SAFEST NEWSLETTER

ISSUE NO 3 | JUNE 2022

SAFEST

OUR PROJECT

The overall aim of SAFEST is to enhance the scientific and technological capacity of Tallinn University of Technology (TalTech) in the field of Hardware Security, to be achieved through networking activities with its internationally leading Twinning partners: CNRS/UM, KU Leuven, TUM and TU Graz.

To achieve this, the 3-year project from 2021 to 2023 builds upon the existing strong competences of TalTech in closely related fields, to be complemented by the specific know-how of the Twinning partners in test for security, reverse engineering and defenses, side channel attacks, and hardware-software architectural vulnerabilities.

MONTPELLIER SUMMER SCHOOL

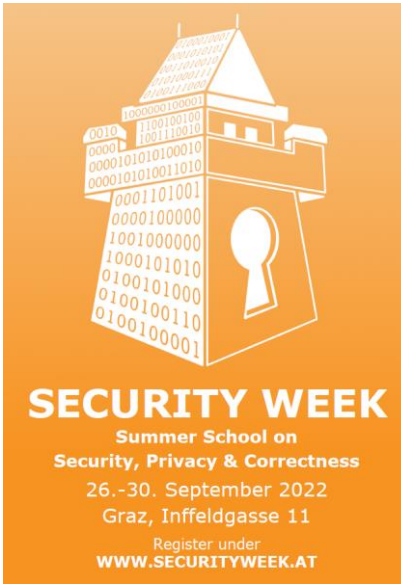
The SAFEST consortium was (finally!) able to hold one of its planned events in a non-virtual setting. Between June 8 and June 10, 30 project members met in Montpellier, France for a 3-day program filled with exciting tutorials and lectures on hardware security.

The topics included obfuscation, side-channels, vulnerabilities, RISC-V security, cryptography and much more. Talks were presented by Samuel Pagliarini, Levent Aksoy, Jaan Raik from TalTech, Alex Hepp and Patrick Karl from TUM, Sujoy Sinha Roy from TU Graz, Milos Grujic and Benedikt Gierlichs from KUL, Marie-Lise Flottes and Florent Bruguier from LIRMM (UM).

Event information and materials are available at https://safest.taltech.ee/events/safest-summer-school-june-8-10/

GRAZ SUMMER SCHOOL

The second SAFEST event of 2022 takes place as the 4th School on Security & Correctness 2022, held from the 26th to the 3th of September, hosted by the Institute of Applied Information Processing and Communication (IAIK) at Graz University of Technology. The school targets PhD students and final year master's students in cryptology, privacy, IT security, and formal methods. Introductory classes are supplemented by advanced courses and practical lab sessions. Therefore, the attendees will get the 'big picture' where theory and practice intersect. Students are encouraged to present their current research topics in a special PhD Forum.



Topics of the school are:

- Runtime Security
- Side-channels
- Privacy
- Secure cryptographic primitives and implementations

Among the speakers there are **Roderick Bloem**, Ilaria Chillotti, Thomas Eisenbarth, Andrea Fioraldi, Anders Fogh, Daniel Gruß, Matteo Maffei, Elisabeth Oswald, **Samuel Pagliarini**, **Michael Pehl**, Peter Schwabe and others.

Registration information: https://securityweek.at/2022/registration/ NB! SAFEST-related participants are exempt from the registration fee – there's an option to mark that at registration time.

PROJECT REVIEW MEETING

The SAFEST project's midterm Review Meeting with the European Commission (EC) took place online on June 14, 2022, with the participation of representatives from all members of the consortium.

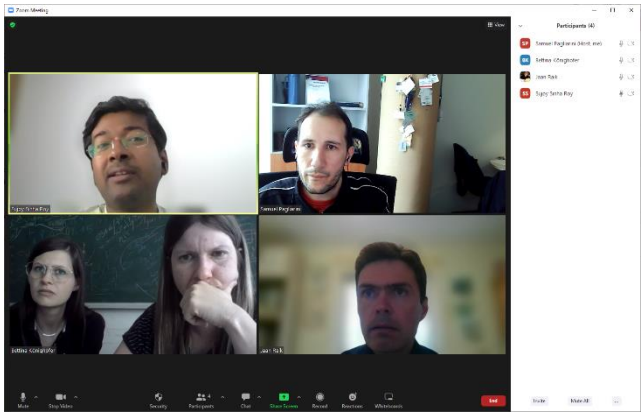
The project's progress was discussed by each work package. The meeting participants discussed the technical and financial matters, and answered the EC's questions based on the freshly submitted Periodic Report. All project activities are on track despite the corona pandemic having forced to alter the form of most staff and ESR exchanges. The project is generally well on track to achieve its objectives.

STAFF AND ESR EXCHANGES

SAFEST **staff exchanges** continued strong despite corona-pandemic having forced most of them to be online. In the 1st half of 2022, (Jan-June) 19 meetings took place with Staff participation from all 5 partners. We have also had two physical site visits: one to KU Leuven and one to TU Graz.

Now is the time to plan more on-site visits!

All these meetings are listed on SAFEST website at https://safest.taltech.ee/exchanges-2022/.

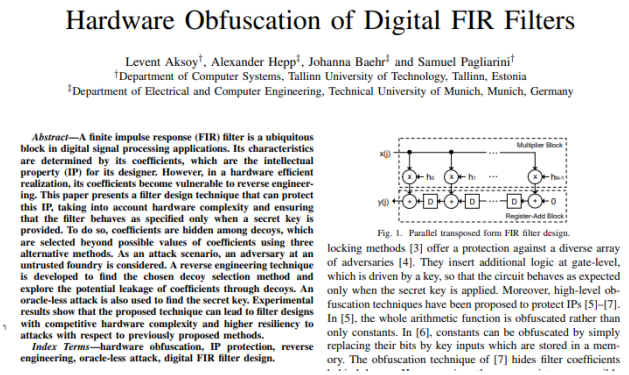


Similarly, 24 **ESR exchanges** continued in 2022 in virtual format.

Details about these meetings, like topic, time, host and number of participants, can be found on the same aforementioned webpage https://safest.taltech.ee/exchanges-2022/.

NEW PUBLICATIONS

A conference paper titled "Hardware Obfuscation of Digital FIR Filters", joint-authored by partners of the SAFEST project, has been recognized with the **best paper award** at the 25th edition of DDECS. The paper was authored by Levent AKSOY (TalTech), Alexander HEPP (TUM), Johanna BAEHR (TUM), and Samuel PAGLIARINI (TalTech). The paper is already available on arXiv as a preprint: https://arxiv.org/abs/2202.10022. Congratulations to all authors!



Hardware Obfuscation of Digital FIR Filters

Levent Aksoy†, Alexander Hepp‡, Johanna Baehr‡ and Samuel Pagliarini†
†Department of Computer Systems, Tallinn University of Technology, Tallinn, Estonia
‡Department of Electrical and Computer Engineering, Technical University of Munich, Munich, Germany

***Abstract*—A finite impulse response (FIR) filter is a ubiquitous block in digital signal processing applications. Its characteristics are determined by its coefficients, which are the intellectual property (IP) for its designer. However, in a hardware efficient realization, its coefficients become vulnerable to reverse engineering. This paper presents a filter design technique that can protect this IP, taking into account hardware complexity and ensuring that the filter behaves as specified only when a secret key is provided. To do so, coefficients are hidden among decoys, which are selected beyond possible values of coefficients using three alternative methods. As an attack scenario, an adversary at an untrusted foundry is considered. A reverse engineering technique is developed to find the chosen decoy selection method and explore the potential leakage of coefficients through decoys. An oracle-less attack is also used to find the secret key. Experimental results show that the proposed technique can lead to filter designs with competitive hardware complexity and higher resiliency to attacks with respect to previously proposed methods.**

***Index Terms*—hardware obfuscation, IP protection, reverse engineering, oracle-less attack, digital FIR filter design.**

Fig. 1. Parallel transposed form FIR filter design.

locking methods [3] offer a protection against a diverse array of adversaries [4]. They insert additional logic at gate-level, which is driven by a key, so that the circuit behaves as expected only when the secret key is applied. Moreover, high-level obfuscation techniques have been proposed to protect IPs [5]–[7]. In [5], the whole arithmetic function is obfuscated rather than only constants. In [6], constants can be obfuscated by simply replacing their bits by key inputs which are stored in a memory. The obfuscation technique of [7] hides filter coefficients