

Sayı :E-65686120-051-50299
Konu :6. Uluslararası Hafif Sıklet Kriptografi
Güvenlik & Gizlilik Çalıştayı (LightSEC
2025)

07.04.2025

DAĞITIM YERLERİNE

Sabancı Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümümüz ve Horizon Avrupa kapsamında, Prof. Dr. Erkey SAVAŞ tarafından yürütülen "enCRYPTON" başlıklı Twinning Projesi adı altında "6. Uluslararası Hafif Sıklet Kriptografi Güvenlik & Gizlilik Çalıştayı" (LightSEC 2025: 6th International Workshop on Lightweight Cryptography For Security & Privacy) 01-03 Eylül 2025 tarihleri arasında İstanbul'da düzenlenecektir.

Afişi ekte yer alan etkinliğe ilişkin detaylı bilgiye <https://www.encrypton.com/activities/conferences/lightsec-2025/> adresinden ulaşılabilir.

Kongrenin Üniversiteniz bünyesinde bulunan ilgili birimlere ve akademik personele duyurulması hususunda gereğini bilgilerinize arz ederim.

Prof. Dr. Yusuf LEBLEBİCİ
Rektör

Ek:LightSEC2025Poster (2 Sayfa)

Dağıtım:

Gereği:

Abdullah Gül Üniversitesi Rektörlüğüne
Acıbadem Mehmet Ali Aydınlar Üniversitesi
Rektörlüğüne
Adana Alparslan Türkeş Bilim Ve Teknoloji
Üniversitesi Rektörlüğüne
Adıyaman Üniversitesi Rektörlüğüne
Afyon Kocatepe Üniversitesi Rektörlüğüne
Afyonkarahisar Sağlık Bilimleri Üniversitesi
Rektörlüğüne
Afyonkarahisar Sağlık Bilimleri Üniversitesi

Bilgi:

Mühendislik ve Doğa Bilimleri Fakültesi
Dekanlığına

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu:BSFC01N3S

Belge Doğrulama Adresi: <https://www.turkiye.gov.tr/sabancı-universitesi-ebys>

Orta Mahalle, Üniversite Caddesi No:27 Tuzla, 34956 İstanbul
Telefon No:+90 (216) 483 90 00 Faks No:+90 (216) 483 90 05
e-Posta: rektorluk@sabancıuniv.edu.tr İnternet Adresi:<https://www.sabancıuniv.edu/>
Kep Adresi:sabancıuniversitesi@hs03.kep.tr

Bilgi için: Kadriye Kahraman
AB Proje Uzmanı



6th International Workshop on LIGHTWEIGHT CRYPTOGRAPHY FOR SECURITY & PRIVACY LightSEC 2025

SEPTEMBER 01-03 2025 | İSTANBUL, TÜRKİYE

LightSEC 2025 promotes and initiates novel research on security, privacy, and trust issues related to applications that fall under the umbrella of lightweight security. The term “lightweight” refers not only to conventional constraints on metrics such as computational and communication complexity, execution time (both throughput and latency), power, energy, area, memory capacity, and bandwidth, but also to constraints concerning the sizes of ciphertexts, public and private keys, and the compactness of proofs in zero-knowledge protocols.

LightSEC 2025 enthusiastically welcomes papers on algorithms, protocols, techniques, and their secure and efficient implementations for applications utilizing advanced cryptographic algorithms such as homomorphic encryption, zero-knowledge proofs, secure multi-party computation, cryptographic consensus protocols in blockchain applications, threshold cryptography, and post-quantum cryptography.

The conference proceedings will be published in **Springer-Verlag’s LNCS series**.

IMPORTANT DATES

Paper submission deadline

April 18, 2025

Author notification:

May 29, 2025

Camera ready for pre-conference proceedings:

August 1, 2025

Camera ready for post-conference proceedings:

September 15, 2025

Workshop date:

September 1-3, 2025



SCAN HERE!

6th International Workshop on LIGHTWEIGHT CRYPTOGRAPHY FOR SECURITY & PRIVACY LightSEC 2025

SEPTEMBER 01-03 2025 | İSTANBUL, TÜRKİYE

TOPICS OF INTEREST *(but not limited to)**

- Design, analysis and implementation of lightweight, fast, low power or compact cryptographic schemes and protocols
- Cryptographic hardware development for constrained domains
- Side channel and fault analysis and countermeasures on constrained devices
- Efficient and secure post-quantum cryptographic algorithms with special emphasis on side-channel and fault attacks; analysis and countermeasures.
- Security and privacy solutions for 5G/6G networks and beyond
- Security and privacy solutions for IoT.
- Fast, efficient and secure acceleration solutions for cryptographic algorithms and schemes
- Cryptographic solutions for RISC-V ecosystem
- Lightweight solutions for privacy-preserving machine learning on edge devices
- Efficient cryptographic solutions for blockchain applications and its ecosystem
- Formal methods for analysis of lightweight cryptographic protocols
- AI for cryptography
- Security and privacy implications of AI

Session on Lattice-Based and Advanced Cryptographic Algorithms:

We will have a special session on the following subjects, which are supported by enCRYPTON project (<https://www.encrypt-on.com/>), funded by European Union through the Twinning Project 101079319.

- Secure and efficient implementation of lattice-based crypto and homomorphic encryption
- Secure and efficient implementation of post-quantum cryptographic algorithms and schemes
- Acceleration of homomorphic encryption schemes and zero-knowledge protocols via ASIC, FPGA and GPU solutions
- Fast, efficient and compact of new generation zero-knowledge algorithms

General Co-Chairs

Erkay Savaş (Sabancı University)
Cihangir Tezcan (Middle East Technical University)
Orhun Kara (İzmir Institute of Technology)

PC Co-Chairs

Erkay Savaş (Sabancı University)
Amir Moradi (Darmstadt Technical University)
Gregor Leander (Ruhr University Bochum)

Program Committee

- Sedat Akleylek (University of Tartu, Estonia)
- Aydın Aysu (North Carolina State University)
- Lejla Batina (Radboud University)
- Christof Beierle (Ruhr-Uni Bochum)
- Emad Heydari Beni (COSIC - KU Leuven and Nokia Bell Labs)
- Rosario Cammarotta (Intel)
- Yarkin Doröz (NVIDIA)
- Kris Gaj (George Mason University)
- Shibam Ghosh (University of Haifa)
- Lorenzo Grassi (Eindhoven University of Technology)
- Orhun Kara (İzmir Institute of Technology)
- Koray Karabina (University of Waterloo)
- Elif Bilge Kavun (University of Passau)
- Mehran Mozaffari Kermani (University of South Florida)
- Ayesha Khalid (Queen's University Belfast)
- Gregor Leander (Ruhr University Bochum)
- Amir Moradi (Darmstadt Technical University)
- Koksal Mus (WPI)
- Elisabeth Oswald (University of Birmingham)
- Kamil OTAL (TÜBİTAK, BILGEM)
- Melek Önen (EURECOM)
- Berna Örs (Istanbul Technical University)
- Svetla Petkova-Nikova (COSIC, KU Leuven)
- Rachel Player (Royal Holloway, University of London)
- Shahram Rasoolzadeh (Ruhr-Uni Bochum)
- Francisco Rodríguez-Henríquez (Technology Innovation Center: Cryptography Research Centre of the Technology Innovation Centre)
- Kurt Rohloff (Duality Technologies)
- Sujoy Sinha Roy (Graz University of Technology)
- Sadeh Sadeghi (Institute for Advanced Studies in Basic Sciences)
- Erkay Savaş (Sabancı University)
- Patrick Schaumont (WPI)
- Meltem Sönmez Turan (NIST)
- Cihangir Tezcan (Middle East Technical University)
- Ingrid Verbauwhede (KU Leuven)