Universität Stuttgart

Press release
28.5.2019

# Cyber defense for nanoelectronics

## New DFG Priority Program “Nano Security” at the University of Stuttgart

**Whether it’s cars, industrial plants or the government network, spectacular cyber attacks over the past few months have shown how vulnerable modern electronic systems are. The aim of the new Priority Program “Nano Security”, which is coordinated by the University of Stuttgart, is protecting you and preventing the cyber attacks of the future. The program, which is funded by the German Research Foundation (DFG), emphasizes making the hardware into a reliable foundation of a system or a layer of security.**

The economy, science and society are now highly dependent on electronic systems, and yet these can be cracked by just a couple of smart hackers – with catastrophic effects. However, the security measures are full of holes. The majority of cyber defense systems on the market concentrate on protecting the software components of electronic systems or their communication interfaces. However, advances in production technology and the increasing complexity of hardware have meant that attackers now increasingly focus on the hardware. There is increasing evidence of major successful attacks on hardware which has been produced using the latest microelectronics technology, including security loopholes such as Rowhammer, Meltdown and Spectre.

### The challenges of nanoelectronics

Completely new challenges also emerge as a result of the switch to radically new nanoelectronic components, which for example are used to master the challenges of the future in terms of energy efficiency, computing power and secure data transmission. For example,


**University Communications**

**Head of University Communications and Press Spokesperson**
Dr. Hans-Herwig Geyer

Contact
T +49 (0)711 685-82555

**Contact person**
Andrea Mayer-Grenu

**Contact**
T +49 (0)711 685-82176
F +49 (0)711 685-82291
hkom@uni-stuttgart.de

memristors (components which are not just used to store information but also function as logic modules), the spintronics, which exploit quantum-mechanical effects, or carbon nanotubes.

The new technologies, as well as the fundamentally different computer architecture associated with them, offer new opportunities for cryptographic primitives in order to achieve an even more secure data transmission. However, they also raise questions about their vulnerability to new types of hardware attacks.

## The problem is part of the solution

In this context, a better understanding should be developed of what consequences the new nanoelectronic technologies have for the security of circuits and systems as part of the new Priority Program. Here, the hardware is not just thought of as part of the problem but also as an important and necessary part of the solution to security problems. The starting points here for example are the hardware-based generation of cryptographic keys, the secure storage and processing of sensitive data, and the isolation of system components which is guaranteed by the hardware. Lastly, it should be ensured that an attack cannot be spread further by the system.

In this process, the scientists want to assess the possible security risks and weaknesses which stem from the new type of nanoelectronics. Furthermore, they want to develop innovative approaches for system security which are based on nanoelectronics as a security anchor.

The Priority Program promotes cooperation between scientists, who develop innovative security solutions for the computer systems of the future on different levels of abstraction. Likewise, it makes methods available to system designers to keep ahead in the race between attackers and security measures over the next few decades.

## The call has started

The DFG Priority Program “Nano Security. From Nano-Electronics to Secure Systems“ (SPP 2253) is scheduled to last for a period of six years. The call for projects for the first three-year funding period was

advertised a few days ago, and the first projects are set to start at the beginning of 2020.

**Further information (in English):** https://spp-nanosecurity.uni-stuttgart.de/

**Specialist contact:**

Prof. Ilia Polian, University of Stuttgart, Institute of Computer Architecture and Computer Engineering, Phone: + 49 (711) 685 60 764, E-mail: ilia.polian (at) informatik.uni-stuttgart.de

**Press contact:**

Andrea Mayer-Grenu, University of Stuttgart, University Communications, Tel. +49 (711) 685 82176,
E-mail: andrea.mayer-grenu (at) hkom.uni-stuttgart.de