move beyond.

11th International Conference On Smart And Sustainable Technologies

Split - Bol // June 23-26, 2026

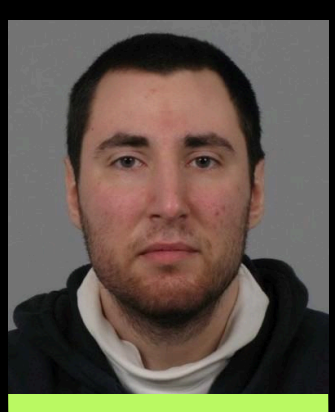
Special Session

Neuromorphic RFID, Hardware Security and Post-Quantum Cryptography for Edge Identification

ORGANIZERS

ALBERTO ARCIELLO
Mediterranea University of Reggio Calabria, Italy

SHEKOUFEH NEISARIAN
University of Passau, Germany



NIKOLAOS ATHANASIOS ANAGNOSTOPOULOS
International Hellenic University, Greece

CALL FOR PAPERS

Neuromorphic computing, emerging non-volatile memories (eNVMs) and novel materials are enabling a new generation of RFID and battery-less edge devices that embed sensing, in-memory computing, identification and hardware security functions directly in the physical substrate. Along with intelligent on-tag processing, next-generation edge devices must provide hardware-rooted trust, intrinsic identity and quantum-resilient security guarantees under strict constraints in power, area and energy harvesting capability. Emerging memristive technologies (ReRAM, PCM, OxRAM, etc.), spiking circuits, crossbar arrays, mixed-signal front-ends, and FPGA-based prototypes offer unique opportunities to co-design computation and security at the device, circuit and architectural levels.

This Special Session invites hardware-level contributions that demonstrate how neuromorphic architectures and emerging materials can enable intrinsic unclonable identities and hardware-rooted security primitives, support secure key generation and storage directly within memory technologies and provide true random number generation through entropy extracted from device variability. It also welcomes works on lightweight and post-quantum cryptographic implementations designed for ultra-low-power, battery-less platforms or resource-constrained devices as well as approaches for quantum-resilient authentication and key-exchange mechanisms targeting RFID systems and edge nodes.

The session is specifically intended for young researchers (PhD students and postdoctoral researchers), providing a focused forum to present experimental results, receive technical feedback and foster interdisciplinary collaborations within this context across neuromorphic computing, hardware security and post-quantum cryptography.

Topics of Interest

We welcome original contributions that address, but are not limited to, the following areas:

- Neuromorphic RFID hardware for on-tag identification and sensing
- Integration and reliability analysis of memristive and eNVM technologies
- Novel materials and prototyping methodologies for neuromorphic tags
- Crossbar arrays and mixed-signal architectures for spiking and event-driven systems
- Hardware implementation of Spiking Neural Networks (SNNs) for ultra-low-power platforms
- FPGA and reconfigurable hardware for rapid system prototyping
- Physical Unclonable Functions (PUFs) based on emerging and memristive devices
- Hardware randomness sources and true random number generators (TRNGs) for ultra-low-power and RF-powered platforms
- Secure key storage and hardware root-of-trust architectures for constrained and battery-less systems
- Anti-tamper, anti-counterfeiting and secure boot with hardware-based attestation mechanisms
- Side-channel, fault-injection and variability-aware security mitigation techniques in neuromorphic circuits
- Efficient and hardware-accelerated implementations of post-quantum cryptographic schemes with architectural optimization and bottleneck analysis
- Side-channel security analysis and fault evaluation of hardware implementations of post-quantum cryptography on FPGA and ASIC platforms
- Memory- and latency-optimized post-quantum-secure architectures for RFID and constrained edge platforms
- Hybrid classical–post-quantum authentication and quantum-resilient key exchange protocols
- Energy-aware and cryptographic co-design strategies for neuromorphic and in-memory computing systems
- Cross-layer hardware–software co-design and resilient architectures for secure neuromorphic systems
- Secure edge accelerators integrating computation and hardware roots of trust
- Distributed trust models and security benchmarking frameworks for emerging-material and edge platforms

FULL PAPER SUBMISSION:
February 20, 2026

SUBMIT PAPER HERE

Notification of acceptance:
April 17, 2026
Camera ready paper:
May 1, 2026

Visit our website for more information
https://splitech.org/