09282 Abstracts Collection
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. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in this paper. The first section describes the seminar topics and goals in general. Links to extended abstracts or full papers are provided, if available.

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

09282 Executive Summary – Foundations for Forgery - Resilient Cryptographic Hardware

From July 5th, 2009 to July 8th, 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.

The Executive Summary describes the goals of the seminar, the topics discussed and provides an overview of the program. The Executive Summary describes the seminar topics and goals in general. Abstracts of the presentations given during the seminar as well as abstracts of seminar results and ideas are put together in the Proceedings. Links to extended abstracts or full papers are provided, if available.

Dagstuhl Seminar Proceedings 09282
Foundations for Forgery-Resilient Cryptographic Hardware
http://drops.dagstuhl.de/opus/volltexte/2010/2407

Keywords: Foundations, forgery resilience, Physical Unclonable Functions (PUFs), modeling, side-channel security models, PUF applications, hardware

Joint work of: Guajardo, Jorge; Preneel, Bart; Sadeghi, Ahmad-Reza; Tuyls, Pim

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2010/2408

Memory Leakage-Resilient Encryption based on Physically Unclonable Functions

Frederik Armknecht (Ruhr-Universität Bochum, DE)

Physical attacks on cryptographic implementations and devices have become crucial. In this context a recent line of research on a new class of side-channel attacks, called *memory attacks*, has received increasingly more attention. These attacks allow an adversary to measure a significant fraction of secret key bits directly from memory, independent of any computational side-channels.

Physically Unclonable Functions (PUFs) represent a promising new technology that allows to store secrets in a tamper-evident and unclonable manner. PUFs enjoy their security from physical structures at sub-micron level and are very useful primitives to protect against memory attacks.

In this talk we present our first steps towards combining and binding algorithmic properties of cryptographic schemes with physical structure of the underlying hardware by means of PUFs. We introduce a new cryptographic primitive based on PUFs, which we call PUF-PRFs. These primitives can be used as a source of randomness like pseudorandom functions (PRFs). We construct a block cipher based on PUF-PRFs that allows simultaneous protection against algorithmic and physical attackers, in particular against memory attacks. While PUF-PRFs in general differ in some aspects from traditional PRFs, we show a concrete instantiation based on established SRAM technology that closes these gaps.

Keywords: PRFs, PUFs, PUF-PRFs, memory leakage, SRAM PUFs, side-channels, memory attacks

Joint work of: Armknecht, Frederik; Maes, Roel; Sadeghi, Ahmad-Reza; Sunar, Berk; Tuyls, Pim

Security Challenges for RFID Systems

Lejla Batina (K.U. Leuven, BE)

In this talk we give an overview of security requirements for RFID systems including scalability, anti-cloning and protection against tracking and impersonation attacks.

We also introduce our novel protocols for security: secure authentication protocols and a secure search protocol. In particular, we discuss several authentication protocols that are all made of the same building blocks but meet different security requirements. This feature allows for a simplified realization of the protocols on a real tag. Our solutions rely exclusively on Elliptic Curve Cryptography (ECC).

In addition, we present our work on an RFID chip with an Elliptic Curve (EC) processor over $GF(2^{163})$. The chip is fabricated in 0.13 um technology and it shows the plausibility of meeting both security and efficiency requirements even in a passive RFID tag.

Keywords: RFID security, authentication protocols, Elliptic Curve Cryptography

Joint work of: Batina, Lejla; Verbauwhede, Ingrid

Medical Applications of PUFs and Other Thoughts on PUFs

Jorge Guajardo (Philips Research - Eindhoven, NL)

The first part of this talk deals with how to make medical data submitted to remote monitoring services more reliable. In particular, remote e-health services are expected to significantly expand in the near future. As a result a multitude of vital body signs will be recorded at a remote location (e.g., at home) and transmitted to a service provider for further processing and assessment. This raises the need for technologies that will allow binding the identity of the person to the measurement, as well as the the measurement to the device performing the measurement. Such technologies would allow proving in an irrefutable manner that a certain measurement corresponds to a particular patient (and not someone else). Furthermore, it would allow healthcare providers to check from which particular device the measurement originates. This supports information reliability allowing healthcare providers to make clinical decisions based on measurements collected by their patients remotely. In this paper, we describe how to achieve this by combining ideas from physical unclonable functions (PUFs) and template protection schemes for biometrics.

The second part of the talk discusses different requirements and properties that different types of PUF and as a result the need for different model capturing these characteristics. In particular, we observe that the identification properties of PUFs that accept a small number of challenges such as SRAM PUFs and Butterfly PUFs, should be modeled so as to capture variability among PUFs instantiations on different devices. Thus, in this case it only makes sense to talk about variability and distribution of PUF outputs across different devices. On the other hand, for PUFs that do accept many (e.g. of the form 2^l for $l \geq 50$) challenges, such as optical PUFs, one may talk of variability across different devices but also for different challenges to a PUF on the same device.

Keywords: PUFs, biometrics, remote health monitoring, authenticity, medical applications, combined fuzzy extractors

Joint work of: Guajardo, Jorge; Asim, Muhammad; Petkovic, Milan

PUF-Based Authentication Protocols, Revisited

Stefan Katzenbeisser (TU Darmstadt, DE)

Classical authentication protocols, where one communication partner proves its identity to another participant, are commonly based on cryptographic primitives. Their security usually relies on a computationally hard problem. Most constructions are based on the possession of a secret key, which is assumed not to fall in the hands of an adversary. However, this assumption may be violated if an adversary has physical access to the device that performs authentication for a short time. In this period, the adversary may read the whole memory of the device including all secret information, unless hardware security measures are taken. With this information, the adversary can finally run an impersonation attack. Such an attack is usually outside of the considered attacker model in classical cryptography. However, in many practical authentication scenarios, this attack is realistic. Consider for example a situation, where a waiter in a restaurant carries a credit card away from the table for billing. During this short time the card is not under full control of the owner and an adversary may read the data of the card memory in order to extract the secret information. Moreover, the card reader is potentially under full control of the adversary. Thus, data stored in the memory of the reader is potentially at risk as well.

Physical Uncloneable Functions (PUFs) were proposed as a building block for authentication schemes that can resist physical attacks. PUFs are physical objects which are unique and uncloneable. Technically speaking, a PUF responds to a stimulus with a physical output (which can be measured and encoded as a bit string) and has the following three properties: First, it is impossible to clone a PUF even with highly complex equipment. Second, it is infeasible to predict the output for a chosen stimulus without physically evaluating the PUF, and third, the output looks random.

Several authors therefore proposed to use PUFs as basic primitives for constructing authentication and key agreement protocols, due to their uncloneability and pseudo-random behavior. However, so far, there is still no acceptable security model that allows to formally prove PUF-based protocols secure. In this talk we give an overview of existing PUF definitions and discuss how they can be extended to a theoretical model of security for PUF-based authentication. Subsequently, we sketch a security problem present in existing authentication protocols that use uncontrolled PUFs.

Keywords: PUF, authentication, security model

Joint work of: Katzenbeisser, Stefan; Busch, Heike; Rührmair, Ulrich

Anti-Counterfeiting: Mixing the Physical and the Digital World

Darko Kirovski (Microsoft Research - Redmond, US)

In this paper, we overview a set of desiderata for building digital anti-counterfeiting technologies that rely upon the difficulty of manufacturing randomized complex 3D objects. Then, we observe how this set is addressed by RF-DNA, an anti-counterfeiting technology recently proposed by DeJean and Kirovski. RF-DNA constructs certificates of authenticity as random objects that exhibit substantial uniqueness in the electromagnetic domain.

Keywords: Certificates of authenticity, RF-DNA, physically unique one-way functions

Full Paper: http://drops.dagstuhl.de/opus/volltexte/2010/2406

GNSS Signal Authentication Methods

Markus Kuhn (University of Cambridge, GB)

In some security-critical applications for satellite-navigation receivers, those in possession of the receiver may have an interest in it producing an incorrect output: vehicle and container tracking, usage-based road charging, prisoner tagging, location-based access control. This talk reports on the ongoing design of a tamper-resistant GPS receiver architecture for such applications, with a particular focus on trust metrics that can be used to distinguish an authentic GPS signal at the RF antenna port from one forged using a signal simulator.

Keywords: GPS, Galileo, tamper-resistant receiver, anti-spoofing, signal simulator

Engineering On-Chip Thermal Effects

Patrick Schaumont (Virginia Polytechnic Institute - Blacksburg, US)

Temperature effects can be used to maliciously affect the behavior of digital crypto-circuits. For example, temperature effects can create covert communication channels, and they can affect the stability of physical unclonable functions (PUFs). This talk observes that these thermal effects can be engineered, and we describe two techniques. The first technique shows how to filter the information through a covert temperature channel. This leads to detectors for very specific events, for example, someone touching the chip package. The second technique shows how to mitigate the impact of temperature on a PUF design while avoiding costly post-processing. We discuss the design of a compact ring-oscillator PUF for FPGA which is tolerant to temperature variations.

Keywords: PUFs, temperature effects, covert temperature channel, ring oscillator PUF, FPGAs

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2010/2403

An efficient fuzzy extractor for limited noise

Boris Škorić (TU Eindhoven, NL)

A fuzzy extractor is a security primitive that allows for reproducible extraction of an almost uniform key from a non-uniform noisy source. We analyze a fuzzy extractor scheme that uses universal hash functions for both information reconciliation and privacy amplification. This is a useful scheme when the number of error patterns likely to occur is limited, regardless of the error probabilities. We derive a sharp bound on the uniformity of the extracted key, making use of the concatenation property of universal hash functions and a recent tight formulation of the leftover hash lemma.

Keywords: Fuzzy Extractor, PUF, physical unclonable function, universal hash

Joint work of: Škorić, Boris; Tuyls, Pim

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2010/2409

Full Paper:
http://eprint.iacr.org/2009/030

Simplification of Controlled PUF primitives

Boris Škorić (TU Eindhoven, NL)

Physical Unclonable Functions (PUFs) are physical objects that are unique, practically unclonable and that behave like a random function when subjected to a challenge. Their use has been proposed for authentication tokens and anti-counterfeiting. A Controlled PUF (CPUF) consists of a PUF and a control layer that restricts a user's access to the PUF input and output. CPUFs can be used for secure key storage, authentication, certified execution of programs, and certified measurements. In this paper we modify a number of protocols involving CPUFs in order to improve their security. Our modifications mainly consist of encryption of a larger portion of the message traffic, and additional restrictions on the CPUF accessibility. We simplify the description of CPUF protocols by using flowchart notation. Furthermore we explicitly show how the helper data for the PUFs is handled.

Keywords: PUF, physical unclonable function, controlled PUF, CPUF

Joint work of: Škorić, Boris; Makkes, Marc X.

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2010/2404

Full Paper:
http://eprint.iacr.org/2009/328

Leakage Resilient Cryptography in Practice

Francois-Xavier Standaert (UC Louvain-la-Neuve, BE)

In this report, we are concerned with models to analyze the security of cryptographic algorithms against side-channel attacks. Our objectives are threefold. In a first part of the paper, we aim to survey a number of well known intuitions related to physical security and to connect them with more formal results in this area.

For this purpose, we study the definition of leakage function introduced by Micali and Reyzin in 2004 and its relation to practical power consumption traces. Then, we discuss the non equivalence between the unpredictability and indistinguishability of pseudorandom generators in physically observable cryptography.

Eventually, we examine the assumption of bounded leakage per iteration that has been used recently to prove the security of different constructions against side-channel attacks. We show that approximated leakage bounds can be obtained using the framework for the analysis of side-channel key recovery attacks published at Eurocrypt 2009.

In a second part of the paper, we aim to investigate two recent leakage resilient pseudorandom generators, both from a theoretical and practical point of view. On the one hand, we consider a forward secure generator from ASIACCS 2008 and its similarities with a previous construction by Bellare and Yee. On the other hand, we analyze Pietrzak's block cipher based construction from Eurocrypt 2009. Doing this, we put forward the difficulty of meaningfully restricting the physical leakages and show that this difficulty leads to different drawbacks. This allows us to emphasize the differences between these two designs. First, one construction that we analyze requires strong black box assumptions (*i.e.* random oracles) - the other one considers unrealistic leakages leading to (possibly useless) performance overheads. Second, one construction considers an adversary able to adaptively choose a leakage function while the second one does not permit this adaptivity. Third, the security proof of the Eurocrypt 2009 construction relies on the assumption that “only computation leaks" (or relaxed but related hypotheses) while this assumption is not necessary for the ASIACCS construction. We then discuss the impact of these hypotheses with respect to recent technological advances.

In the third part of the paper, we show that Pietrzak's leakage resilient mode of operation from Eurocrypt 2009 can be broken with a standard DPA if it is re-initialized without sharing new keys. Then, we propose solutions to fix this issue and extend the initial proposal from ASIACCS 2008 in order to rely on more standard cryptographic constructions. We use these alternative designs to illustrate the incompatibility between a fully adaptive selection of the leakage function and the secure initialization of a pseudorandom generator. We also argue that simple pseudorandom functions (*e.g.* the one of Goldreich, Goldwasser, Micali) can be shown leakage resilient under certain black box assumptions (again, using the random oracle methodology). We additionally discuss the security *vs.* performance trade-off that is inherent to these different schemes and the (im)possibility to obtain similar results with pseudorandom permutations (*e.g.* the one of Luby, Rackoff). Eventually, we show that the security of standard pseudorandom number generators against side-channel adversaries cannot be directly generalized in the standard model. It is an open problem to determine the minimum black box assumptions and restrictions of the leakage function that would be required for this purpose.

Keywords: Side-channel attack security model, assumptions, bounded leakage, leakage resilient PRNGs and modes of operation

Joint work of: Standaert, Francois-Xavier;Pereira, Olivier; Yu, Yu; Quisquater, Jean-Jacques; Yung, Moti; Oswald, Elisabeth

Full Paper:
http://eprint.iacr.org/2009/341

Hardware Authentication Leveraging Performance Limits in Detailed Simulations and Emulations

G. Edward Suh (Cornell University, US)

This talk will present a new approach to check the authenticity of hardware based on the inevitable performance gap between real hardware and simulations or emulations that impersonate it.

More specifically, we demonstrate that each processor design can be authenticated by requiring a checksum incorporating internals of complex micro-architectural mechanisms to be computed within a time limit; this checksum is different for each processor model and only authentic secure hardware can obtain the checksum fast enough.

This new authentication approach provides potential solutions to privacy, scaling, and security issues of traditional approaches that rely only on certificates.

Architectural simulations and an RTL implementation show that the proposed approach is viable with very low hardware overheads.

See also: Dan Deng, Andrew H. Chan, G. Edward Suh, "Hardware Authentication Leveraging Performance Limits in Detailed Simulations and Emulations", to appear in Proceedings of the 46th Design Automation Conference.

Fingerprints from Optical Discs

Berk Sunar (Worcester Polytechnic Institute, US)

In this talk we outline a new technique for extracting unique fingerprints from identical CDs. The proposed technique takes advantage of manufacturing variability found in the length of the CD lands and pits. Although the variability measured is on the order of 20 nm the technique does not require the use of microscopes or any advanced equipment. Instead, the electrical signal produced by the photodetector inside the CD reader will be sufficient to measure the desired variability. We provide empirical evidence obtained by analyzing 100 identical CDs and show how to extract a unique fingerprint for each CD. Furthermore, we introduce a novel technique for utilizing fuzzy extractors over the Lee metric without much change to the typical code offset construction. With the aid of the proposed fuzzy extractor we give specific parameters and code constructions to convert the derived fingerprints into 128-bit cryptographic keys.

Keywords: Discs, fingerprinting, manufacturing variability, copy protection

Joint work of: Hammouri, Ghaith; Dana, Aykutlu

How to Make Smartcards Resistant to Hackers' Lightsabers?

Philippe Teuwen (NXP Semiconductors - Leuven, BE)

Cracking smartcards has always been a prized hobby, for the academic glory , for fun (ha, breaking the self-claimed unbreakable...) and for profit (ask the mafia).

State-of-the-art techniques include laser blasts that inject various transient or permanent faults in a program execution, potentially making the smartcard do whatever the attacker wants.

After a brief recap of the attack tools and their effects, we'll see how the programmer can protect his code with software techniques ranging from cookbook recipes to tool chain automation and how he can evaluate the robustness of his code by means of fault injection simulators.

Keywords: Fault-injection, smartcard, simulator

Extended Abstract: http://drops.dagstuhl.de/opus/volltexte/2010/2401

Foundations for Forgery Resilient Cryptographic Hardware

Pim Tuyls (Intrinsic-ID - Mol, BE)

Counterfeiting of goods in general and of electronic goods in particular is a growing problem with a huge impact on the global economy, the society and the security of its critical infrastructure.

Various examples are known where companies suffer from economic and brand damage due to competition with counterfeit goods. In some cases the use of counterfeit components has even led to tragic accidents in which people are killed. Finally, it has been shown that counterfeit products can penetrate the critical and security infrastructure of our modern societies and hence cause a threat to the national security. One of the difficulties to deal with this problem stems from the fact that counterfeit goods can originate from sources that are able to make copies that are very hard to distinguish from their legitimate counterpart. A first well-known aspect of counterfeiting is product cloning. A second much less known but increasingly dangerous aspect consists of over-production of goods. In order to deal with these two aspects of counterfeiting a secret unclonable identifier is required together with strong cryptographic protocols. In this paper we focus on a new way to deal with these problems: Hardware Intrinsic Security. It is based on the implementation and generation of secret physically unclonable identifiers. Some important examples will be presented and their implementation, reliability and security aspects are discussed.

Keywords: Counterfeiting of goods, product cloning, overproduction, Hardware Intrinsic Security

Joint work of: Handschuh, Helena; Tuyls, Pim

Enhancing RFID Security and Privacy by Physically Unclonable Functions

Christian Wachsmann (Ruhr-Universität Bochum, DE)

RFID-enabled systems allow fully automatic wireless identification of objects and are rapidly becoming a pervasive technology with various applications. However, despite their benefits, RFID-based systems also pose challenging risks, in particular concerning user privacy.

Indeed, improvident use of RFID can disclose sensitive information about users allowing the creation of detailed user profiles. Hence, a careful analysis in appropriate security and privacy models is needed before deployment to practice. Moreover, most RFID chips are computational and memory constrained devices without protection against physical tampering. Thus, existing, usually computationally demanding privacy-protecting schemes cannot be applied while physical attacks that reveal the tag secrets impede the use of symmetric-key based techniques. Hence, the design of a *usable* privacy-preserving RFID protocol currently is a challenging open problem. In this context, Physically Unclonable Functions (PUFs) provide cost-efficient means to fingerprint chips based on their physical properties and can be used to realize tamper-evident storage for cryptographic secrets.

Recently, Vaudenay presented a comprehensive RFID security and privacy framework that captures authentication of tags to readers and anonymity aspects (Vaudaney, 2007). This framework defines eight privacy notions that correspond

to adversaries of different strength, i.e., that differ in their ability to access the secrets of (i.e., to corrupt) tags and to obtain auxiliary information from tag to reader communication.

We will present an efficient privacy-preserving PUF-based RFID protocol that addresses Vaudenay's open question on the feasibility of *destructive privacy*, i.e., privacy of tags that are destroyed during corruption. This means that our protocol provides untraceability of tags against adversaries that permanently destroy a tag by physically attacking (i.e., corrupting) it. It is based on the weak private protocol proposed in (Vaudenay, 2007) and uses Physically Unclonable Functions (PUFs) as tamper-evident key storage in a similar way as described in (Tuyls, P. and Batina, L., 2006). This means that the tag authentication key is not stored on the tag but reconstructed from the physical characteristics of the RFID chip each time it is needed. The properties of the PUF ensure that any attempt to physically tamper with the PUF to obtain the authentication secret of the tag result in destruction of the PUF and the tag secret, which corresponds to the definition of a destructive adversary in the security and privacy model of (Vaudenay, 2007).

Keywords: PUFs, RFID, chip fingerprinting, privacy preserving authentication RFID protocols

Joint work of: Wachsmann, Christian; Sadeghi, Ahmad-Reza; Visconti, Ivan