SAFEST NEWSLETTER

ISSUE NO 2 | FEBRUARY 2022

SAFEST

- FIRST SUMMER SCHOOL
- HIGHLIGHTED RESEARCH
- EXCHANGES IN YEAR 1
- YEAR 2 ACTIVITIES

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.

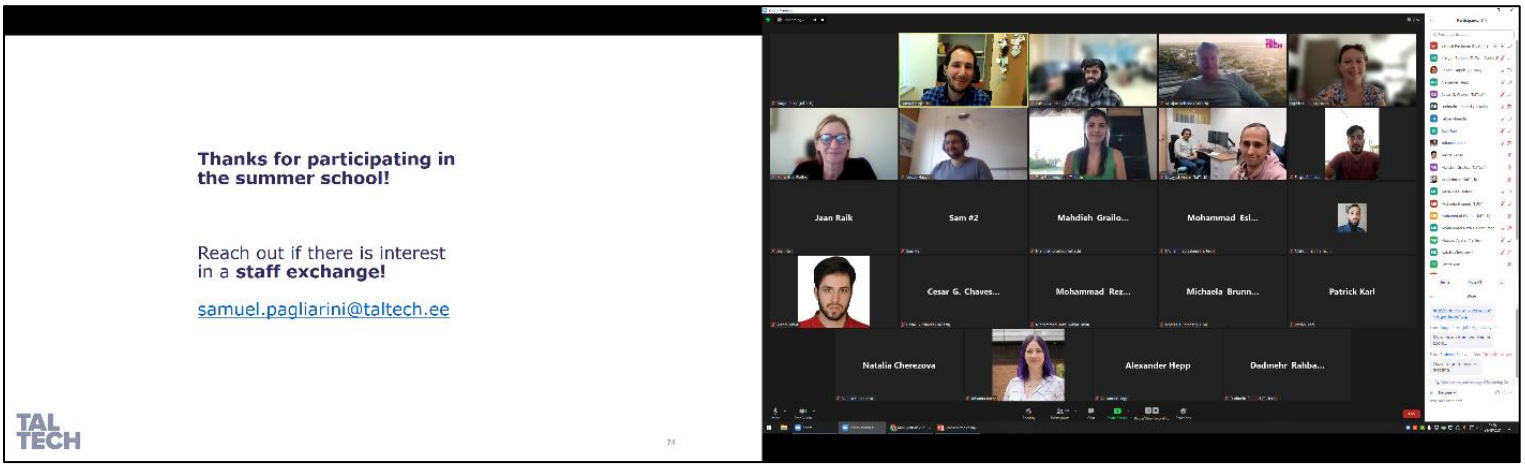
To achieve this, the 3 year project from 2021 to 2023 will build upon the existing strong competences of TalTech in closely related fields, to be complemented by the specific know-how of the Twinning partners in test for security, reverse engineering and defences, side channel attacks, and hardware-software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

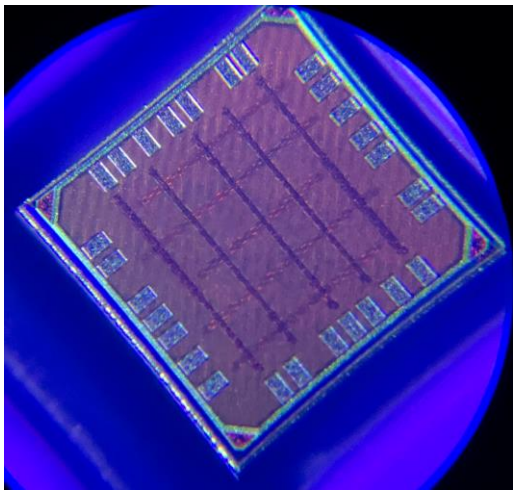
FIRST SUMMER SCHOOL

The first SAFEST Summer School took place online on September 27-28, 2021. It was postponed several times until the September dates were settled upon, because it was hoped with the alleviation of coronavirus infection rates in the summer to organise the event as a physical gathering, while the negative trends from as early as July first forced to postpone the summer school, and then eventually to organise it in virtual format.

Nevertheless, the summer school was a success and fulfilled its goals. It was attended by more than 30 participants, including 19 ESRs and students from project partner universities (including 12 from TalTech, 5 from TUM, 2 from KUL, 1 from TUG, and 1 from CNRS). Over the course of two days, it featured lectures form the key people of all the SAFEST project partners. The course materials covered the very latest findings on Hardware Security including the following topics:

- Hardware trust: protections against hardware Trojans and overproduction,
- Test and testability for digital designs and related security issues,
- Hardware reverse engineering: from chip to RTL and beyond,
- Side channel attacks,
- Verifying resilience against power side channel attacks, and
- Chips on the cheap.





HIGHLIGHTED RESEARCH

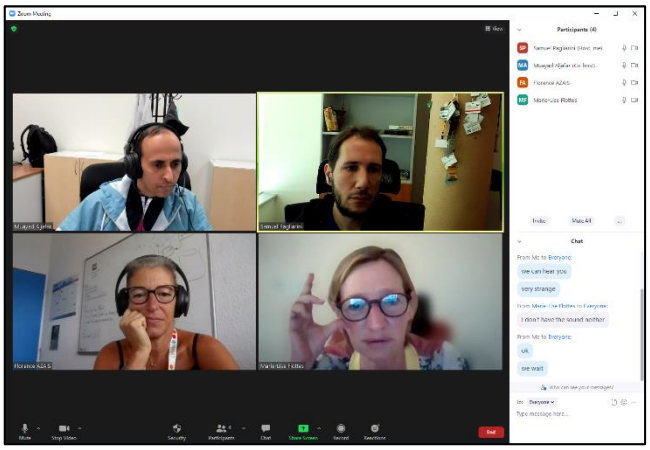
The picture on the left is of a 65nm chip developed by TalTech and TU Graz. Measuring 1mm x 1mm, the chip implements the SABER post-quantum Key Encapsulation Mechanism. The design has been sent for fabrication in September 2021 and was tested in early 2022.

More details about the work can be found on https://dl.acm.org/doi/10.1145/3474376.3487278

EXCHANGES IN YEAR 1

The aim of SAFEST exchanges is to enhance the scientific and technological capacity of TalTech in the field of Hardware Security subtopics (with partners leading in respective competencies):

1. Test for security (CNRS),
2. Reverse engineering and defences (TUM),
3. Side channel attacks (KU Leuven),
4. Hardware-software architectural vulnerabilities (TU Graz).



Due to circumstances with coronavirus pandemic, most of the SAFEST project short-term **staff exchanges** took place in virtual format, i.e. on collaboration platforms such as Teams, Zoom, etc. In total, 74 meetings took place online in 2021 hosted by all 5 partners and attended by 7 staff members from TalTech, 4 from CNRS, 5 from KUL, 4 from TUM and 2 from TUG. All these meetings are listed on SAFEST website at https://safest.taltech.ee/exchanges-2021/.

During very short periods of time, whenever there was a possibility for physical exchanges between SAFEST partners, four site visits took place, and so both TUM and CNRS/UM hosted two visitors from TalTech.

Likewise, most of the SAFEST project short-term **ESR exchanges** took place in virtual format. In total, 65 meetings took place online in 2021 hosted by all 5 partners and attended by 12 ESRs from TalTech, 1 from CNRS, 10 from KUL, 12 from TUM and 5 from TUG. 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-2021/.

The project also managed to carry out three physical short-term ESR exchanges in the 2nd half of 2021: one to TUM, one to CNRS, and one hosted by TalTech.

YEAR 2 ACTIVITIES

Year 2 of our project is here, which means that in addition to continuing with numerous staff and ESR exchanges both in person and online, we have two events to organize: a summer school and a workshop. The plan is to hold the summer school in **Montpellier** on **June 8-10, 2022**. Please save the date for now! We will continue to monitor the pandemic situation and the viability of the summer school as a physical event.

The 2022 workshop is planned for the second semester and will take place in **Tallinn** if the conditions allow.