



Horizon 2020

The EU Framework Programme for
Research and Innovation



SAFEST

D4.5 Project newsletters

Project acronym: SAFEST

H2020 Call: H2020-WIDESPREAD-2020-5

Grant Agreement: 952252

Deliverable Lead: TalTech

Submission Date: 13 December 2023

Dissemination Level: Public

Status: Final

Document Information

Deliverable ID:	D4.5
Deliverable Name:	Project newsletters
Due Date of Deliverable:	M36, 31 December 2023
Actual Submission Date:	M36, 13 December 2023
Work Package:	WP4
Lead Organisation for Deliverable:	KU Leuven
Author(s):	Samuel Pagliarini (TalTech)

Abstract

The deliverable describes the aim and target audience of the SAFEST project's newsletters, tracks the pieces of information shared through the newsletter over the duration of the project.

Disclaimer

The views represented in this document only reflect the views of the authors and not the views of the European Union. The European Union is not liable for any use that may be made of the information contained in this document.

Furthermore, the information is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user of the information uses it at its sole risk and liability.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the SAFEST consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the SAFEST Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the SAFEST Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Status

This deliverable is subject to final acceptance by the European Commission.

Table of Contents

1. Introduction	4
2. Target Audience	4
3. Newsletter contents	5
4. Appendices	6
4.1. SAFEST Newsletter #1 (June 2021)	6
4.2. SAFEST Newsletter #2 (February 2022)	7
4.3. SAFEST Newsletter #3 (June 2022)	8
4.4. SAFEST Newsletter #4 (February 2023)	9
4.5. SAFEST Newsletter #5 (June 2023)	10
4.6. SAFEST Newsletter #6 (December 2023)	11

1. Introduction

Part of the SAFEST project's dissemination and outreach activities in Work Package 4 (WP4) were 1-2 newsletters per year over the duration of the project. Project newsletters were used to record noteworthy accomplishments, list recent activities, publications, and exchanges, as well as announce upcoming events. The main distribution channels were the SAFEST mailing lists, while the PDF-files were also published on the SAFEST website giving it a wider readership than the list-subscribers. There were 6 newsletters published on average every 6 months. The autumn-winter newsletters usually fell into February, which is the reason the final year has 3 issues in order to publish the last issue before the end of the project on Dec 31, 2023.

This deliverable gives an overview of the target audience and distribution channels, the main topics and contents of the newsletters, as well as the copies of the newsletters in the appendices.

2. Target Audience

The main distribution channel for the newsletters were the project mailing lists for PIs and others (mostly ESRs), respectively safest-pi@lists.ttu.ee and safest-all@lists.ttu.ee. The former had 14 subscribers and the latter 71 subscribers (as of December 2023). All newsletters were sent out via mailing-list first before posting them to the website.

The secondary distribution channel was the [SAFEST website](https://safest.taltech.ee) (see Figure 1) where all the newsletters were published shortly after mailing them out. The website had an added benefit of archiving all the newsletters in one place for public access at <https://safest.taltech.ee/research/>. The website was designed to be an information platform for those who would like to know more about the project. with target audiences including such categories as:

- EU organisations involved in research and innovation in the field of computer hardware security;
- Scientists focused on such hardware security research subtopics as testing for security, reverse engineering and defences, side channel attacks, hardware-software architectural vulnerabilities, etc.;
- Representatives from the industry interested in the results of the project;
- Other stakeholders;
- Events (both physical and virtual) participants;
- General public without scientific background.

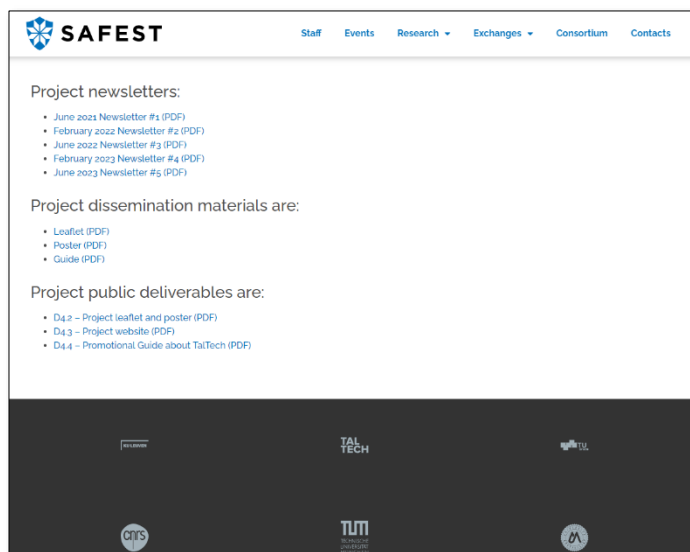


Figure 1 - Newsletters on the SAFEST website (screenshot from Nov 24, 2023)

3. Newsletter contents

The SAFEST newsletters served the aim of informing the stakeholders and the public of the project's past and upcoming activities. Each newsletter contained 4-6 news items on 3-4 pages, mostly looking back into the period since the last newsletter, but occasionally also announcing upcoming events. There were no fixed news sections, but most of the newsletters included updates about

- Staff exchanges,
- ESR exchanges,
- Highlighted research,
- New publications, and
- Events.

Apart from the regular news items, the newsletters also featured short articles about one-off events like the launch of website and YouTube channel, project review at midterm or wrap-up of the SAFEST project.

The newsletter used consistently the same design template that was compiled for the first issue and stemmed from the colour scheme and visual identity of the SAFEST project. The newsletter was published only in English.

4. Appendices

4.1. SAFEST Newsletter #1 (June 2021)

SAFEST NEWSLETTER
ISSUE NO 1 | JUNE 2021

SAFEST

- KICK-OFF
- FIRST WORKSHOP
- FIRST JOINT PUBLICATION
- WEBSITE AND YOUTUBE CHANNEL
- STAFF AND RESEARCHERS' EXCHANGES
- DISSEMINATION MATERIALS

OUR PROJECT

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

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

ISSUE NO 1 | JUNE 2021 PAGE 2

KICK-OFF

SAFEST project's kick-off took place on 8 January 2021 via Zoom and was attended by all key senior personnel from all partners, EC/REA representatives, and PhD students and postdoctoral researchers from different groups or listeners. The project coordinator gave an overview of the SAFEST project while project officer Alina-Varia Bercea introduced EC/REA view on H2020 projects. TallTech was described by the Dean of the School of IT, prof. Gert Jansen before prof. Jaan Raik talked about lessons learned from previous Twinning round based on his TUTORIAL project. Concluding discussions were preceded by team introductions of all the SAFEST partners.

FIRST SAFEST WORKSHOP

The first SAFEST workshop took place on 26 March 2021 containing a whole day of technical presentations from all the partners involved in SAFEST. At that virtual Zoom-meeting there were talks about logic locking, side channel attacks, fault injection, reverse engineering, hardware trojans, etc. More than 15 senior staff members from partner institutions attended, as well as nearly 20 early stage researchers (ESRs).

High-level Intellectual Property Obfuscation via Decoy Constants

The first joint publication of the SAFEST project saw light in June 2021 at the 27th IEEE International Symposium on On-Line Testing and Robot System Design. The paper's titled "High-level Intellectual Property Obfuscation via Decoy Constants" and its authors are Levent Aksoy, Quang-linh Nguyen, Felipe Almeida, Jaan Raik, Marie-Line Roches, Sophie Dupuis, and Samuel Pajcini.

Link to abstract and paper's full-text version: <https://onlinelibrary.ingenta.com/doi/10.1109/OLST.2021.9611292>

ISSUE NO 1 | JUNE 2021 PAGE 3

WEBSITE AND YOUTUBE CHANNEL LAUNCHED

The SAFEST project's online presence was established on 10 March 2021 with the launching of the project's official website <https://safest.talltech.ee>. The website contains information about staff, events, research, exchanges, project consortium and contact. Deliverables and dissemination materials can be found on "Research" tab, and a list of all (virtual) events is kept up-to-date on "Exchanges" tab.

The website is complemented by the SAFEST project's YouTube channel that went live on 24 May 2021. The channel hosts clips and recordings from project-related workshops, seminars and other public events. YouTube channel "SAFEST Project" is located at <https://tinyurl.com/SAFESTProject1> and we encourage you all to subscribe and spread the word!

STAFF AND RESEARCHERS' EXCHANGES

An important part of the SAFEST project are short term staff and researcher's exchanges. Due to travel restrictions from the coronavirus pandemic, they have so far have had to take place virtually. Despite of odds, more than 30 virtual meetings, seminars, and workshops have taken place in the first 6 months of the project between the consortium partners. TallTech staff members participated in 55 different occasions, while ESRs participated in 27. From the project partners, the numbers are ~60 and ~130 for staff and ESRs, respectively. Many events also had participation of Bachelor's or Master's level students.

PROJECT DISSEMINATION MATERIALS

In March 2021, several dissemination materials of the SAFEST project, its research areas, and consortium were compiled and published both digitally and on paper:

- Leaflet (PDF version available at https://safest.talltech.ee/wp-content/uploads/SAFEST_Leaflet.pdf)
- Poster (PDF version available at https://safest.talltech.ee/wp-content/uploads/SAFEST_Poster.pdf)
- TallTech Promotion Guide (only in electronic format, PDF: https://safest.talltech.ee/wp-content/uploads/SAFEST_PromotionGuide.pdf)

Please contact samuel.pajcini@talltech.ee if you would like to have paper copies of leaflets and/or posters.

4.2. SAFEST Newsletter #2 (February 2022)

SAFEST NEWSLETTER

ISSUE NO 2 | FEBRUARY 2022



SAFEST

OUR PROJECT

The overall aim of SAFEST is to enhance the scientific and technological capacity of Tallinn University of Technology (TallTech) 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 TallTech 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
- HIGHLIGHTED RESEARCH
- EXCHANGES IN YEAR 1
- YEAR 2 ACTIVITIES

ISSUE NO 2 | FEBRUARY 2022

PAGE 2

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 TallTech, 5 from TUM, 2 from KUL, 1 from TUG, and 1 from CNRS). Over the course of two days, it featured lectures from 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.



Thanks for participating in the summer school!

Reach out if there is interest in a staff exchange!
safest.ppt@talltech.ee



HIGHLIGHTED RESEARCH

The picture on the left is of a 65nm chip developed by TallTech 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://doi.org/10.1146/annex-07-2021-0001>

ISSUE NO 2 | FEBRUARY 2022

PAGE 3

EXCHANGES IN YEAR 1

The aim of SAFEST exchanges is to enhance the scientific and technological capacity of TallTech in the field of Hardware Security sub-topics (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 TallTech, 4 from CNRS, 5 from KUL, 4 from TUM and 2 from TUG. All these meetings are listed on SAFEST website at <https://safest.talltech.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 TallTech.



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 TallTech, 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.talltech.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 TallTech.



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 visibility 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.



4.3. SAFEST Newsletter #3 (June 2022)

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 (TallTech) in the field of Hardware Security, to be achieved through networking activities with its internationally leading Twinning partners: CHRS/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 TallTech in closely related fields, to be complemented by the specific know-how of the Twinning partners in test for security, reverse engineering and disassembly, side-channel attacks, and hardware-of-hware architectural vulnerabilities.

- MONTPELLIER SUMMER SCHOOL
- GRAZ SUMMER SCHOOL
- PROJECT REVIEW MEETING
- STAFF AND ESR EXCHANGES
- NEW PUBLICATIONS

ISSUE NO 3 | JUNE 2022

PAGE 2

MONTPELLIER SUMMER SCHOOL

The SAFEST consortium was finally able to hold one of its planned events in a non-virtual setting. Between June 9 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, Levant Aksoy, Jaan Raik from TallTech, Alex Hepp and Patrick Karl from TUM, Sujoy Sinha Roy from TU Graz, Milos Gujic and Benedikt Gierlich from KUL, Marie-Lise Rofes and Florent Buguier from LIRMM (UM).

Event information and materials are available at <https://safest@tech.eel.evsn.fr/safest-summer-school-june-9-10/>

GRAZ SUMMER SCHOOL

The second SAFEST event of 2022 takes place as the 4th School on Security & Comexness 2022, held from the 26th to the 30th of September, hosted by the Institute of Applied Information Processing and Communication (IAIK) at Graz University of Technology. The school targets PhD students and first 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, Iaria Chillotti, Thomas Eisenbarth, Andrea Riolati, Anders Fogh, Daniel Gröb, Matteo Maffei, Biabath Oswald, Samuel Pagliarini, Michael Peht, Peter Schwabe and others.

Registration information: <https://securityweek.at/2022/registration/#1>
SAFEST-related participants are exempt from the registration fee – there's an option to mark that at registration time.

ISSUE NO 3 | JUNE 2022

PAGE 3

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's staff exchanges continued strong despite corona-pandemia 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@tech.eel.evsn.org/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@tech.eel.evsn.org/2022/>.

ISSUE NO 3 | JUNE 2022

PAGE 4

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 Levant AKSOY (TallTech), Alexander HEPP (TUM), Johanna BAEHR (TUM), and Samuel PAGLIARINI (TallTech). 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

Levant Aksoy, Alexander Hepp, Johanna Baehr, and Samuel Pagliarini
Department of Systems Security, Cyber Protection and Trust (CyberTrust)
University of Duisburg-Essen, Essen, Germany; Institute of Applied Information Processing and Communication (IAIK), Graz University of Technology, Graz, Austria

4.4. SAFEST Newsletter #4 (February 2023)

SAFEST NEWSLETTER

ISSUE NO 4 | FEBRUARY 2023

SAFEST

- GRAZ SUMMER SCHOOL
- HIGHLIGHTED RESEARCH
- PROJECT REVIEW MEETING
- STAFF AND ESR EXCHANGES
- NEW PUBLICATIONS

OUR PROJECT

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

To achieve this, the 3-year project from 2021 to 2023 builds upon the existing strong competence of TallTech 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.

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952252.

ISSUE NO 4 | JANUARY 2023
PAGE 2

GRAZ SUMMER SCHOOL

This year's 2nd summer school took place in June in the framework of TU Graz Security Week on Sept 26-30, 2022. The summer school spanned five days and in addition to prof. Pagliarini's (TallTech) presentation "Hardware Trojan Horses: from Theory to Practice" covered numerous other related topics, like:

- Fully Homomorphic Encryption and Applications,
- Side Channel Attacks,
- High-Assurance Crypto Software,
- Modern Fuzzing Research and Engineering,
- etc.

There participated ESRs from all the SAFEST consortium universities. There were separate workshops for the PhD students to discuss work in progress as well as many practical lab exercises.

The programme and presentation slides are available on the security week's webpage: <https://securityweek.at/2022/programme/>

HIGHLIGHTED RESEARCH

Members of the SAFEST project have been collaborating on post-quantum cryptographic solutions and looking at how to build efficient hardware accelerators for the many algorithms being considered for standardization. In "Kall: A Crystal for Post-Quantum Security using Kyber and Dilithium", researchers from TU Graz and from TallTech have built a unified architecture that supports both Kyber and Dilithium, thus allowing for key exchange mechanism and digital signatures to share hardware resources.

The paper was published in the journal "IEEE Transactions on Circuits and Systems I: Regular Papers". Abstract and full text can be found at <https://ieeexplore.ieee.org/abstract/document/992271086>

Kall: A Crystal for Post-Quantum Security using Kyber and Dilithium

Alexis Akiba, Abhishek Gupta, Mubir Hossain, Samarth Pappas, Raju Saha, Roy

ISSUE NO 4 | JANUARY 2023
PAGE 3

PROJECT REVIEW MEETING

The Review Meeting for the SAFEST Reporting Period 1 (Jan 2021 – March 2022) took place on June 14, 2022 in Zoom with the participation SAFEST Steering Committee (with one representative from each consortium member), EC representative and an independent reviewer. The meeting summarised the reporting documentation submitted by the consortium. Prof. Pagliarini's presentation was followed by several rounds of Q&A. A few followup topics (like spending balances, different approaches to use of PMs with partners) were identified, addressing which over the next few weeks eliminated the last remaining unclear issues. In August 2022 the Period Reports were approved by the EC.

STAFF AND ESR EXCHANGES

SAFEST's staff exchanges and ESR exchanges continued in the 2nd half of 2022 (July-Dec) with virtual meetings with Staff participation from all 5 partners. We also had a small number of physical site visits.

All these meetings are listed on SAFEST website at <https://safest.talltech.eu/en/homepage/2022/>

The last year of the SAFEST project has started and now is a perfect time to take most out of this project and plan for both virtual meetings and ON-SITE visits!

ISSUE NO 4 | JANUARY 2023
PAGE 4

NEW PUBLICATIONS

The 2nd half of 2022 was especially prolific for SAFEST-related research. In addition to the aforementioned Kall paper, three more papers were published:

"Multiplierless Design of Very Large Constant Multiplications in Cryptography" by Lavent Aksoy (TallTech), Debapriya Roy (TUM), Malik Imran (TallTech), Patrick Kozi (TUM), and Samuel Pagliarini (TallTech) in the journal "IEEE Transactions on Circuits and Systems II". See more at <https://arxiv.org/abs/2202.10002>

"A Pragmatic Methodology for Blind Hardware Trojan Insertion in Rintalized Layouts" by Alexander Hago (TUM), Tago Diadami Perez (TallTech), Samuel Pagliarini (TallTech) and Georg Sigl (TUM) at International Conference on Computer-Aided Design (ICCAD). Have a look at <https://arxiv.org/abs/2203.07235>

"Leveraging Layout-based Effects for Locking Analog ICs" by Mucayad Aljatar (TallTech), Renée Azis (CNRS), Marie-Lise Rothen (CNRS) and Samuel Pagliarini (TallTech) at ASHES'22: Workshop on Attacks and Solutions in Hardware Security. More info at <https://arxiv.org/abs/2202.01856>

Congratulations to all authors!

4.5. SAFEST Newsletter #5 (June 2023)

SAFEST NEWSLETTER

ISSUE NO 5 | JUNE 2023

SAFEST

- SAFEST TALLINN WORKSHOP 2023
- SAFEST SUMMER SCHOOL IN GRAZ
- LAST CALL FOR STAFF AND ESR EXCHANGES
- NEW PUBLICATIONS

OUR PROJECT

The overall aim of SAFEST is to enhance the scientific and technological capacity of Tallinn University of Technology (TallTech) in the field of Hardware Security, to be achieved through networking activities with its internationally leading Twinning partners: CHRS/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 TallTech in closely related fields, to be complemented by the specific know-how of the Twinning partners in test for security, reverse engineering and defence, side channel attacks, and hardware-software architectural vulnerabilities.

ISSUE NO 5 | JUNE 2023

SAFEST TALLINN WORKSHOP 2023

The 3rd SAFEST workshop took place in Tallinn, Estonia from June 19 to June 21. During the three days participants from all of the SAFEST consortium members delivered and attended talks on numerous HW security topics, like:

- Logic locking,
- Side Channel Leakage,
- Post-quantum Cryptography,
- Homomorphic Encryption,
- and much more during the more than 20 presentations.

Social activities included a tour of the Old Town, a spa visit and a joint dinner at a seaside restaurant aptly called Ocean 11.

The event info and presentation slides are available on the workshop's webpage: <https://safest.talltech.ee/en/23/safest-workshop-2023-in-tallinn-june-19-21-2023/>

SAFEST SUMMER SCHOOL IN GRAZ IN SEPT 2023

Graz security week 2023 will be held from 4-8 September, and under the auspices of it the SAFEST Summer School of 2023 will also take place. The main topics of the summer school are:

- Runtime Security,
- Side-Channels,
- Privacy,
- Secure Cryptographic Implementations,
- Security Verification.

The programme is available at <https://gscw.utyweek.at/2023/>

SAFEST participants do not have to pay the registration fee to attend the Summer School. Please discuss with your supervisor/PI about attending the event. Ask your PI for the link to the free registration!

The project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 952252.

ISSUE NO 5 | JUNE 2023

LAST CALL FOR STAFF AND ESR EXCHANGES

SAFEST's staff exchanges and ESR exchanges continued in the 1st half of 2023 (Jan-June) mostly virtually, but the number of physical visits has clearly picked up – 8 compared to 3 in the last year's same period.

All these meetings are listed on SAFEST website at <https://safest.talltech.ee/exchanges/2023/>. The previous years can be found at <https://safest.talltech.ee/exchanges/2021/> and <https://safest.talltech.ee/exchanges/2022/>.

PAGE 3

NOW is the best time to make ON-SITE visit plans for the remainder of SAFEST project till the end of 2023.

We encourage you to visit TallTech for the face-to-face meetings with the colleagues you have had so many online meetings with. Similarly, the TallTech SAFEST staff and ESR are welcome to visit their partners at other SAFEST consortium universities.

NEW PUBLICATIONS

In the 1st half of 2023 SAFEST partners continues strong in publishing four joint authored papers in internationally renowned conferences and journals:

"Resynthesis-based Attacks Against Logic Locking" by Felipe Almeida (TallTech), Levent Aksoy (TallTech), Quang-Linh Nguyen (CHRS), Sophie Dupuis (CHRS), Marie-Lise Roffes (CHRS), and Samuel Pagliani (TallTech) in the proceedings of "2023 24th International Symposium on Quality Electronic Design (IQED)". See more at <https://arxiv.org/abs/2301.04400>

"Hybrid Protection of Digital PR Filters" by Levent Aksoy (TallTech), Quang-Linh Nguyen (CHRS), Felipe Almeida (TallTech), Joan Ruk (TallTech), Marie-Lise Roffes (CHRS), Sophie Dupuis (CHRS), Samuel Pagliani (TallTech) in the "IEEE Transactions on VLSI". Have a look at <https://arxiv.org/abs/2301.11115>.

ISSUE NO 5 | JUNE 2023

"High-speed SABER Key Encapsulation Mechanism in 65nm CMOS" by Abak Inan (TallTech), Felipe Almeida (TallTech), Andrea Basso (TUG), Sujoy Sinha Roy (TUG) and Samuel Pagliani (TallTech) in the "Journal of Cryptographic Engineering (JCE)". More info at <https://ieeexplore.ieee.org/abstract/document/10202530>

"Towards High-speed ASIC Implementations of Post-Quantum Cryptography" by Abak Inan (TallTech), Aikata Akata (TUG), Sujoy Sinha Roy (TUG), and Samuel Pagliani (TallTech) in the "IEEE Transactions on Circuits and Systems II: Express Briefs". Read more about the publication at <https://ieeexplore.ieee.org/abstract/document/10203716>

Congratulations to all authors!

PAGE 4

