



4th Workshop on Nano Security (NanoSec'26)

From Nano-Electronics to Secure Systems

(co-located with Design, Automation and Test in Europe)

April 20 – 22, 2026, Verona, Italy

<https://spp-nanosecurity.uni-stuttgart.de/nanosec26>

Call for Papers

Today's societies critically depend on electronic systems. Security of such systems are facing completely new challenges due to the ongoing transition to radically new types of nano-electronic devices, such as memristors, spintronics, or carbon nanotubes. The use of such emerging nano-technologies is inevitable to address the essential needs related to energy efficiency, computing power and performance. These technologies come with new properties and also facilitate the development of radically different computer architectures.

The fourth edition of the workshop will bring together researchers from hardware-oriented security and emerging hardware technology. It will explore the potential of new technologies and architectures for achieving security targets, but also raise questions about their vulnerabilities to new types of hardware-oriented attacks.

The workshop invites submissions on, but not limited to, the following topics:

- **Nano-electronic security primitives**, such as physical unclonable functions, random number generators, cryptographic blocks, reconfigurable nano-fabrics, or obfuscation/camouflaging structures
- **Integration of secure primitives** into larger systems, protocols and architectures, translating security guarantees for lower-level primitives in higher-order, system- and architecture-level security properties
- **Attacks against systems with nano-electronic components**, including side-channel analysis, fault injection, microarchitectural covert channels, and countermeasures against such attacks

This year, the workshop will feature a **Special Session on Secure Compute-in-Memory Architectures**, organized by Prof. Mahdi Fazeli (Halmstad University) and Prof. Ahmad Patooghy (North Carolina A&T University)

A submission can describe a novel scientific result, provide a position statement about a new and relevant problem, or report a case study on practical experiences with a technique from the list above. The submissions should not be formally published in the past. The workshop will have no formal proceedings, so authors will be free to resubmit their work to conferences or journals. Accepted papers can, at the discretion and with an approval of their authors, be published on the workshop's website.

Author instructions: Submit full 6-page papers or 1-2 page extended abstracts (in IEEE double-column format, A4 or US Letter) through EasyChair. **You will be able to indicate during submission whether you are submitting to the regular program or to the Special Session on Secure Compute-in-Memory Architectures.**

<https://easychair.org/conferences/?conf=nanosec25>

Key dates:

Submission deadline: **February 2, 2026**

Acceptance notification: February 16, 2026

PDF file for publishing on the workshop's website (optional): March 10, 2026

Registration: This workshop is co-located with the DATE Conference and will use its registration facilities. Please register through <https://www.date-conference.com/registration> The early-bird deadline is March 4, 2026

Workshop organizers:

Iliia Polian, University of Stuttgart, Germany

Nan Du, Friedrich Schiller University Jena, Germany

Yunsi Fey, Northeastern University, Boston, USA

Shahar Kvatinsky, Technion – Israel Institute of Technology

Fareena Saqib, University of North Carolina, Charlotte, USA

The workshop is organized by the DFG Priority Program Nano Security
<https://spp-nanosecurity.uni-stuttgart.de/>

