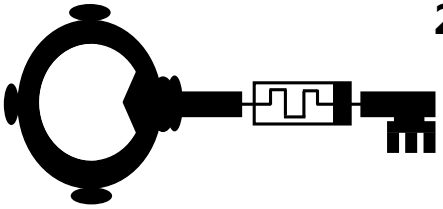

2nd Workshop on Nano Security (NanoSec'24)

From Nano-Electronics to Secure Systems

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

March 25, 2024, Valencia, Spain

https://spp-nanosecurity.uni-stuttgart.de/nanosec24

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. Therefore, the entire industry are switching to emerging nano-electronics alongside scaled CMOS technologies in heterogeneous integrated systems. These technologies come with new properties and also facilitate the development of radically different computer architectures.

The second edition of the workshop will bring together researchers from hardware-oriented security and from emerging hardware technology. It will explore the potential of new technologies and architectures to provide new opportunities for achieving security targets, but it will 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 defined and validated 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

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: Submissions in form of full 6-page papers or 1-2 page extended abstracts (in IEEE double-column format, either A4 or US Letter) should be submitted through EasyChair:

https://easychair.org/conferences/?conf=nanosec24

Key dates:

Submission deadline: **January 15, 2024**

Acceptance notification: January 25, 2024

PDF file for publishing on the workshop's website (optional): March 10, 2024

Workshop: March 25, 2024 14:00-18:00

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 January 24, 2024

Workshop organizers:

Ilia Polian, University of Stuttgart, Germany

Nan Du, Friedrich Schiller University Jena, Germany

Shahar Kvatinsky, Technion – Israel Institute of Technology

Ingrid Verbauwhede, KU Leuven, Belgium

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