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 (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.

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 as listeners. The project coordinator gave an overview of the SAFEST project while project officer Alina-Maria Bercea introduced EC/REA view on H2020 projects. TalTech was described by the Dean of the School of IT, prof Gert Jervan 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.

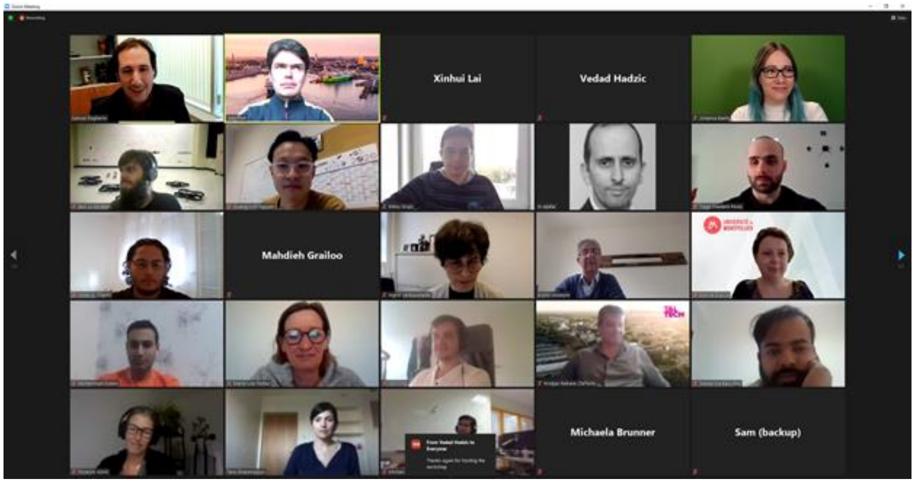
KICK-OFF MEETING
8TH JANUARY 2021
1:30PM TO 5PM CET

*PLEASE MUTE YOUR MIC!

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

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

Levent Aksoy[†], Quang-Linh Nguyen[‡], Felipe Almeida[†], Jaan Raik[†], Marie-Lise Flottes[‡], Sophie Dupuis[‡]
and Samuel Pagliarini[†]
[†]Department of Computer Systems, Tallinn University of Technology, Tallinn, Estonia
Email: {levent.aksoy, felipe.almeida, jaan.raik, samuel.pagliarini}@taltech.ee
[‡]LIRMM, University of Montpellier, Montpellier, France
Email: {quang-linh.nguyen, marie-lise.flottes, sophie.dupuis}@lirmm.fr

***Abstract*—This paper presents a high-level circuit obfuscation technique to prevent the theft of intellectual property (IP) of integrated circuits. In particular, our technique protects a class of circuits that relies on constant multiplications, such as filters and neural networks, where the constants themselves are the IP to be protected. By making use of decoy constants and a key-based scheme, a reverse engineer adversary at an untrusted foundry is rendered incapable of discerning true constants from decoy constants. The time-multiplexed constant multiplication (TMCM) block of such circuits, which realizes the multiplication of an input variable by a constant at a time, is considered as our case study for obfuscation. Furthermore, two TMCM design architectures are taken into account; an implementation using a multiplier and a multiplierless shift-adds implementation. Optimization methods are also applied to reduce the hardware complexity of these architectures. The well-known satisfiability (SAT) and automatic test pattern generation (ATPG) attacks are used to determine the vulnerability of the obfuscated designs. It is observed that the proposed technique incurs small overheads in area, power, and delay that are comparable to the hardware complexity of prominent logic locking methods. Yet, the advantage of our approach is in the insight that constants – instead of arbitrary circuit nodes – become key-protected.**

***Index Terms*—hardware obfuscation, reverse engineering, IP obfuscation, SAT attack, digital FIR filter design.**

I. Introduction

The involvement of multiple entities in the design and fabrication process of integrated circuits (ICs) potentially leads to security threats, such as reverse engineering, overbuilding, and insertion of malicious hardware Trojans [1]–[3]. Many efficient techniques, such as watermarking [4], IC metering [5], IC camouflaging [6], and logic locking [7], have been proposed to address these issues. Among these techniques, logic locking stands out, offering a protection against a diverse array of adversaries [8]. Logic locking inserts additional logic into a circuit, such as XOR/XNOR gates [9], AND/OR gates [10], or look-up tables [11], driven by a secret key, so that the circuit behaves as specified only when the correct key inputs are applied. The logic locking and activation of a locked circuit in the IC design flow are shown in Fig. 1.

Many widely employed circuits, such as artificial neural networks (ANNs) and finite impulse response (FIR) filters, require the multiplication of constant(s) by input variable(s). In these applications, ANN weights and filter coefficients are constants determined beforehand using sophisticated algorithms [12], [13]. These constants are, therefore, an intellectual property (IP). Hence, there is a clear interest in protecting the constants since they are valuable, perhaps even more so than the circuit architecture, e.g., the number of layers in an ANN or the multiplier and accumulate block in a filter.

The hardware complexity of ANNs and filters increases as the number of neurons and filter coefficients increases, respectively, restricting their applications on design platforms with a limited number of computing resources, such as FPGAs, and on designs having a strict area requirement [14], [15]. To reduce the design area, taking into account an increase in latency, such IPs are generally implemented under a folded architecture re-using the computing resources [16]. In a folded design, the time-multiplexed constant multiplication (TMCM) operation is a fundamental block that realizes the multiplication of an input variable by a single constant selected from a set of multiple constants at a time [17], [18]. Since a design's layout is inevitably available to an adversary at an untrusted foundry, constants of the TMCM block are vulnerable to reverse engineering even if a logic locking method is employed. Logic locking, despite its popularity, is not particularly well suited for hiding constants or similar design features.

Given the limitations discussed above, the main contribution of this paper is an **obfuscation technique that protects the sensitive constants from an adversary at an untrusted foundry by hiding them among decoy constants using additional logic with keyed inputs**. The proposed technique implements the obfuscation of the TMCM operation at the register-transfer level (RTL) as shown in Fig. 1. This enables a synthesis tool to optimize the design complexity and also promotes resource sharing, as opposed to traditional logic locking methods which are applied post synthesis at gate level. This paper considers two TMCM design architectures referred to as TMCM-MUL and TMCM-SA. While the former utilizes multiplexors and a multiplier, the latter utilizes shifts, adders, subtractors, adders/subtractors (determined by a select input), and multiplexors under a shift-adds architecture, but no multiplier.

The rest of this paper is organized as follows. Section II gives the background concepts on the TMCM block and folded FIR filter design and presents the related work. The proposed TMCM obfuscation technique is described in Section III. Experimental results are presented in Section IV and finally, Section V concludes the paper.

FIRST JOINT PUBLICATION IN SAFEST

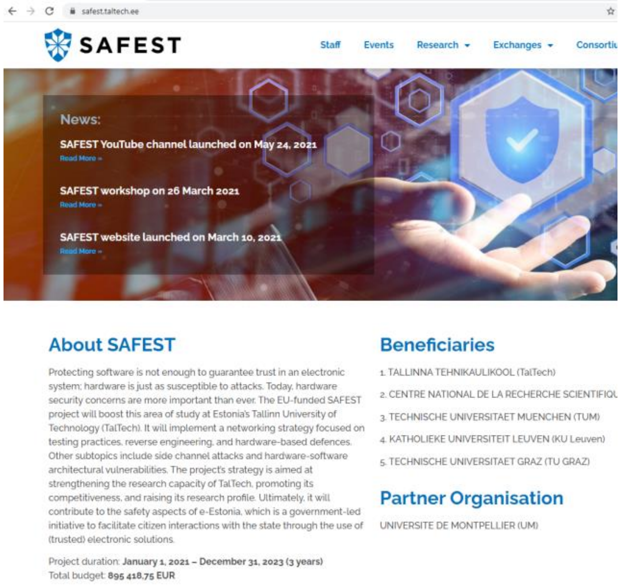
The first joint publication of the SAFEST project saw light in June 2021 at the 27th IEEE International Symposium on On-Line Testing and Robust System Design. The paper is titled "High-level Intellectual Property Obfuscation via Decoy Constants" and its authors are Levent Aksoy, Quang-Linh Nguyen, Felipe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

Link to abstract and paper's full-text version:
https://arxiv.org/abs/2105.06122

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.taltech.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/SAFESTproject and we encourage you all to subscribe and spread the word!



News:

SAFEST YouTube channel launched on May 24, 2021
Read More »

SAFEST workshop on 26 March 2021
Read More »

SAFEST website launched on March 10, 2021
Read More »

About SAFEST

Protecting software is not enough to guarantee trust in an electronic system; hardware is just as susceptible to attacks. Today, hardware security concerns are more important than ever. The EU-funded SAFEST project will boost this area of study at Estonia's Tallinn University of Technology (TalTech). It will implement a networking strategy focused on testing practices, reverse engineering, and hardware-based defences. Other subtopics include side channel attacks and hardware-software architectural vulnerabilities. The project's strategy is aimed at strengthening the research capacity of TalTech, promoting its competitiveness, and raising its research profile. Ultimately, it will contribute to the safety aspects of e-Estonia, which is a government-led initiative to facilitate citizen interactions with the state through the use of (trusted) electronic solutions.

Project duration: **January 1, 2021 – December 31, 2023 (3 years)**
Total budget: **895 418,75 EUR**

Beneficiaries

1. TALLINNA TEHNIKAULIKOOL (TalTech)
2. CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQU
3. TECHNISCHE UNIVERSITAET MUENCHEN (TUM)
4. KATHOLIEKE UNIVERSITEIT LEUVEN (KU Leuven)
5. TECHNISCHE UNIVERSITAET GRAZ (TU GRAZ)

Partner Organisation

UNIVERSITE DE MONTPELLIER (UM)

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 all odds, more than 30 virtual meetings, seminars, and workshops have taken place in the first 6 months of the project between the consortium partners. TalTech staff members participated in 55 different ocasions, 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.

ON THE USE OF HARDWARE MONITORING SCHEMES FOR SECURITY

Mohammad Eslami
Centre for Hardware Security
Department of Computer Systems
Tallinn University of Technology

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.taltech.ee/wp-content/uploads/SAFEST_Leaflet.pdf)
* Poster (PDF version available at https://safest.taltech.ee/wp-content/uploads/SAFEST_Poster.pdf)
* TalTech Promotion Guide (only in electronic format; PDF: https://safest.taltech.ee/wp-content/uploads/SAFEST_Guide.pdf)

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

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