





# LightSEC 2025

6th International Workshop on LIGHTWEIGHT CRYPTOGRAPHY FOR **SECURITY & PRIVACY** 

**SEPTEMBER 01-02 2025** CONRAD İSTANBUL BOSPHORUS BEŞİKTAŞ, İSTANBUL, TÜRKİYE



### 1<sup>st</sup> Day:

Welcome & Registration 08.00-09.10

Protocol Security and Efficient Cryptography: 09.10-10.25

Paper 1: Alberto Battistello et al.

JWT Back to the Future: On the (Ab)use of JWTs in IoT Transactions

Paper 2: Gökçe Düzyol and Kamil Otal Leveraging Smaller Finite Fields for More Efficient ZK-Friendly Hash Functions

Pape<mark>r 3: Bar</mark>dia Taghavi et al. LightNTT: A High-Efficiency NTT/iNTT Core for ML-DSA

Coffee Break 10.25-10.55

10.55-12.10 Post-Quantum Cryptography:

Paper 4: Arda Sayo HAPPIER: Hash-bas

ed, Aggregatable, Practical Post-quant<mark>um si</mark>gnatures Implemented Efficiently with Risc0

Paper 5: Martin Feussner and Igor Semaev

Isotropic Quadratic Forms, Diophantine Equations and Digital Signatures (DEFIv2)

Paper 6: Invited paper Sujoy Sinha Roy et al.
Stealthy Hardware Trojan Attacks on MQ-Based Post-Quantum Digital Signatures

12.10-13.25 Lunch

13.25-14.25 **Invited Talk:** 

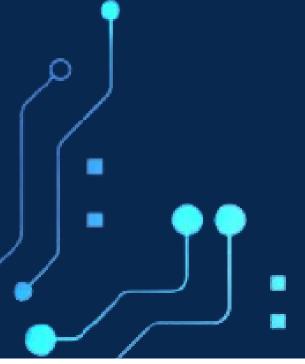
Mark M. Tehranipoor – New Innovation Frontiers with Large Language Models for SoC Security

14.45-17.45

**Bosphorus Tour** 

18.30-20.30

**Banquet Dinner** 



#### **More information**

lightsec2025@sabanciuniv.edu

Click for the conference web page.



**Click** for the registration page.



Funded by the European Union. There will be no registration fee. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union, European Commission or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.







# LightSEC 2025

6th International Workshop on LIGHTWEIGHT CRYPTOGRAPHY FOR **SECURITY & PRIVACY** 

**SEPTEMBER 01-02 2025** CONRAD İSTANBUL BOSPHORUS BEŞİKTAŞ, İSTANBUL, TÜRKİYE



### 2<sup>nd</sup> Day:

09.00-10.15

10.15-10.45

10.45-12.00

08.00-09.00 Registration

Efficient Implementation of Post-Quantum Cryptography:

Paper 7: Rahul Magesh et al.

Unified Multiplier Designs for the FALCON Post-Quantum Digital Signature

Paper 8: Tolun Tosun and Selim Kirbiyik et al.
Optimized FPGA Architecture for Modular Reduction in NTT

Paper 9: Giuseppe Ma<mark>nzoni et</mark> al. An Optimized FrodoKE<mark>M Imple</mark>mentation on Reconfigurable

Hardware

**Coffee Break** 

Hardware and Architecture Security 1:

Paper 10: Asmita Adhikary et al. ARCHER: Architecture-Level Simulator for Side-Channel Analysis

in RISC-V Processors

Paper 11: Lizzy Grootjen et <mark>al.</mark>

MIDSCAN: Investigating the Portability Problem for Cross-Device DL-SCA

Paper 12: Invited paper by Svetla Nikova et al.
Protecting AES-128 Against First-Order Side-Channel Analysis in Micro-Architectures by Enforcing Threshold Implementation

**Principles** 

14.40-15.10

15.10-16.25

25-16.40

#### Hardware and Architecture Security II:

Paper 13: Charilaos Memeletzoglou et al. Hardware Trojan Detection Against Lightweight Block Ciphers

Paper 14: Subhadeep Banik and Francesco Regazzoni Hardware Circuits for the Legendre PRF

Paper 15: Saeed Aghapour et al. Lightweight Fault Detection Architecture for Modular Exponentiation on ARM and FPGA

### **Cryptanalysis and Attacks:**

Paper 16: Mohammad Vaziri and Vesselin Velichkov Cube-Attack-Like Cryptanalysis of Keccak-Based Constructions

Paper 17: Murat Burhan Ilter et al.
Differential and Linear Analyses of DIZY through MILP Modeling

Paper 18: Mohammad Vaziri

Automated Tool for Meet-in-the-Middle Attacks with Very Low

Data and Memory Complexity

Closing remarks

Coffee break

12.00-13.25

Lunch

**More information** 

lightsec2025@sabanciuniv.edu

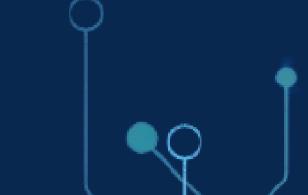
Click for the conference web page.

**Registration** 

Click for the registration page.











Funded by the European Union. There will be no registration fee. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union, European Commission or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.