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

SCAN HERE!

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