations, data storage, and production to potentially untrusted parties over which they have limited control. Medical records are transmitted through and processed by various IT systems such as Handhelds, PCs or hospital servers. Biometric data are carried by individuals on their ID card or electronic passport. Fake and counterfeited pharmaceuticals or automotive and avionic spare parts are packaged in some countries and distributed illegally to worldwide destinations.

Dagstuhl Seminar Proceedings 09282
Foundations for Forgery-Resilient Cryptographic Hardware
http://drops.dagstuhl.de/opus/volltexte/2010/2408

IT system security is, however, not only based on strong cryptographic primitives and protocols but also on technological support for secure implementation of the corresponding algorithms. In particular, this concerns security functionality provided by the underlying hardware, which is commonly deployed in the form of cryptographic hardware. The study of how to model, design, evaluate and deploy such cryptographic hardware was the focus of our seminar.

The recent trend of deploying security functionality in hardware typically assumes trust in the various parties involved in the design and manufacturing of the hardware. The life-cycle of cryptographic hardware begins with the IC design step, which results in IC blue-prints being shipped for production to (typically overseas) low-cost manufacturer's facilities. This trend is driven by economic and strategic reasons as well as by globalization. Although this model has many advantages, it also has the disadvantage that it becomes much easier for attackers to compromise hardware devices commonly used in critical infrastructure, which includes commercial, health and defense applications.

As a result, today many ICs and components are overbuilt (over-produced in an unauthorized manner). This, in turn, allows such devices and components to enter the market through gray channels and erode the revenues of legitimate Intellectual Property (IP) owners. In addition, there is a high risk that the functionality on the chip is (deliberately) modified or supplemented with a hidden trapdoor circuit, e.g., a hardware Trojan. For instance, keys which were never supposed to leave a security chip might be leaked (e.g., via padding), the tamper or leakage protection circuits of a chip may be disabled or weakened, a True Random Number Generator may be biased or the IC might have a kill switch that makes it stop functioning under certain conditions. Even in the non-malicious case, overseas manufacturers may try to cut costs by omitting or reducing security measures from the original design. Any single one of these manufacturing attacks or malpractices will have serious consequences for any security application, allow industrial espionage, privacy violations, and finally even threaten national security.

Current methods for assuring the trustworthiness of cryptographic hardware rely heavily on the skills of an evaluator. The lack of standardized methodologies and tools requires that the evaluator correctly identifies and manually evaluates each risk area. The evaluator must be aware and execute all known attacks while also formulating and exercising new forms of attack. The evaluator knows only what was found, not what's left to be found. More resources are used to obtain higher levels of assurance with the ultimate measure of assurance being what happens once the product is in production or it has been deployed. Advances in commercially viable approaches to assure the security of hardware is critical. From defining systematic approaches for assurance to identifying tools to automate and continuously improve assurance levels, significant new research is required. Moreover, commercial hardware engineering practices are well behind software engineering when it comes to establishing a set of best practices that will yield high-quality security products. Existing methods developed for high assurance hardware, typically for use by governments, either break down when

considering the size of designs (e.g., microprocessors) or are unacceptable from an economic perspective. Thus, a systematic approach with a solid scientific basis is required to ensure that hardware as the security anchor (or root of trust) for computing will deliver the necessary security guarantees.

2 Objectives and Goals of the Seminar

Based on the previous discussion, it is clear that there is an urgent need to design and develop methods that increase the security and trust in current hardware solutions. The purpose of this seminar was to bring together researchers from academia and industry and from different disciplines (cryptography, information theory, theoretical and experimental physics, hardware architectures and processor design), and allow them to investigate a whole new set of security and cryptographic methodologies which will allow for the development of reliable and trustworthy hardware components. Such trustworthy components will constitute the "root of trust" for future generation security devices and applications.

We have identified as the main challenges to provide strong, cost-effective and easily deployable methodologies and technological means to solve the following issues:

Exploiting inherent nano-scale physical properties (randomness) in hardware as a new key feature for a new level of security:

- The randomness caused by inherent variations in the hardware manufacturing process can be exploited to uniquely identify devices. In this context the most promising and interesting recent development based on primitives called Physically Unclonable Functions (PUFs), which are functions embodied in a physical structure. Due to their random structure a physical stimulus/challenge generates an unpredictable response which can be used for the purpose of device authentication. Regardless of their particular instantiation, the unclonability, tamper-evidence and tamper-resistance properties of PUFs are very useful tools in anti-counterfeiting, secure secret key storage or binding software components to the underlying hardware.
- Investigating what sources of randomness we can exploit for this purpose, and how to use them efficiently.
- Integrating components based on unique physical properties into cryptographic primitives and security protocols, and investigating the security properties achieved by such systems.
- Investigating the construction of cost-effective and easy to use "Reconfigurable Physically Unclonable Functions (rPUF)" that can be physically reconfigured.

A framework offering provable security which is based on physical properties: We aim to discuss appropriate models and methodologies to realize and to analyze the security of resulting cryptographic primitives and security protocols that concern the following aspects:

- Manufacturing security: Preventing/detecting overproduction and ensuring security in the commercial manufacturing environment also under insider threats.
- Identification and evaluation of malicious (Trojan) and unspecified functionality in hardware: Ensuring the trustworthiness and full functionality of security sensitive ICs. Recent research results indicate that new hardware components are required to achieve this goal.
- Anti-Counterfeiting, verifiability and auditability of security critical devices: Investigating hardware and system components that are needed and economically implementable to prevent or detect counterfeited devices.
- Trade-off unique device identification versus privacy: Unique identification of objects stands clearly in contrast with privacy. In particular, in the medical device setting, it is, on the one hand, important to uniquely identify devices for reasons of security and safety, and on the other it is important to provide mechanisms enabling access control to this unique identifying information. This can include merely protecting the existence of the device, device type, or its ID, or the confidential information stored on it or broadcasted by it.
- Dynamic and distributed Trusted Computing: Designing security modules with dynamic trusted computing functionality, i.e., a minimum root of trust both for PC and mobile scenario where various cryptographic functionalities can be securely generated and loaded when needed. In particular we aim at investigating the questions such as what functionality does it really need to be included inside the trust boundary, how can we verify the trusted functionality in a meaningful way and how can we distribute trusted functionality over several ICs on the platform?

The relevance of the previously mentioned problems is only made clearer by looking at recent developments and trends in the commercial deployment of cryptographic hardware. Prominent examples include Intel's Trusted Execution Technology and next generation CPUs, AMD's Presidio, and the TPM (Trusted Platform Module) proposed by the Trusted Computing Group (TCG). Moreover, future generations of CPUs are expected to provide a variety of cryptographic functions, all embedded into a single chip set. Their deployment is also the subject of large European projects such as OpenTC or TECOM.

The goals and challenges mentioned above comply with the objectives and challenges of secure, dependable and trusted infrastructures and bridge the gap between the current black-box security models and the real world we live in. Given recent important advancements and developments in the area of cryptographic hardware that concern many various disciplines, we expected this Dagstuhl seminar to be an appropriate platform for experts from various disciplines to benefit from the mutual exchange of ideas across these research communities. In addition, we hoped that the results of the discussions and interactions during the seminar would become the corner stone in theoretical and practical foundations for forgery-resilient cryptographic hardware.

3 The participants

The seminar counted with the participation of 30 researchers, who are currently working in the following countries:

Belgium(8), Canada (1), Germany (10), Great Britain (1), Israel (1), The Netherlands (2), Poland (1), Switzerland (1) , United States (5)

These researchers brought to the seminar a rich variety of backgrounds in computer science and engineering. These included theoretical and practical cryptography, algorithms design, chip design, VLSI, low power design, system security, security evaluation, side-channel countermeasures and attacks, design of cryptographic primitives for constrained environments, and standardization. The diverse backgrounds created an stimulating atmosphere and allowed for interesting discussions.

4 The program

The program was organized so as to combine theoretical talks describing models to analyze the security of forgery resilient hardware with more practical ones, which describe either the actual implementation of such hardware, its applications, or its security evaluation.

Speakers for the first day (July 6th, 2009)	
Ahmad-Reza Sadeghi	(Ruhr-Universität Bochum, Germany) Foundations for Forgery-Resilient Cryptographic Hardware I
Pim Tuyls	(Intrinsic-ID, The Netherlands) Foundations for Forgery-Resilient Cryptographic Hardware II
Frederik Armknecht	(Ruhr-Universität Bochum, Germany) Memory Leakage-Resilient Encryption based on Physically Unclonable Functions
Boris Škorić	(TU Eindhoven, The Netherlands) An efficient fuzzy extractor for limited noise
G. Edward Suh	(Cornell University, U.S.) Processor Hardware Authentication Leveraging Performance Limits in Detailed Simulations and Emulations

In addition to the formal talks, there were several discussions and active interactions among small groups of participants throughout the duration of the seminar.

Speakers for the second day (July 7th, 2009)	
Francois-Xavier Standaert	(UC Louvain-la-Neuve, Belgium) Leakage resilient cryptography in practice
Markus Kuhn	(University of Cambridge, Great Britain) GNSS signal authentication methods
Stefan Katzenbeisser	(TU Darmstadt, Germany) PUF-Based Authentication Protocols, Revisited
Boris Škorić	(TU Eindhoven, The Netherlands) Simplification of Controlled PUF primitives
Berk Sunar	(Worcester Polytechnic Institute, U.S.) Fingerprints from Optical Discs
Darko Kirovski	(Microsoft Research - Redmond, US) Anti-Counterfeiting: Mixing the Physical and the Digital World
Adi Shamir	(Weizmann Institute, Israel) Trapdoors in Cryptographic Hardware
Jorge Guajardo	(Philips Research Eindhoven, The Netherlands) Medical Applications of PUFs and Other Thoughts on PUFs

Speakers for the third day (July 8th, 2009)	
Jean-Pierre Seifert	(TU Berlin & Deutsche Telekom Labs, Germany) Forgery-resilient Circuit Encoding
Lejla Batina	(KU Leuven, Belgium) Security Challenges for RFID Systems
Patrick Schaumont	(Virginia Polytechnic Institute - Blacksburg, U.S.) Engineering On-Chip Thermal Effects
Philippe Teuwen	(NXP Semiconductors - Leuven, Belgium) How to Make Smartcards Resistant to Hackers' Lightsabers?
Christian Wachsmann	(Ruhr-Universität Bochum, Germany) Enhancing RFID Security and Privacy by Physically Unclonable Functions

5 Concluding Remarks

We found the seminar to be fruitful in the sense that several modeling issues were raised, which we expect will lead the community to understand better the security issues and requirements of forgery resilient hardware. In addition, the participation of both, theoretical computer scientists and more implementation oriented scientists, allowed for a better understanding from both sides: what models are realistic, what needs to be formalized to be able to prove security of an implementation, and what emerging applications of security hardware exist.

Moreover, it appears that the formal modelings of hardware primitives and the subsequent deployment of such hardware will remain hot topics for the next few years. In the future, we plan further workshops to encourage continued interdisciplinary interactions.

The organizers:

Jorge Guajardo
Bart Preneel
Ahmad-Reza Sadeghi
Pim Tuyls