

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. Erkay 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/sabanci-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@sabanciuniv.edu.tr İnternet Adresi:<https://www.sabanciuniv.edu/>
Kep Adresi:sabanciuniversitesi@hs03.kep.tr

Bilgi için: Kadriye Kahraman
AB Proje Uzmanı



Rektörlüğüne
Ağrı İbrahim Çeçen Üniversitesi Rektörlüğüne
Akdeniz Üniversitesi Rektörlüğüne
Aksaray Üniversitesi Rektörlüğüne
Alanya Alaaddin Keykubat Üniversitesi
Rektörlüğüne
Alanya Üniversitesi Rektörlüğüne
Altınbaş Üniversitesi Rektörlüğüne
Amasya Üniversitesi Rektörlüğüne
Anadolu Üniversitesi Rektörlüğüne
Ankara Bilim Üniversitesi Rektörlüğüne
Ankara Hacı Bayram Veli Üniversitesi
Rektörlüğüne
Ankara Medipol Üniversitesi Rektörlüğüne
Ankara Müzik ve Güzel Sanatlar Üniversitesi
Rektörlüğüne
Ankara Sosyal Bilimler Üniversitesi Rektörlüğüne
Ankara Üniversitesi Rektörlüğüne
Ankara Yıldırım Beyazıt Üniversitesi
Rektörlüğüne
Antalya Belek Üniversitesi Rektörlüğüne
Antalya Bilim Üniversitesi Rektörlüğüne
Ardahan Üniversitesi Rektörlüğüne
Artvin Çoruh Üniversitesi Rektörlüğüne
Ataşehir Adıgüzel Meslek Yüksekokulu
Müdürlüğüne
Atatürk Üniversitesi Rektörlüğüne
Atılım Üniversitesi Rektörlüğüne
Avrasya Üniversitesi Rektörlüğüne
Adnan Menderes Üniversitesi Rektörlüğüne
Bahçeşehir Üniversitesi Rektörlüğüne
Balıkesir Üniversitesi Rektörlüğüne
Bandırma Onyedil Eylül Üniversitesi Rektörlüğüne
Bartın Üniversitesi Rektörlüğüne
Başkent Üniversitesi Rektörlüğüne
Batman Üniversitesi Rektörlüğüne
Bayburt Üniversitesi Rektörlüğüne
Beykoz Üniversitesi Rektörlüğüne
Bezm-i Alem Vakıf Üniversitesi Rektörlüğüne
Bilecik Şeyh Edebali Üniversitesi Rektörlüğüne
Bingöl Üniversitesi Rektörlüğüne
Biruni Üniversitesi Rektörlüğüne
Bitlis Eren Üniversitesi Rektörlüğüne
Boğaziçi Üniversitesi Rektörlüğüne
Bolu Abant İzzet Baysal Üniversitesi
Rektörlüğüne
Burdur Mehmet Akif Ersoy Üniversitesi
Rektörlüğüne
Bursa Teknik Üniversitesi Rektörlüğüne
Bursa Uludağ Üniversitesi Rektörlüğüne
Çağ Üniversitesi Rektörlüğüne

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu:BSFC01N3S

Belge Doğrulama Adresi: <https://www.turkiye.gov.tr/sabanci-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@sabanciuniv.edu Internet Adresi:<https://www.sabanciuniv.edu/>
Kep Adresi:sabanciuniversitesi@hs03.kep.tr

Bilgi için: Kadriye Kahraman
AB Proje Uzmanı



Çanakkale Onsekiz Mart Üniversitesi
Rektörlüğüne
Çankaya Üniversitesi Rektörlüğüne
Çankırı Karatekin Üniversitesi Rektörlüğüne
Çukurova Üniversitesi Rektörlüğüne
Demiroğlu Bilim Üniversitesi Rektörlüğüne
Dicle Üniversitesi Rektörlüğüne
Doğuş Üniversitesi Rektörlüğüne
Dokuz Eylül Üniversitesi Rektörlüğüne
Düzce Üniversitesi Rektörlüğüne
Ege Üniversitesi Rektörlüğüne
Erciyes Üniversitesi Rektörlüğüne
Erzincan Binali Yıldırım Üniversitesi
Rektörlüğüne
Erzurum Teknik Üniversitesi Rektörlüğüne
Eskişehir Osmangazi Üniversitesi Rektörlüğüne
Eskişehir Teknik Üniversitesi Rektörlüğüne
Fatih Sultan Mehmet Vakıf Üniversitesi
Rektörlüğüne
Fenerbahçe Üniversitesi Rektörlüğüne
Fırat Üniversitesi Rektörlüğüne
Galatasaray Üniversitesi Rektörlüğüne
Gazi Üniversitesi Rektörlüğüne
Gaziantep İslam Bilim ve Teknoloji Üniversitesi
Rektörlüğüne
Gaziantep Üniversitesi Rektörlüğüne
Gebze Teknik Üniversitesi Rektörlüğüne
Giresun Üniversitesi Rektörlüğüne
Gümüşhane Üniversitesi Rektörlüğüne
Hacettepe Üniversitesi Rektörlüğüne
Hakkari Üniversitesi Rektörlüğüne
Haliç Üniversitesi Rektörlüğüne
Harran Üniversitesi Rektörlüğüne
Hasan Kalyoncu Üniversitesi Rektörlüğüne
Hatay Mustafa Kemal Üniversitesi Rektörlüğüne
Hitit Üniversitesi Rektörlüğüne
Iğdır Üniversitesi Rektörlüğüne
Isparta Uygulamalı Bilimler Üniversitesi
Rektörlüğüne
Işık Üniversitesi Rektörlüğüne
İbn Haldun Üniversitesi Rektörlüğüne
İhsan Doğramacı Bilkent Üniversitesi
Rektörlüğüne
İnönü Üniversitesi Rektörlüğüne
İskenderun Teknik Üniversitesi Rektörlüğüne
İstanbul 29 Mayıs Üniversitesi Rektörlüğüne
İstanbul Arel Üniversitesi Rektörlüğüne
İstanbul Atlas Üniversitesi Rektörlüğüne
İstanbul Aydın Üniversitesi Rektörlüğüne
İstanbul Beykent Üniversitesi Rektörlüğüne
İstanbul Bilgi Üniversitesi Rektörlüğüne

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu:BSFC01N3S

Belge Doğrulama Adresi: <https://www.turkiye.gov.tr/sabanci-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@sabanciuniv.edu.tr İnternet Adresi:<https://www.sabanciuniv.edu/>
Kep Adresi:sabanciuniversitesi@hs03.kep.tr

Bilgi için: Kadriye Kahraman
AB Proje Uzmanı



İstanbul Esenyurt Üniversitesi Rektörlüğüne
İstanbul Galata Üniversitesi Rektörlüğüne
İstanbul Gedik Üniversitesi Rektörlüğüne
İstanbul Gelişim Üniversitesi Rektörlüğüne
İstanbul Kent Üniversitesi Rektörlüğüne
İstanbul Kültür Üniversitesi Rektörlüğüne
İstanbul Medeniyet Üniversitesi Rektörlüğüne
İstanbul Medipol Üniversitesi Rektörlüğüne
İstanbul Nişantaşı Üniversitesi Rektörlüğüne
İstanbul Okan Üniversitesi Rektörlüğüne
İstanbul Rumeli Üniversitesi Rektörlüğüne
İstanbul Sabahattin Zaim Üniversitesi
Rektörlüğüne
İstanbul Sağlık ve Sosyal Bilimler Meslek
Yüksekokulu Müdürlüğüne
İstanbul Sağlık ve Teknoloji Üniversitesi
Rektörlüğüne
İstanbul Şehir Üniversitesi Rektörlüğüne
İstanbul Şişli Meslek Yüksekokulu Müdürlüğüne
İstanbul Teknik Üniversitesi Rektörlüğüne
İstanbul Ticaret Üniversitesi Rektörlüğüne
İstanbul Topkapı Üniversitesi Rektörlüğüne
İstanbul Üniversitesi Rektörlüğüne
İstanbul Üniversitesi-Cerrahpaşa Rektörlüğüne
İstanbul Yeni Yüzyıl Üniversitesi Rektörlüğüne
İstinye Üniversitesi Rektörlüğüne
İzmir Bakırçay Üniversitesi Rektörlüğüne
İzmir Demokrasi Üniversitesi Rektörlüğüne
İzmir Ekonomi Üniversitesi Rektörlüğüne
İzmir Katip Çelebi Üniversitesi Rektörlüğüne
İzmir Kavram Meslek Yüksekokulu Müdürlüğüne
İzmir Tınaztepe Üniversitesi Rektörlüğüne
İzmir Yüksek Teknoloji Enstitüsü Rektörlüğüne
Kadir Has Üniversitesi Rektörlüğüne
Kafkas Üniversitesi Rektörlüğüne
Kahramanmaraş İstiklal Üniversitesi Rektörlüğüne
Kahramanmaraş Sütçü İmam Üniversitesi
Rektörlüğüne
Kapadokya Üniversitesi Rektörlüğüne
Karabük Üniversitesi Rektörlüğüne
Karadeniz Teknik Üniversitesi Rektörlüğüne
Karamanoğlu Mehmetbey Üniversitesi
Rektörlüğüne
Kastamonu Üniversitesi Rektörlüğüne
Kayseri Üniversitesi Rektörlüğüne
Kırıkkale Üniversitesi Rektörlüğüne
Kırklareli Üniversitesi Rektörlüğüne
Kırşehir Ahi Evran Üniversitesi Rektörlüğüne
Kilis 7 Aralık Üniversitesi Rektörlüğüne
Kocaeli Sağlık ve Teknoloji Üniversitesi
Rektörlüğüne

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu:BSFC01N3S

Belge Doğrulama Adresi: <https://www.turkiye.gov.tr/sabanci-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@sabanciuniv.edu İnternet Adresi:<https://www.sabanciuniv.edu/>
Kep Adresi:sabanciuniversitesi@hs03.kep.tr

Bilgi için: Kadriye Kahraman
AB Proje Uzmanı



Kocaeli Üniversitesi Rektörlüğüne
Koç Üniversitesi Rektörlüğüne
Konya Gıda ve Tarım Üniversitesi Rektörlüğüne
Konya Teknik Üniversitesi Rektörlüğüne
KTO-Karatay Üniversitesi Rektörlüğüne
Kütahya Dumlupınar Üniversitesi Rektörlüğüne
Kütahya Sağlık Bilimleri Üniversitesi
Rektörlüğüne
Lokman Hekim Üniversitesi Rektörlüğüne
Malatya Turgut Özal Üniversitesi Rektörlüğüne
Maltepe Üniversitesi Rektörlüğüne
Manisa Celal Bayar Üniversitesi Rektörlüğüne
Mardin Artuklu Üniversitesi Rektörlüğüne
Marmara Üniversitesi Rektörlüğüne
MEF Üniversitesi Rektörlüğüne
Mersin Üniversitesi Rektörlüğüne
Milli Savunma Üniversitesi Rektörlüğüne
Mimar Sinan Güzel Sanatlar Üniversitesi
Rektörlüğüne
Mudanya Üniversitesi Rektörlüğüne
Muğla Sıtkı Koçman Üniversitesi Rektörlüğüne
Munzur Üniversitesi Rektörlüğüne
Muş Alparslan Üniversitesi Rektörlüğüne
Necmettin Erbakan Üniversitesi Rektörlüğüne
Nevşehir Hacı Bektaş Veli Üniversitesi
Rektörlüğüne
Niğde Ömer Halis Demir Üniversitesi
Rektörlüğüne
Nuh Naci Yazgan Üniversitesi Rektörlüğüne
Ondokuz Mayıs Üniversitesi Rektörlüğüne
Ordu Üniversitesi Rektörlüğüne
Orta Doğu Teknik Üniversitesi Rektörlüğüne
Osmaniye Korkut Ata Üniversitesi Rektörlüğüne
Ostim Teknik Üniversitesi Rektörlüğüne
Özyeğin Üniversitesi Rektörlüğüne
Pamukkale Üniversitesi Rektörlüğüne
Piri Reis Üniversitesi Rektörlüğüne
Recep Tayyip Erdoğan Üniversitesi Rektörlüğüne
Sakarya Uygulamalı Bilimler Üniversitesi
Rektörlüğüne
Sakarya Üniversitesi Rektörlüğüne
Samsun Üniversitesi Rektörlüğüne
Sanko Üniversitesi Rektörlüğüne
Selçuk Üniversitesi Rektörlüğüne
Siirt Üniversitesi Rektörlüğüne
Sinop Üniversitesi Rektörlüğüne
Sivas Bilim ve Teknoloji Üniversitesi
Rektörlüğüne
Sivas Cumhuriyet Üniversitesi Rektörlüğüne
Süleyman Demirel Üniversitesi Rektörlüğüne
Şırnak Üniversitesi Rektörlüğüne

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu:BSFC01N3S

Belge Doğrulama Adresi: <https://www.turkiye.gov.tr/sabanci-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@sabanciuniv.edu.tr İnternet Adresi:<https://www.sabanciuniv.edu/>
Kep Adresi:sabanciuniversitesi@hs03.kep.tr

Bilgi için: Kadriye Kahraman
AB Proje Uzmanı



Tarsus Üniversitesi Rektörlüğüne
Ted Üniversitesi Rektörlüğüne
Tekirdağ Namık Kemal Üniversitesi Rektörlüğüne
Tobb Ekonomi ve Teknoloji Üniversitesi
Rektörlüğüne
Tokat Gaziosmanpaşa Üniversitesi Rektörlüğüne
Toros Üniversitesi Rektörlüğüne
Trabzon Üniversitesi Rektörlüğüne
Trakya Üniversitesi Rektörlüğüne
Türk Hava Kurumu Üniversitesi Rektörlüğüne
Türk-Alman Üniversitesi Rektörlüğüne
Türk-Japon Bilim ve Teknoloji Üniversitesi
Rektörlüğüne
Ufuk Üniversitesi Rektörlüğüne
Uşak Üniversitesi Rektörlüğüne
Üsküdar Üniversitesi Rektörlüğüne
Van Yüzüncü Yıl Üniversitesi Rektörlüğüne
Yalova Üniversitesi Rektörlüğüne
Yaşar Üniversitesi Rektörlüğüne
Yeditepe Üniversitesi Rektörlüğüne
Yıldız Teknik Üniversitesi Rektörlüğüne
Yozgat Bozok Üniversitesi Rektörlüğüne
Yüksek İhtisas Üniversitesi Rektörlüğüne
Zonguldak Bülent Ecevit Üniversitesi
Rektörlüğüne

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Belge Doğrulama Kodu:BSFC01N3S

Belge Doğrulama Adresi: <https://www.turkiye.gov.tr/sabanci-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@sabanciuniv.edu İnternet Adresi:<https://www.sabanciuniv.edu/>
Kep Adresi:sabanciuniversitesi@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)
- Koksai 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)
- Sadegh 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)