SAFEST SUMMER SCHOOL

SAFEST

PROGRAM

June 8-10, 2022

LIRMM, Montpellier, France

Detailed Program

Wednesday, June 8th

08 :45-09 :00 Marie-Lise Flottes, LIRMM, Samuel Pagliarini, TalTech
Opening

09 :00-10 :00 Samuel Pagliarini, TalTech
"A Tutorial on Design Obfuscation: from Transistors to Systems"

Samuel Pagliarini received the PhD degree from Telecom ParisTech, Paris, France, in 2013. He has held research positions with the University of Bristol, Bristol, UK, and with Carnegie Mellon University, Pittsburgh, PA, USA. He is currently a Professor at Tallinn University of Technology (TalTech) in Tallinn, Estonia where he leads the Centre for Hardware Security. He is also the SAFEST coordinator.

The recent advances in the area of design obfuscation are encouraging, but may present themselves as hard to interpret at times. This tutorial covers advances in design obfuscation in a clear language, contrasting the approaches that can be implemented at layout level, in the netlist of a circuit, or even at chip level. This tutorial also highlights the available support, both from the tooling side and the logistics of fabricating an obfuscated integrated circuit today.

10:00-10:15 Break

10:15-11:15 Levent Aksoy, TalTech
"Behavioral obfuscation"
Levent Aksoy received his M.S. and Ph.D. degrees in electronics and communication engineering and electronics engineering from Istanbul Technical University (ITU), Istanbul, Turkey, in 2003 and 2009, respectively. He worked as a researcher in ITU and INESC-ID, Lisbon and as a digital design engineer at Dialog Semiconductor. Currently, he is a postdoctoral researcher in TalTech Tallinn University of Technology. His research interests include hardware security and CAD for VLSI circuits with emphasis on solving EDA problems using SAT models and optimization techniques.

While the globalization of the integrated circuit (IC) supply chain reduces the cost and time spent for generating an IC, it introduces security and privacy threats, especially for intellectual properties (IPs). In this course, we ***focus on*** *the* ***behavioral obfuscation techniques*** *developed for IP protection* ***which can take place at high-level synthesis (HLS) and register transfer level (RTL)****. This course initially gives background concepts on IP threats in the IC design flow and HLS. Then, it presents prominent behavioral obfuscation techniques, which can handle designs under different description formats, and briefly describes their flows, strategies, and impact on the design overhead. It also describes de-obfuscation methods, which can be applied to designs obfuscated by the proposed techniques, and presents their performance on the designs obfuscated at HLS and RTL. Finally, it summarizes the research on the behavioral obfuscation and highlights the challenging problems.*

11:15-11:30 Break

11:30-12:30 Jaan Raik, TalTech
"Architectural side-channels and vulnerabilities"

Prof. Raik received his M.Sc. and Ph.D. degrees at Tal Tech in 1997 and in 2001, respectively. He has co-authored more than 200 peer-reviewed scientific publications. His research interests cover a wide area in electrical engineering and computer science domains including hardware test, functional verification, fault-tolerance and security as well as emerging computer architectures. He is a member of IEEE Computer Society, HiPEAC and a member of steering/program committees of several leading conferences in his fields. He acted as the General Co-Chair of IEEE European Test Symposium 2020, the General Chair of the IFIP/IEEE VLSI-SoC'16 and IEEE DDECS'12 Conferences and the Program Co-Chair of CDN-Live'16 and the Program Chair of IEEE DDECS'15. He was the main coordinator for several Europe-wide research and collaboration actions, including Horizon 2020 RIA IMMORTAL, Widening Twinning TUTORIAL and FP7 Collaborative Research DIAMOND. He has also acted as the local lead for the FP6 STREP VERTIGO and FP7 Collaborative Research BASTION. He has been awarded the national Young Scientist Award (2004), Estonian Academy of Science's Bernhard Schmidt Award for innovation (2007) and the Order of the White Star 4th class medal by the President of Estonia (2016). 15 PhD Theses have been successfully defended under his supervision.

The talk will present cache-side channel attacks as a special case of architectural attacks and vulnerabilities. First, the basics of architectural attacks is given. It will be explained how the architectural attacks work on shared caches and an overview of related known threat models and attacks is provided. Then, existing models to represent such threats is given. Finally, the presentation explains how to monitor cache side-channel attacks and provides an overview of ways to mitigate them.

12:30-14:00 Lunch Time

14:00-15:30 Alex Hepp and Patrick Karl, TUM
"RISC-V: Security with and in an Open Source Instruction Set"

Alexander Hepp received M.S. in electrical and computer engineering from Technical University of Munich, Germany in 2019. Currently he is a research assistant and doctoral candidate at the Chair of Security in Information Technology at the Technical University of Munich. His current research focuses on silicon hardware design, reverse engineering for secure open-source systems, hardware obfuscation and the detection of hardware Trojans through machine learning.

Patrick Karl is a doctoral candidate at the Chair of Security in Information Technology at Technical University of Munich, Germany. He obtained his B.Sc. and M.Sc. at the same university in 2018 and 2020, respectively.His research interests include hardware implementations of post-quantum cryptography and in particular, hardware/software codesigns based on RISC-V platforms.

Dedicated hardware accelerators as well as ISA extensions for cryptographic applications can be integrated and evaluated. Furthermore, the open-source character allows independent researchers to review and analyze specific implementations with respect to security issues.In the first part of this talk, *we give an introduction into RISC-V and explain, how processors can be customized specifically for cryptographic applications. Different approaches and their corresponding pros and cons are discussed.*

15:30-15:45 *Break*

15:45-17:15 Alex Hepp and Patrick Karl, TUM
"RISC-V: Security with and in an Open Source Instruction Set" (cont'd)

In the second part, we inspect how open-source ISAs and processors enable improved, as well as diminished (can impact)security. Detailed insights into the inner workings of hardware designs allow (reverse-engineering-based) inspection for vulnerabilites such as hardware trojans. But at the same time, the deep understanding also allows to compose attacks more easily. We will try out reverse engineering methods and threat analysis techniques on a toy example and perform our own RISC-V IP attack.

17:00 *Contest -1st Round- : "who can find the key?" or how to introduce information security to undergraduate students, Florent Bruguier, LIRMM*

Thursday, June 9th

09 :00-10 :30 Sujoy SINHA ROY, TU Gratz
"Post quantum cryptography"

Sujoy Sinha Roy is an assistant professor at IAIK, the Graz University of Technology. He works on secure and efficient implementation of cryptographic algorithms on hardware and software platforms. His doctoral thesis was awarded the 'IBM Innovation Award 2018' that recognizes an outstanding doctoral thesis in informatics. He is a co-designer of 'Saber' which is a finalist in NIST's Post-Quantum Cryptography Standardization Project.

If a sufficiently powerful quantum computer is ever constructed, then the most widely used public-key cryptographic algorithms, namely the RSA and Elliptic-Curve Cryptosystems, can be broken efficiently using thor's quantum algorithm. Post-quantum cryptography is a branch of cryptography that focuses on designing new cryptographic schemes that will remain secure against quantum attacks.
In this 3 hours long tutorial, I will give an overview of the implementation aspects of post-quantum cryptography. with a focus on code-based and lattice-based post-quantum cryptography. Side-channel attacks and countermeasures will be discussed.

10:30-10:45 *Break*

10:45-12:15 Sujoy SINHA ROY, TU Gratz
"Post quantum cryptography" (cont'd)

12:15-14:00 *Lunch Time*

14:00-15:00 Milos Grujic, KUL
"Introduction to PUFs"

Milos Grujic received his B.Sc. and M.Sc. degrees in electrical engineering from the University of Belgrade - School of Electrical Engineering. He is final-year PhD student at the COSIC research group, the Department of Electrical Engineering (ESAT), KU Leuven, Belgium. His main research interests include true random number generators (RNGs), randomness extractors, hardware implementations of cryptographic primitives and physically unclonable functions (PUFs).

Providing high-quality, secure keys without secure non-volatile memories (NVM) is a difficult task. As a potential solution to this problem, constructions called physically unclonable functions (PUFs) have been proposed. PUFs are hardware-entangled security anchors based on inherent manufacturing variations that provide intrinsic security properties. In this presentation, we discuss the essential properties of PUFs and explain two design flavors - weak and strong PUFs. We discuss the most representative PUF circuit designs of both flavors, such as SRAM and Arbiter PUFs. We also explain different methods to increase PUFs' reliability and how the appropriate helper data algorithms can be used to make PUFs suitable for authentication as well as key generation.

15:00-15:15 Break

15:15-16:15 Florent Bruguier, LIRMM
"Tutorial on Rowhammer and Countermeasures"

Florent Bruguier received a M.S. and PhD degrees in Microelectronics from the University of Montpellier, France, in 2009 and 2012, respectively. In 2015, he joined the ADAC Team at LIRMM as an Associate Professor. Since 2016, he has been in charge of the SECNUM Platform, a platform dedicated to the side-channel attacks. His research interests include self-adaptive and secured approaches for embedded and high-performance systems.

In this talk, we focus on the principle of Rowhammer attacks and the related countermeasures. These attacks rely on the corruption of DRAM memories. After a short overview of memory hierarchy organisation in modern computer, we introduce DRAM subsystem organization. Then, we elaborate about the attack and its implementation on several platforms and several DRAM technologies [1]. We present the most promising countermeasures both at software and hardware level [2-3]. Finally, to develop new solutions, a simulator is proposed [4].

[1] Kim, Jeremie S., et al. "Revisiting rowhammer: An experimental analysis of modern dram devices and mitigation techniques." 2020 ACM/IEEE 47th Annual International Symposium on Computer Architecture (ISCA). IEEE, 2020.
[2] Park, Yeonhong, et al. "Graphene: Strong yet lightweight row hammer protection." 2020 53rd Annual IEEE/ACM International Symposium on Microarchitecture (MICRO). IEEE, 2020.
[3] Yağlikçi, A. Giray, et al. "Blockhammer: Preventing rowhammer at low cost by blacklisting rapidly-accessed dram rows." 2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA). IEEE, 2021.

[4] France, Loïc, et al. "Implementing Rowhammer Memory Corruption in the gem5 Simulator." 32nd International Workshop on Rapid System Prototyping (RSP). IEEE, 2021.

16:30 *Contest -2nd round-: "Prison Island", Dinner*

Friday, June 10th

09 :00-10 :00 Benedikt Gierlichs, KUL
"DPA and side channel attacks"

Dr Benedikt Gierlichs received a MSc degree in IT Security Engineering from the University of Bochum (Germany) in 2006 and a PhD degree from the electrical engineering department of the KU Leuven (Belgium) in 2011. He is a research expert in the COSIC (Computer Security and Industrial Cryptography) research group at KU Leuven in Belgium. He works with the embedded security group and leads the attacks and evaluations team. His research focuses on the (physical) security of embedded devices.

After summarizing the basics of side-channel analysis we will introduce the classical Differential Power Analysis (DPA) and explain it in several different ways. Then we discuss strengths and weaknesses of DPA. Finally we introduce improved variants of DPA such as Correlation Power Analysis (CPA) and discuss their strengths and weaknesses.

10:00-10:15 *Break*

10:15-11:15 Benedikt Gierlichs, KUL
"DPA countermeasures"

We begin by identifying critical links that enable side-channel analysis. Then we introduce and discuss various countermeasures that aim to break these links in order to protect against side-channel attacks.

11:15-12:30 *Lunch Time*

12:30-14:30 Florent Bruguier, LIRMM
DPA platform and demonstrator

In this presentation, we use the SECNUM platform [1] to demonstrate a side-channel attack. This attack targets an hardware implementation on FPGA of the AES algorithm. The last round and an Hamming distance model are considered. Measurements and associated techniques are performed in real time by the students before programming the attack. Finally, guessing entropy model is introduced and implements for this target.

[1] Bourrée, Morgan, et al. "Secnum: an open characterizing platform for integrated circuits." European Workshop on Microelectronics Education (EWME). 2012.

14:30-14:45 Break

14:45-16:45 Samuel Pagliarini, Felipe Almeida, Mohammad Eslami, Tiago Perez, TalTech
"Beating the ISPD'22 contest: security closure"

For the first time, the ISPD'22 design contest had a theme related to hardware security. Teams had to design circuits that would withstand both hardware trojan insertion and fault injection attacks. In this talk, the TalTech team will share the lessons learned during the 8-week long contest, including the dozens of techniques that were explored to harden designs during physical synthesis.

16:45-17:00 Marie-Lise Flottes, LIRMM
Closing

Program at a glance

	Wenesday June 8th	Thursday June 9th	Friday June 10th
08:00			
08:15			
08:30			
08:45	Intro		
09:00	A Tutorial on Design Obfuscation: from Transistors to Systems, Samuel Pagliarini, TalTech	Post quantum cryptography, Sujoy SINHA ROY, TU Gratz	DPA and side channel attack Benedikt Gierlichs, KUL
09:15			
09:30			
09:45			
10:00	Break		Break
10:15	Behavioral obfuscation, Levent Aksoy, TalTech		DPA countermeasures Benedikt Gierlichs, KUL
10:30		Break	
10:45		Post quantum cryptography, Sujoy SINHA ROY, TU Gratz	
11:00			
11:15	Break		Lunch time
11:30	Architectural side-channels and vulnerabilities, Jaan Raik, TalTech		
11:45			
12:00			
12:15		Lunch time	
12:30	Lunch time		DPA platform and demonstrator Florent Bruguier, LIRMM
12:45			
13:00			
13:15			
13:30			
13:45			
14:00	RISC-V: Security with and in an Open Source Instruction Set, Alex Hepp and Patrick Karl, TUM	Introduction to PUFs , Milos Grujic, KUL	
14:15			
14:30			Break
14:45			Beating the ISPD'22 contest: security closure, Samuel Pagliarini, Felipe Almeida, Mohammad Eslami, Tiago Perez, TalTech
15:00		Break	
15:15		Tutorial on Rowhammer and Countermeasures, Florent Bruguier, LIRMM	
15:30	Break		
15:45	RISC-V: Security with and in an Open Source Instruction Set, Alex Hepp and Patrick Karl, TUM (cont'd)		
16:00			
16:15			
16:30		Social Event	
16:45			Closing
17:00	Welcom Drink		
17:15			
17:30			
17:45			
18:00			
18:15			
18:30			
18:45			
19:00			
19:15			
19:30			
19:45			
20:00			