SAFEST NEWSLETTER

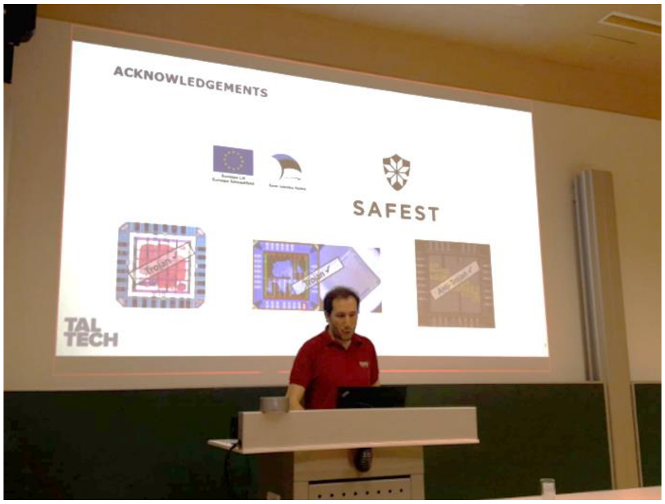
ISSUE NO 4 | FEBRUARY 2023

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 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.



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 (TalTech) 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.

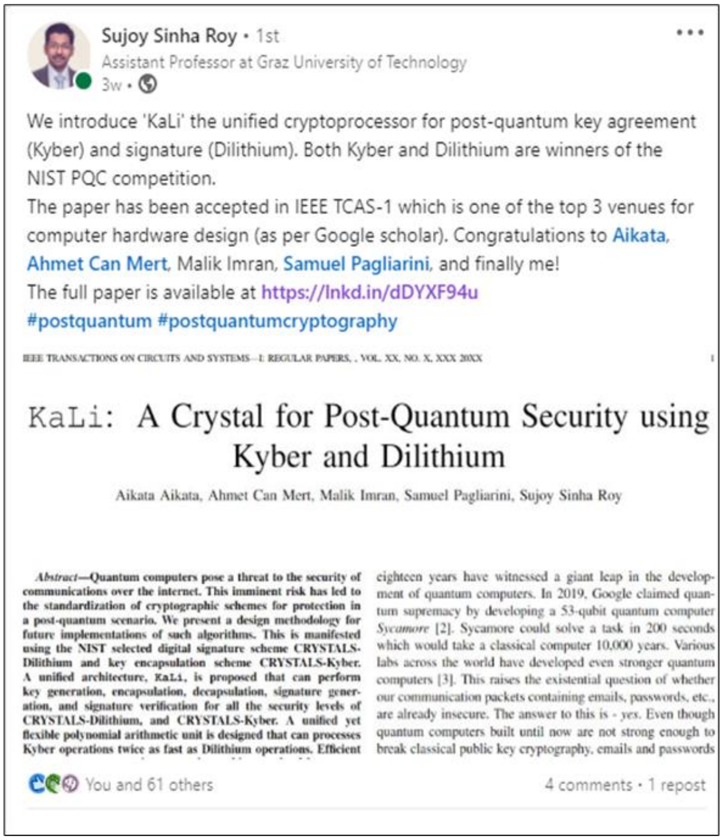
There participated ESRs from all the SAFEST consortium universities. There were separate workshops for the PhD students to discuss work in progress as well as many practical lab exercises.

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

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 "KaLi: A Crystal for Post-Quantum Security using Kyber and Dilithium", researchers from TU Graz and from TalTech 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://eprint.iacr.org/2022/1086



Sujoy Sinha Roy • 1st
Assistant Professor at Graz University of Technology
3w •

We introduce 'KaLi' the unified cryptoprocessor for post-quantum key agreement (Kyber) and signature (Dilithium). Both Kyber and Dilithium are winners of the NIST PQC competition.
The paper has been accepted in IEEE TCAS-1 which is one of the top 3 venues for computer hardware design (as per Google scholar). Congratulations to Aikata, Ahmet Can Mert, Malik Imran, Samuel Pagliarini, and finally me!
The full paper is available at https://lnkd.in/dDYXF94u
#postquantum #postquantumcryptography

IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: REGULAR PAPERS, , VOL. XX, NO. X, XXX 20XX 1

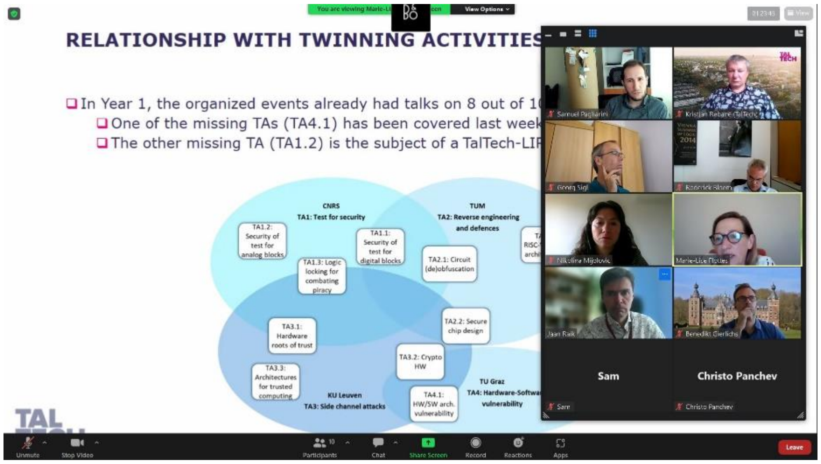
KaLi: A Crystal for Post-Quantum Security using Kyber and Dilithium

Aikata Aikata, Ahmet Can Mert, Malik Imran, Samuel Pagliarini, Sujoy Sinha Roy

***Abstract*—Quantum computers pose a threat to the security of communications over the internet. This imminent risk has led to the standardization of cryptographic schemes for protection in a post-quantum scenario. We present a design methodology for future implementations of such algorithms. This is manifested using the NIST selected digital signature scheme CRYSTALS-Dilithium and key encapsulation scheme CRYSTALS-Kyber. A unified architecture, KaLi, is proposed that can perform key generation, encapsulation, decapsulation, signature generation, and signature verification for all the security levels of CRYSTALS-Dilithium, and CRYSTALS-Kyber. A unified yet flexible polynomial arithmetic unit is designed that can processes Kyber operations twice as fast as Dilithium operations. Efficient**

eighteen years have witnessed a giant leap in the development of quantum computers. In 2019, Google claimed quantum supremacy by developing a 53-qubit quantum computer *Sycamore* [2]. Sycamore could solve a task in 200 seconds which would take a classical computer 10,000 years. Various labs across the world have developed even stronger quantum computers [3]. This raises the existential question of whether our communication packets containing emails, passwords, etc., are already insecure. The answer to this is - *yes*. Even though quantum computers built until now are not strong enough to break classical public key cryptography, emails and passwords

You and 61 others 4 comments • 1 repost



RELATIONSHIP WITH TWINNING ACTIVITIES

- In Year 1, the organized events already had talks on 8 out of 1
  - One of the missing TAs (TA4.1) has been covered last week
  - The other missing TA (TA1.2) is the subject of a TalTech-LIF

You are viewing Marie-Li
View Options
CNRS
TA1: Test for security
TUM
TA2: Reverse engineering and defences
TA1.2: Security of test for analog blocks
TA1.1: Security of test for digital blocks
TA1.3: Logic locking for combating piracy
TA2.1: Circuit (de)obfuscation
TA2.2: Secure chip design
TA3.1: Hardware roots of trust
TA3.2: Crypto HW
TA3.3: Architectures for trusted computing
KU Leuven
TA3: Side channel attacks
TA4.1: HW/SW arch. vulnerability
TU Graz
TA4: Hardware-Softwa vulnerability
TAL TECH
Samuel Pagliarini
Kristjan Rebane (TalTech)
Georg Sigl
Roderick Bloem
Nikolina Mijolovic
Marie-Lise Flottes
Jaan Raik
Benedikt Gierlichs
Sam
Christo Panchev
Unmute
Stop Video
Participants
Chat
Share Screen
Record
Reactions
Apps
Leave

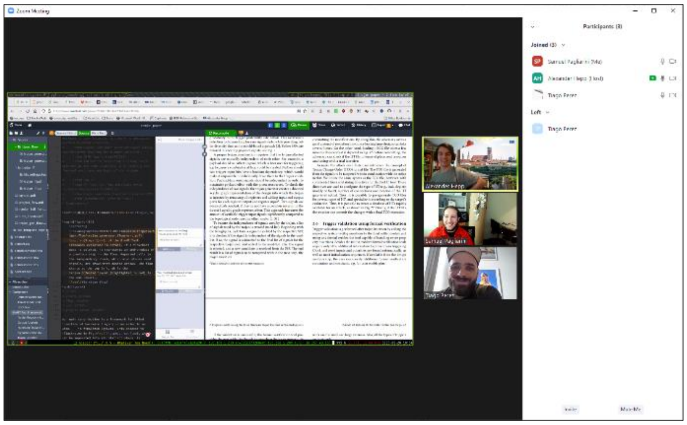
PROJECT REVIEW MEETING

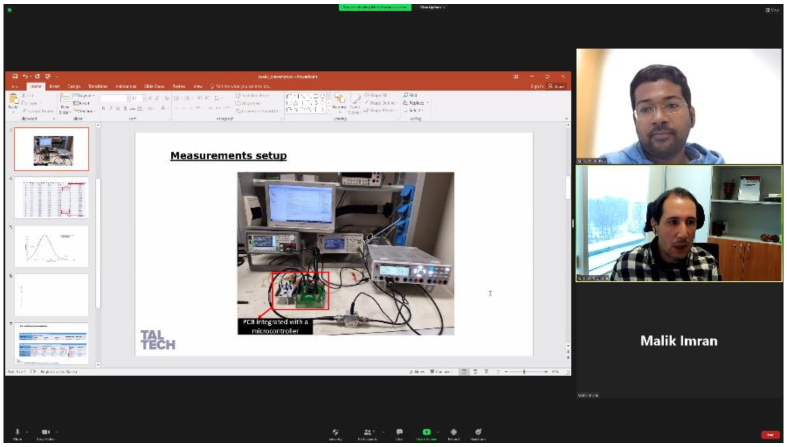
The Review Meeting for the SAFEST Reporting Period 1 (Jan 2021 – March 2022) took place on June 14, 2022 in Zoom with the participation SAFEST Steering Committee (with one representative from each consortium member), EC representative and an independent reviewer. The meeting summarised the reporting documentation submitted by the consortium. Prof. Pagliarini's presentation was followed by several rounds of Q&A. A few follow-up 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 **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.taltech.ee/exchanges-2022/





Measurements setup

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!

NEW PUBLICATIONS

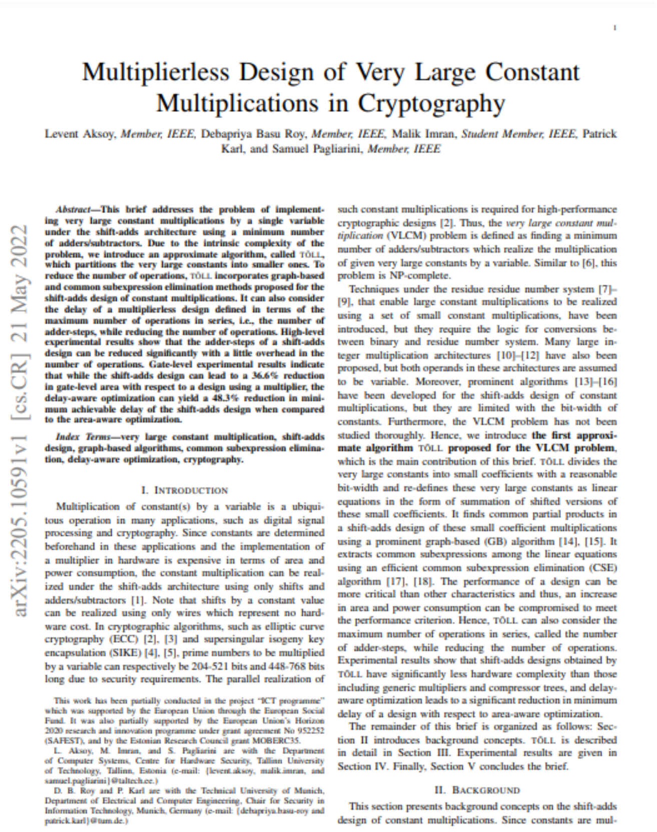
The 2nd half of 2022 was especially prolific for SAFEST-related research. In addition to the aforementioned KaLi paper, three more papers were published:

“Multiplierless Design of Very Large Constant Multiplications in Cryptography” by Levent Aksoy (TalTech), Debapriya Roy (TUM), Malik Imran (TalTech), Patrick Karl (TUM), and Samuel Pagliarini (TalTech) in the journal "IEEE Transactions on Circuits and Systems II". See more at https://arxiv.org/abs/2202.10022

“A Pragmatic Methodology for Blind Hardware Trojan Insertion in Finalized Layouts” by Alexander Hepp (TUM), Tiago Diadami Perez (TalTech), Samuel Pagliarini (TalTech) and Georg Sigl (TUM) at International Conference on Computer-Aided Design (ICCAD). Have a look at https://arxiv.org/abs/2208.09235

“Leveraging Layout-based Effects for Locking Analog ICs” by Muayad Aljafar (TalTech), Florence Azaïs (CNRS), Marie-Lise Flottes (CNRS) and Samuel Pagliarini (TalTech) at ASHES’22: Workshop on Attacks and Solutions in Hardware Security. More info at https://arxiv.org/abs/2209.01856

Congratulations to all authors!



Multiplierless Design of Very Large Constant Multiplications in Cryptography

Levent Aksoy, *Member, IEEE*, Debapriya Basu Roy, *Member, IEEE*, Malik Imran, *Student Member, IEEE*, Patrick Karl, and Samuel Pagliarini, *Member, IEEE*

***Abstract*—This brief addresses the problem of implementing very large constant multiplications by a single variable under the shift-adds architecture using a minimum number of adders/subtractors. Due to the intrinsic complexity of the problem, we introduce an approximate algorithm, called** TÕLL**, which partitions the very large constants into smaller ones. To reduce the number of operations,** TÕLL **incorporates graph-based and common subexpression elimination methods proposed for the shift-adds design of constant multiplications. It can also consider the delay of a multiplierless design defined in terms of the maximum number of operations in series, i.e., the number of adder-steps, while reducing the number of operations. High-level experimental results show that the adder-steps of a shift-adds design can be reduced significantly with a little overhead in the number of operations. Gate-level experimental results indicate that while the shift-adds design can lead to a 36.6% reduction in gate-level area with respect to a design using a multiplier, the delay-aware optimization can yield a 48.3% reduction in minimum achievable delay of the shift-adds design when compared to the area-aware optimization.**

***Index Terms*—very large constant multiplication, shift-adds design, graph-based algorithms, common subexpression elimination, delay-aware optimization, cryptography.**

I. Introduction

Multiplication of constant(s) by a variable is a ubiquitous operation in many applications, such as digital signal processing and cryptography. Since constants are determined beforehand in these applications and the implementation of a multiplier in hardware is expensive in terms of area and power consumption, the constant multiplication can be realized under the shift-adds architecture using only shifts and adders/subtractors [1]. Note that shifts by a constant value can be realized using only wires which represent no hardware cost. In cryptographic algorithms, such as elliptic curve cryptography (ECC) [2], [3] and supersingular isogeny key encapsulation (SIKE) [4], [5], prime numbers to be multiplied by a variable can respectively be 204-521 bits and 448-768 bits long due to security requirements. The parallel realization of such constant multiplications is required for high-performance cryptographic designs [2]. Thus, the *very large constant multiplication* (VLCM) problem is defined as finding a minimum number of adders/subtractors which realize the multiplication of given very large constants by a variable. Similar to [6], this problem is NP-complete.

Techniques under the residue residue number system [7]–[9], that enable large constant multiplications to be realized using a set of small constant multiplications, have been introduced, but they require the logic for conversions between binary and residue number system. Many large integer multiplication architectures [10]–[12] have also been proposed, but both operands in these architectures are assumed to be variable. Moreover, prominent algorithms [13]–[16] have been developed for the shift-adds design of constant multiplications, but they are limited with the bit-width of constants. Furthermore, the VLCM problem has not been studied thoroughly. Hence, we introduce **the first approximate algorithm** TÕLL **proposed for the VLCM problem**, which is the main contribution of this brief. TÕLL divides the very large constants into small coefficients with a reasonable bit-width and re-defines these very large constants as linear equations in the form of summation of shifted versions of these small coefficients. It finds common partial products in a shift-adds design of these small coefficient multiplications using a prominent graph-based (GB) algorithm [14], [15]. It extracts common subexpressions among the linear equations using an efficient common subexpression elimination (CSE) algorithm [17], [18]. The performance of a design can be more critical than other characteristics and thus, an increase in area and power consumption can be compromised to meet the performance criterion. Hence, TÕLL can also consider the maximum number of operations in series, called the number of adder-steps, while reducing the number of operations. Experimental results show that shift-adds designs obtained by TÕLL have significantly less hardware complexity than those including generic multipliers and compressor trees, and delay-aware optimization leads to a significant reduction in minimum delay of a design with respect to area-aware optimization.

The remainder of this brief is organized as follows: Section II introduces background concepts. TÕLL is described in detail in Section III. Experimental results are given in Section IV. Finally, Section V concludes the brief.

II. Background

This section presents background concepts on the shift-adds design of constant multiplications. Since constants are mul-

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 the European Union's Horizon 2020 research and innovation programme under grant agreement No 952252 (SAFEST), and by the Estonian Research Council grant MOBERC35.

L. Aksoy, M. Imran, and S. Pagliarini are with the Department of Computer Systems, Centre for Hardware Security, Tallinn University of Technology, Tallinn, Estonia (e-mail: {levent.aksoy, malik.imran, and samuel.pagliarini}@taltech.ee.)

D. B. Roy and P. Karl are with the Technical University of Munich, Department of Electrical and Computer Engineering, Chair for Security in Information Technology, Munich, Germany (e-mail: {debapriya.basu-roy and patrick.karl}@tum.de.)