



# 7th International Workshop on LIGHTWEIGHT CRYPTOGRAPHY FOR SECURITY & PRIVACY LightSEC 2026

**October 9-10, 2026**  
**AKDENİZ UNIVERSITY, ANTALYA, TÜRKİYE**

LightSEC 2026 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 2026 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

EVENT	DATE
Paper submission deadline:	June 19, 2026
Author notification:	August 21, 2026
Camera ready for pre-conference proceedings:	September 21, 2026
Camera ready for post-conference proceedings:	October 26, 2026
Workshop date:	October 9-10, 2026



# 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

## General Chair

Ahmet SINAĞ (Akdeniz University, Türkiye)

## Program Co-Chairs

Aydın AYSU, Electrical and Computer Engineering, NC State Universit USA

Elif Bilge KAVUN, Faculty of Computer Science, Dresden University of Technology, Dresden, Germany

## Organizing Committee

Murat Ak (Akdeniz University, Antalya)

Sedat Akleylek (University of Tartu, Estonia)

Mustafa Alkan (Akdeniz University, Antalya)

Melis Aslan (FAME CRYPT)

Aslı Bay (Antalya Bilim University, Antalya)

Orhun Kara (İzmir Institute of Technology, Izmir)

Neşe Koçak (ASELSAN Elektronik San. ve Tic. A.Ş.)

Kamil Otal (TÜBİTAK-BİLGE)

Mustafa Özdemir (Akdeniz University, Antalya)

## Program Committee

Sedat Akleylek (University of Tartu)

Erdem Alkim (Ondokuz Mayıs University)

Aydin Aysu (North Carolina State University)

Reza Azaderakhsh (Florida Atlantic University)

Lejla Batina (Radboud University)

Christof Beierle (Ruhr University Bochum)

Emad Heydari Beni (COSIC, KU Leuven &

Nokia Bell Labs)

Shivam Bhasin (Nanyang Technological University)

Begül Bilgin (Rambus)

Rosario Cammarota (Intel Labs)

Yarkın Doröz (NVIDIA)

Krzysztof M. Gaj (George Mason University)

Shibam Ghosh (University of Haifa)

Lorenzo Grassi (Eindhoven University of Technology)

Tim Güneysu (Ruhr University Bochum)

Koray Karabina (University of Waterloo)

Orhun Kara (İzmir Institute of Technology)

Elif Bilge Kavun (Dresden University of Technology)

Mehran Mozaffari Kermani (University of South Florida)

Ayesha Khalid (Queen's University Belfast)

Gregor Leander (Ruhr University Bochum)

Amir Moradi (Darmstadt Technical University)

Debdeep Mukhopadhyay (Indian Institute of Technology Kharagpur)

Köksal Mus (Worcester Polytechnic Institute – WPI)

Kamil Otal (TÜBİTAK BİLGE)

Elisabeth Oswald (University of Birmingham)

Melek Önen (EURECOM)

Svetla Petkova-Nikova (KU Leuven)

Rachel Player (Royal Holloway, University of London)

Shahram Rasoolzadeh (Ruhr University Bochum)

Francisco Rodríguez-Henríquez

(Technology Innovation Institute – Cryptography Research Centre)

Kurt Rohloff (Duality Technologies)

Sujoy Sinha Roy (Graz University of Technology)

Erkay Savaş (Sabancı University)

Özgür Sinanoğlu (New York University Abu Dhabi)

Cihangir Tezcan (Middle East Technical University)

Meltem Sönmez Turan (NIST)