



## 4th Workshop on Enabling Security, Trust, and Privacy in 6G Wireless Systems

### Steering Committee

Arsenia Chorti  
Gerhard Fettweis  
Eduard Jorswieck  
Philippe Sehier

### General Chair

Thuy Pham

### TPC Chairs

Albena Mihovska  
Gunes Karabulut-Kurt  
Stefano Tomasin  
Rafael Schaefer

### TPC Members

Linda Senigagliesi  
Muralikrishnan  
Srinivasan  
Bharat S. Rawal  
Francesco Ardizzon  
Stefan Köpsel  
Maode Ma  
Marco Baldi  
Sara Berri  
Antoni Ivanov  
Haotong Cao  
Peter Langendörfer  
Onur Günlü

### Important Deadlines

**Paper submission:**  
25 January 2025

**Acceptance notification:**  
28 February 2025

**Camera-ready due:**  
15 March 2025

The 4<sup>th</sup> Workshop on Enabling Security, Trust, and Privacy in 6G Wireless Systems will take place on 8<sup>th</sup> June 2025 in Montreal, Canada. The objective of the workshop is to both foster and develop the ground-breaking technique to provide trustworthy and resilient wireless communications. In line with such objectives, original contributions are solicited in topics of interest to include, but not limited to, the following:

- Physical layer security for 6G
- Trust and trustworthiness in 6G
- Secure signal processing
- Information theoretic security
- Security verification and performance metrics
- Cross-layer security solutions
- 5G/6G security (false base station attacks, sidelink security, integration of new services)
- Zero-touch security solutions
- Context-aware, semantic security
- Covert wireless communications
- Physical layer authentication and key agreement
- Security and privacy for IoTs, HetNets, massive MIMO systems, and mm-wave, THz transmission
- Security and privacy of joint communications and sensing / integrated sensing and communication
- Interplay between emerging technologies (intelligent reflecting surface, joint communication and sensing, AI) and their role towards trustworthy communication
- Hardware security
- Attack/defense modelling (active and jamming attacks, man-in-the-middle attacks, etc.)
- Post-Quantum security and cryptography
- Security challenges for AI/ML technologies
- Security of space information systems
- Optical wireless technology for secure connectivity
- Security mechanisms for zero-energy devices
- Security-aware access control
- AI-based security solutions for wireless systems
- Prototype, practical testbeds, and performance evaluation

### Submission Guidelines:

Authors are invited to submit original papers of up to 6 pages including figures, tables, and references, in PDF format, for possible publication in IEEE ICC 2025 Conference Proceedings, which will be included in IEEE Digital Library. Submission implies that at least one of the authors will register and present the paper at the conference.