SAFEST NEWSLETTER

ISSUE NO 5 | JUNE 2023

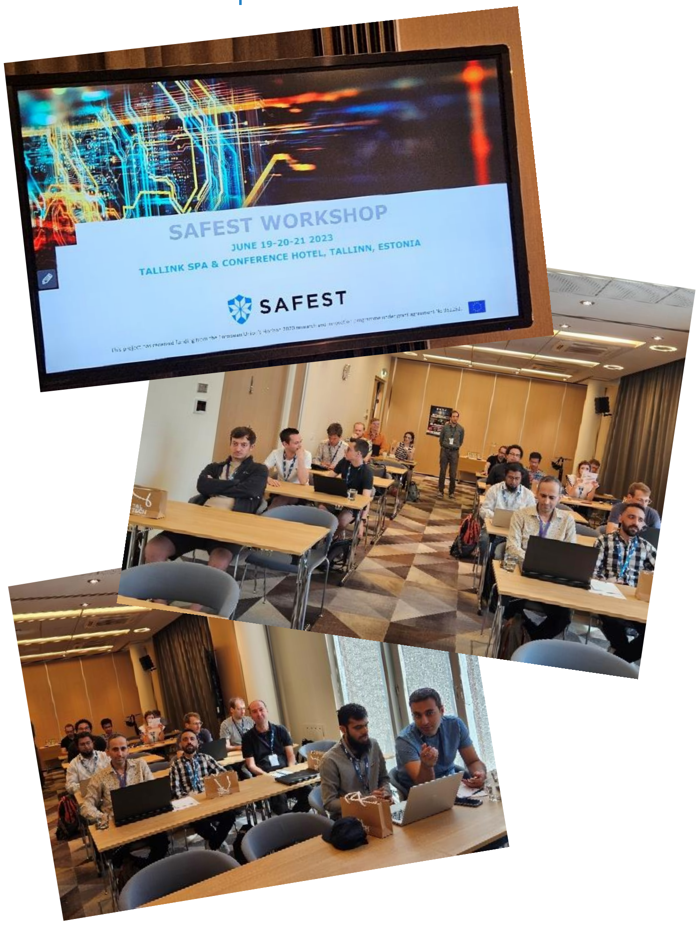
SAFEST

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 defences, 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.



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 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.taltech.ee/events/safest-workshop-2023-in-tallinn-june-19-21-2023/

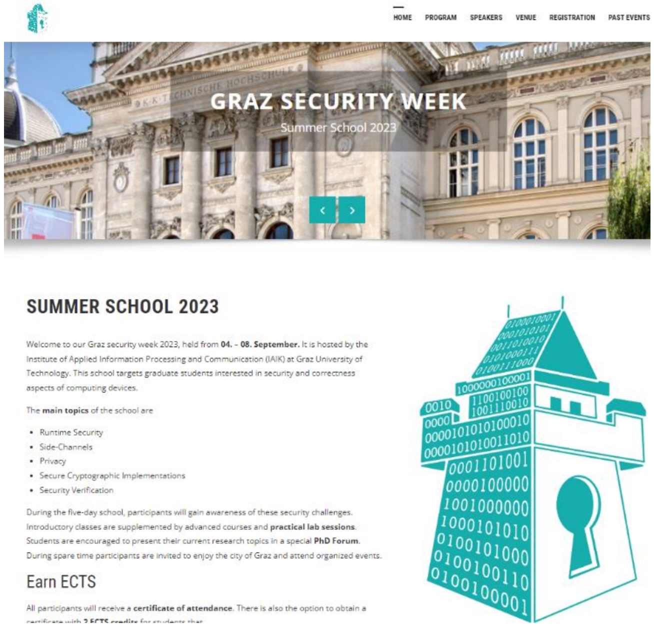
SAFEST SUMMER SCHOOL IN GRAZ IN SEPT 2023

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://securityweek.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!



SUMMER SCHOOL 2023

Welcome to our Graz security week 2023, held from **04. - 08. September.** It is hosted by the Institute of Applied Information Processing and Communication (IAIK) at Graz University of Technology. This school targets graduate students interested in security and correctness aspects of computing devices.

The **main topics** of the school are

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

During the five-day school, participants will gain awareness of these security challenges. Introductory classes are supplemented by advanced courses and **practical lab sessions**. Students are encouraged to present their current research topics in a special **PhD Forum**. During spare time participants are invited to enjoy the city of Graz and attend organized events.

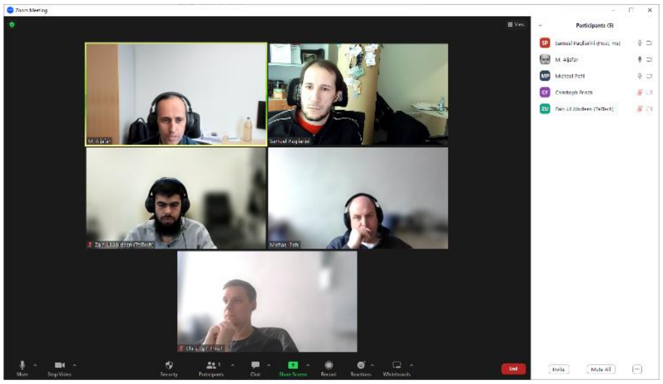
Earn ECTS

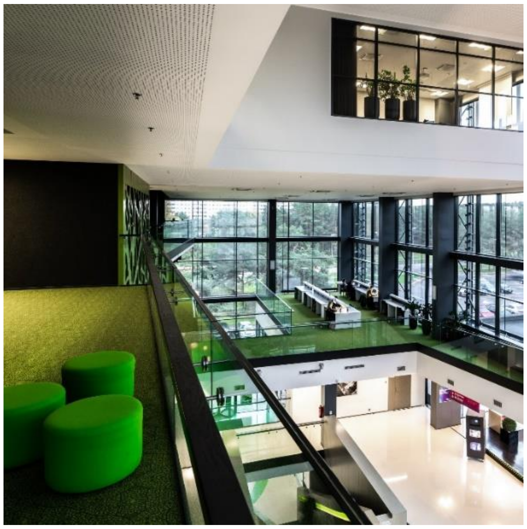
All participants will receive a **certificate of attendance**. There is also the option to obtain a certificate with **2 ECTS credits** for students that

LAST CALL FOR STAFF AND ESR EXCHANGES

SAFEST **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.taltech.ee/exchanges-2023/
The previous years can be found at https://safest.taltech.ee/exchanges-2021/ and https://safest.taltech.ee/exchanges-2022/





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 TalTech for the face-to-face meetings with the colleagues you have had so many online meetings with. Similarly, the TalTech 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 (TalTech), Levent Aksoy (TalTech), Quang-Linh Nguyen (CNRS), Sophie Dupuis (CNRS), Marie-Lise Flottes (CNRS), and Samuel Pagliarini (TalTech) in the proceedings of " 2023 24th International Symposium on Quality Electronic Design (ISQED)". See more at https://arxiv.org/abs/2301.04400

"Hybrid Protection of Digital FIR Filters" by Levent Aksoy (TalTech), Quang-Linh Nguyen (CNRS), Felipe Almeida (TalTech), Jaan Raik (TalTech), Marie-Lise Flottes (CNRS), Sophie Dupuis (CNRS), Samuel Pagliarini (TalTech) in the "IEEE Transactions on VLSI". Have a look at https://arxiv.org/abs/2301.11115

Resynthesis-based Attacks Against Logic Locking

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

arXiv:2301.04400v1 [cs.CR] 11 Jan 2023

Abstract—**Logic locking has been a promising solution to many hardware security threats, such as intellectual property infringement and overproduction. Due to the increased attention that threats have received, many efficient specialized attacks against logic locking have been introduced over the years. However, the ability of an adversary to manipulate a locked netlist prior to mounting an attack has not been investigated thoroughly. This paper introduces a resynthesis-based strategy that utilizes the strength of a commercial electronic design automation (EDA) tool to reveal the vulnerabilities of a locked circuit. To do so, in a pre-attack step, a locked netlist is resynthesized using different synthesis parameters in a systematic way, leading to a large number of functionally equivalent but structurally different locked circuits. Then, under the oracle-less threat model, where it is assumed that the adversary only possesses the locked circuit, not the original circuit to query, a prominent attack is applied to these generated netlists collectively, from which a large number of key bits are deciphered. Nevertheless, this paper also describes how the proposed oracle-less attack can be integrated with an oracle-guided attack. The feasibility of the proposed approach is demonstrated for several benchmarks, including remarkable results for breaking a recently proposed provably secure logic locking method and deciphering values of a large number of key bits of the CSAW'19 circuits with very high accuracy.**

Index Terms—**Logic locking, resynthesis, EDA tools, oracle-less and oracle-guided attacks.**

I. INTRODUCTION

Due to the globalized integrated circuit (IC) supply chain, serious security threats, such as hardware Trojans, piracy, overbuilding, reverse engineering, and counterfeiting, have emerged [1]. Many defense techniques, such as watermarking [2], digital rights management [3], metering [4], and logic locking [5], have been introduced over the years to deal with these threats. Among those, logic locking stands out by being a well-established technique and by offering protection against a diverse array of adversaries [6]. Logic locking inserts additional logic driven by key bits so that the circuit behaves as expected only when the secret key is applied.

On the other hand, many efficient attacks have been introduced to overcome the defenses built by logic locking [7]. However, the impact of an electronic design automation (EDA) tool on the manipulation of the locked netlist **before** performing an attack has not been investigated thoroughly. In this work, we explore if EDA tools can be used to make a locked circuit vulnerable to existing logic locking attacks. Thus, the main contributions of this work are three-fold: (i) we introduce a resynthesis procedure that is a **pre-attack** step, where functionally equivalent but structurally different locked circuits are generated by resynthesizing the original locked circuit using different optimization parameters and delay constraints in order to create structural vulnerabilities that can be exploited by existing attacks; (ii) we present an oracle-less (OL) **resynthesis-based attack**, which applies the prominent SCOPE attack [8] to these resynthesized circuits and gathers all its solutions to discover the secret key; (iii) we show that our OL attack can be **combined** with a traditional oracle-guided (OG) attack for further improving the number of correctly deciphered key bits. The last contribution is essential, since we consider circuits from the CSAW'19 contest – these circuits compound the use of two logic locking techniques at the same time.

The main finding of this work is that the use of many resynthesized locked circuits enables us to discover values of more key bits, and even the whole key, when compared to a single attack mounted on the original locked netlist.

The remainder of this paper is organized as follows: Section II presents the background concepts and related work. The resynthesis process and the proposed attacks are described in Section III. Experimental results are given in Section IV. Finally, Section V concludes the paper.

II. BACKGROUND

A. Logic Locking and Threat Models

The procedure of logic locking is applied at the gate level in the IC design flow, as shown in Fig. 1. Note that the layout of the locked circuit is sent to the foundry without revealing the secret key. After the locked IC is produced and delivered to the design house, the values of the secret key are stored in a tamper-proof memory, before the functional IC is sent to the market.

It is assumed that the gate-level netlist of the locked circuit can be obtained directly by an untrusted foundry or by reverse-engineering a functional IC obtained from the open market. An adversary can also use the functional IC programmed with the secret key as an oracle to apply inputs and observe outputs. Thus, in logic locking, there are generally two threat models: OL and OG. In the OL threat model, only the gate-level netlist of the locked circuit is available to the

This work has been partially conducted in the project "ICT programme" which was supported by the European Union through the European Social Fund. It was also partially supported by European Union's Horizon 2020 research and innovation programme under grant agreement No 952252 (SAFEST).

“High-speed SABER Key Encapsulation Mechanism in 65nm CMOS” by Malik Imran (TalTech), Felipe Almeida (TalTech), Andrea Basso (TUG), Sujoy Sinha Roy (TUG), and Samuel Pagliarini (TalTech) in the “Journal of Cryptographic Engineering (JCEN)”. More info at https://eprint.iacr.org/2022/530

“Towards High-speed ASIC Implementations of Post-Quantum Cryptography” by Malik Imran (TalTech), Aikata Aikata (TUG), Sujoy Sinha Roy (TUG), and Samuel Pagliarini (TalTech) in the “IEEE Transactions on Circuits and Systems II: Express Briefs”. Read more about the publication at https://eprint.iacr.org/2023/716

Congratulations to all authors!