Faculty of Computer Science

At the **Institute of Computer Engineering,** the **Chair of Processor Design** offers a project position in a collaborative project which aims to design hardware security solutions using reconfigurable transistors to enable secure circuits as

Research Associate

(subject to personal qualification employees are remunerated according to salary group E 13 TV-L)

starting **as soon as possible**.

Research area: **SecuReFET: Secure Circuits through inherent Reconfigurable FET**

Terms: Balancing family and career is an important issue. The position is basically suitable for candidates seeking part-time employment as well with at least 50% of the fulltime weekly hours.
The position is limited initially for three years. The period of employment is governed by the Fixed Term Research Contracts Act (Wissenschaftszeitvertragsgesetz – WissZeitVG).

The project is granted by the DFG (German Research Foundation) under the Special Priority Program on "Nano Security: From Nano-Electronics to Secure Systems". The project SecuReFET will be carried out in collaboration with the NaMLab gGmbH Dresden.

Position and Requirements

At the Chair of Processor Design we have the long-term vision of shaping the way future electronic systems are to be designed.
Today's societies critically depend on electronic systems. Over the last years, the security of these systems has been at risk by a number of hardware-level attacks that circumvent software-level security mechanisms. Solutions based on classical CMOS electronics have been shown to be either cost intensive due to a high area overhead or energy inefficient. One promising alternative against such hardware level attacks are security primitives based on emerging reconfigurable nanotechnologies. Transistors based on these disruptive reconfigurable nanotechnologies, termed as *Reconfigurable Field-Effect Transistors* (RFETs), offer programmable p- and n-type behavior from a single device. The runtime-reconfigurable nature of these nano-electronic devices yields to an inherent polymorphic functionality at the logical abstraction. As a result, circuits made of regular RFET blocks are able to provide a large number of possible functional combinations based on the apparently same circuit representation. The manufacturers, therefore, are able to program the desired functionality after chip production. The big difference to standard CMOS electronics is, that the actual circuit or function remains hidden since they cannot be differentiated from other possible combinations by physical reverse engineering.
In SecuReFET, methodologies and circuits will be developed exploiting the inherent polymorphic property of RFETs. RFET-based security-primitives, such as *Physically Unclonable Functions* (PUFs) which aim to protect proprietary IP designs, will be designed, modeled, manufactured and measured. The benefit of those cells regarding their resilience against side-channel attacks and reverse engineering will be demonstrated. In addition, potential security threats stemming from the very same reconfigurable nature of the technology, such as hardware Trojans, will be investigated.

Measures to mitigate those vulnerabilities by circuit as well as device-design will be explored. Furthermore, an RFET-compatible automated design-synthesis environment (EDA) for logic and physical design of secure circuits will be established based on the modified modern design rules. Finally, the developed concepts will be verified and benchmarked by means of modern security tests.

Tasks:

- work in collaboration with the NaMLab gGmbH, Dresden
- design secure circuits with reconfigurable field effect transistors
- identify the side-channel vulnerabilities in modern circuits
- design an RFET-compatible automated design-synthesis environment for logic and physical design of security circuits
- publish the works in international conferences and/or journals.

Requirements:

- university degree in electrical engineering or computer science
- a deep understanding of the EDA flow from design specification to place and route
- strong background in HDL either Verilog or VHDL
- strong foothold in security principles
- understanding of reconfigurable circuits will be an added advantage
- good knowledge of Computer Architecture and algorithm design
- good communication skills
- proficiency in C/C++ or any other programming language.

What we offer

You will join a team of enthusiastic researchers who pursue creatively their individual research agenda. Other ongoing projects at the Chair of Processor Design can be found at https://www.cfaed.tu-dresden.de/pd-about. The chair is a part of the Cluster of Excellence **"Center for Advancing Electronics Dresden"**, which offers plenty of resources and structures for career development.

Informal enquiries can be submitted to Prof. Dr. Akash Kumar, Tel +49 (351) 463 39274; Email: akash.kumar@tu-dresden.de

Applications from women are particularly welcome. The same applies to people with disabilities.

Application Procedure

Please submit your comprehensive application **(in English only)** including the following: motivation letter, CV, copy of degree certificate, transcript of grades (i.e. the official list of coursework including your grades) and proof of English language skills preferably via the TU Dresden Secure-Mail Portal https://securemail.tu-dresden.de by sending it as a single pdf document quoting the reference number **PhD20-05-PD** in the subject header to **recruiting.cfaed@tu-dresden.de** or by post to: **TU Dresden, Fakultät Informatik, Institut für Technische Informatik, Professur für Prozessorentwurf, Prof. Akash Kumar, Helmholtzstr. 10, 01069 Dresden, Germany**. The closing date for applications is **11.08.2020** (stamped arrival date of the university central mail service applies). Please submit copies only, as your application will not be returned to you. Expenses incurred in attending interviews cannot be reimbursed

---