7th International Workshop on LIGHTWEIGHT CRYPTOGRAPHY FOR SECURITY & PRIVACY

(LightSEC 2026)

October 9-10, 2026, Akdeniz University, Antalya, Türkiye

ABOUT LightSEC 2026

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. As new applications based on novel and advanced cryptographic schemes become increasingly ubiquitous and provide immense value to society across sectors such as AI, blockchain, IoT, and 5G/6G, they also impact a larger portion of the public, raising numerous security and privacy concerns that must be thoroughly addressed before widespread deployment. LightSEC 2026 enthusiastically welcomes papers on algorithms, protocols, techniques, and their secure and efficient implementations for applications that utilise 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.

IMPORTANT DATES

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

CONFERENCE WEBSITE & E-MAIL

Website: https://lightsec2026.com/

E-mail: info@lightsec2026.com

*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 their ecosystem
- Formal methods for analysis of lightweight cryptographic protocols
- AI for cryptography
- Security and privacy implications of AI

SUBMISSION INSTRUCTIONS

Submissions must be anonymous, with no author names, affiliations, or obvious identifying references. Submissions must not substantially duplicate work that any of the authors has published in a journal or a conference/workshop with proceedings, or has submitted or plans to submit before the author notification deadline to a journal or other conferences/workshops that have proceedings. Accepted submissions may not appear in any other conference or workshop that has proceedings.

LightSEC 2026 is a refereed workshop. All submissions will undergo a rigorous double-blind peer-review process conducted by the Program Committee and external reviewers.

The proceedings will be published in Springer-Verlag's LNCS series. Hence, the final version of accepted papers must follow the LNCS guidelines (https://www.springer.com/gp/computer-science/lncs), using Springer's standard fonts, font sizes, and margins, with a total page limit of 20 pages including references and appendices. Submissions to LightSEC 2026 must follow the same format. Clearly marked supplementary materials may be appended without a page limit, but reviewers are neither required to read them nor will they be printed in the proceedings. Hence, papers must be intelligible and self-contained within the 20-page bound.

Submission website: http://www.easychair.org/conferences/?conf=lightsec2026

PREVIOUS PROCEEDINGS

1. LightSec 2011 - 2011 Workshop on Lightweight Security & Privacy: Devices, Protocols, and Applications, 14 -15 March 2011, İstanbul, Türkiye
2. LightSec 2013, 2nd International Workshop, LightSec 2013, Gebze, Turkey, May 6-7, 2013
3. LightSec 2014, Third International Workshop, LightSec 2014, Istanbul, Turkey, September 1-2, 2014
4. LightSec 2015, 4th International Workshop, LightSec 2015, Bochum, Germany, September 10-11, 2015
5. LightSec 2016, 5th International Workshop, LightSec 2016, Aksaray, Turkey, September 21-22, 2016
6. LightSec 2025, 6th International Workshop, LightSec 2025, Isttanbul, Turkey, September 01-02, 2025

CONFERENCE ORGANISATION

General Chair:

- Ahmet SINAK (Akdeniz University, Türkiye)

Program Co-Chairs:

- Aydın AYSU (Electrical and Computer Engineering, North Carolina State University, 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, Ankara)
- Aslı Bay (Antalya Bilim University, Antalya)
- Orhun Kara (İzmir Institute of Technology, İzmir)
- Neşe Koçak (ASELSAN Elektronik San. ve Tic. A.Ş, Ankara)
- Kamil Otal (TÜBİTAK-BİLGEM, Gebze)
- Mustafa Özdemir (Akdeniz University, Antalya)

Program Committee:

- Sedat Akleylek (University of Tartu)
- Erdem Alkim (Ondokuz Mayıs University)
- Aydin Aysu (North Carolina State University)
- Reza Azarderakhsh (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 BİLGEM)
- 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)