

SAFEST NEWSLETTER

ISSUE NO 6 | DECEMBER 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.

- SAFEST SUMMER SCHOOL IN GRAZ
- NEW PUBLICATIONS
- NEW SAFEST YOUTUBE CLIP
- EXCHANGES IN YEAR 3
- WRAP-UP OF SAFEST



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

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.



SAFEST SUMMER SCHOOL IN GRAZ IN SEPT 2023

Graz Security Week 2023 was held from 4.-8. September, and the SAFEST Summer School of 2023 also took place under the auspices of it. The main topics of the summer school were:

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

The full programme is available at

<https://securityweek.at/2023/>

There were 12 SAFEST participants, mostly ESRs, from five different countries attending and joining in to the discussions at the Graz Security Week in 2023.

NEW PUBLICATIONS

In the 2nd half of 2023 SAFEST partners published one jointly authored paper in an internationally renowned conference proceedings in addition to the publication highlighted in the previous section:

“Multiplierless Design of High-Speed Very Large Constant Multiplications” by Levent Aksoy, Debapriya Roy, Malik Imran, and Samuel Pagliarini in the proceedings of 2024 29th Asia and South Pacific Design Automation Conference (ASP-DAC). Read the paper at <https://arxiv.org/abs/2309.05550>

Congratulations to all authors!

Multiplierless Design of High-Speed Very Large Constant Multiplications

Levent Aksoy¹, Debapriya Roy², Malik Imran¹, Samuel Pagliarini¹
¹Department of Computer Systems, Tallinn University of Technology, Tallinn, Estonia
 Email: {levent.aksoy, malik.imran, samuel.pagliarini}@tut.ee
²Computer Science and Engineering, IIT Kanpur, Kanpur, India
 Email: droy@iitk.ac.in

Abstract—In cryptographic algorithms, the constants to be multiplied by a variable can be very large due to security requirements. Thus, the hardware complexity of such algorithms heavily depends on the design architecture handling large constants. In this paper, we introduce an electronic design automation tool, called *LEICA*, which can automatically generate the realizations of very large constant multiplications for low-complexity and high-speed applications, targeting the ASIC design platform. *LEICA* is able to synthesize the multiplierless and non-2-input of CSAs in order to reduce using a proposed optimization algorithm. In this paper, we present a multiplierless multiplier in a hybrid design architecture, where 2-input 3-input operations are used at different stages. However, it can describe constant multiplication with its constant multiplier block realized under the proposed architecture. Experimental results indicate that *LEICA* enables a designer to explore the trade-off between area and delay of the very large constant and Montgomery multiplication and leads to designs with area-time product, delay, and energy consumption three (approximately) times less than those realized by a fully multiplierless constant multiplication, add-sub design, compressor trees, high-speed design, area optimization, Montgomery multiplication, cryptographically.

1. INTRODUCTION
 The Montgomery modular multiplication [1] is an essential operation in cryptographic algorithms, such as RSA [2], elliptic curve cryptography (ECC) [3], and supersingular isogeny key encapsulation (SIKE) [4]. Since these algorithms operate on large prime numbers, e.g., 2048, 3264, and 7680 in RSA, ECC, and SIKE, respectively, the operands of the Montgomery multiplication are generally divided into smaller multiple bits, so that reasonable sizes of multiplication and addition operations can be used to compute the modular multiplication in acceptable latency [5], [6]. Note that the size of these multiple bits in the very large constant and input variable has a significant impact on the hardware complexity of the Montgomery multiplication design and thus, the exploration of values of these parameters is important to find the design, which fits perfectly in a low-complexity and high-speed application [6]. The Montgomery multiplication includes the multiplication of a very large prime number by an input variable, called the very large constant multiplication (VLCM) operation. There is only the algorithm of [7], which aims to reduce the hardware complexity of the VLCM operation under the shift-add architecture using only shift and addition/subtraction operations. To do so, it uses adders, which increase the amount of common subexpressions among constant multiplications. However, it does not consider the high-speed realization of the VLCM operation, which is essential for high-performance cryptographic algorithms. To the best of our knowledge, there exist no algorithms proposed for the low-complexity and high-speed realization of the VLCM operation.

Thus, in this paper, we introduce an electronic design automation (EDA) tool, called *LEICA*, which can describe the high-speed design of the VLCM operation taking into account the area and targeting the ASIC design platform under three different architectures: (i) the shift-add architecture using carry-save adders (CSAs), denoted as SA-CSA; (ii) the shift-add architecture using 2-input adders/subtractors and 3-input CSAs at different stages, denoted as SA-Hybrid; (iii) the design architecture using compressor trees, denoted as CT. The very large constants are divided into smaller coefficients under the shift-add architecture and the number of 2-input operations and CSAs is reduced using optimization algorithms [8]-[11]. The input variable is partitioned into smaller bits under the CT architecture and compressor trees are used to add the multiple of very large constants. Moreover, *LEICA* can automatically generate the entire Montgomery multiplication including its high-speed VLCM operation implemented under a given design architecture. Thus, the main contributions of this paper are two-fold: (i) a proposed design architecture to realize the VLCM operation for high-speed applications, incorporating prominent algorithms to reduce its complexity; (ii) it introduces high-speed Montgomery multiplication designs including the VLCM operation realized under the proposed architectures. It is observed from the experimental results that the exploration of the number of bits used in partitioning the very large constant and input variable in the VLCM operation is crucial while finding a low-complexity and high-speed design. It is shown that when compared to *LEICA*, the algorithm of [7] leads to VLCM operation and Montgomery multiplication designs with 1.3- and 13.3- larger area-time product (ATP) values, respectively.

The rest of this paper is organized as follows: Section II presents the background concepts. The proposed design archi-

NEW SAFEST VIDEO ON YOUTUBE

Prof Samuel Pagliarini has recorded a short 10-minute talk **“Is it possible to fingerprint a computer chip?”** for a high-school audience that explains how we can get digital signatures out of computer chips. From these signatures, we can tell whether a chip is authentic or fake. The technology behind these signatures is a Physically Unclonable Function, or PUF. We can get PUFs out of SRAM memory bits.


The video is available at

<https://youtu.be/WpfSITw32MU>

or browse the other SAFEST-project related videos

here: <https://www.youtube.com/@safestproject155>


ANALOGY: A SEESAW IN A PLAYGROUND

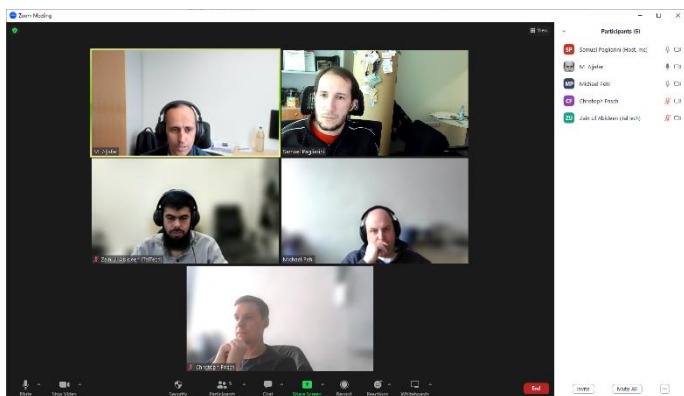


Two young scientists try to balance the toy...

Step 1: level both sides
 Step 2: release
 Step 3: observe

Surprising scientific discovery
 N repeats of the experiment...
 Same answer!





STAFF AND ESR EXCHANGES IN YEAR 3

In 2023 **17 staff meetings** took place online and attended by 3 staff members from TalTech, 2 from KUL, 2 from TUM and 1 from TUG while **14 ESR meetings** took place the same year and attended by 3 ESRs from TalTech, 1 from KUL, 5 from TUM and 1 from TUG. All these meetings are listed at <https://safest.taltech.ee/exchanges-2023/>.

There were also **nine physical short-term exchanges** in 2023: 4 CNRS and 1 TUM staff to TalTech, 2 TUM and 1 TUG ESRs to TalTech while 1 TalTech ESR visited TUM.

WRAP-UP OF SAFEST PROJECT

The SAFEST project is approaching the end of its 3rd year, which marks the end of the planned life cycle of this multi-partner international cooperation project.

And what a ride it has been! Start of the project coincided with the explosion of global corona pandemic, which caused most of the exchanges to become virtual – more than **130 online meetings**, big and small, have taken place. Despite that over **20 real-life exchanges** and **5 summer schools** took place in all the countries of the consortium partners. **12 jointly authored papers** in both conference/workshop proceedings and renowned international journals were published. SAFEST project spread information via **mailing list**, **6 newsletters** like this one, **a website**, **YouTube channel**, **leaflets and posters**.

By no means does the end of the project mark the end of cooperation between the SAFEST consortium partners. The many working partnerships and friendships will continue under new collaborations. So, see you around!



SAFEST
See you around!