平成３０年１月２４日

Kyutech
Kyushu Institute of Technology

DISC
International

# 九州工業大学
# ディペンダブル集積システム研究センター（DISC）

# 特別セミナーのご案内

**日時：** 平成30年2月15日（火） 10:00〜14:00

**場所：** 九州工業大学サテライト福岡天神
福岡市中央区天神 1-7-11 イムズビル 11 階

**講師：** Prof. Bernd Becker
University of Freiburg, Germany

**内容：**

## Towards Automatic Construction of Algebraic Fault Attacks

**概要：**

New applications in embedded, cyberphysical and internet of-things (IoT) domains increasingly incorporate access to and processing of sensitive data. Privacy and integrity of these data typically are achieved by (lightweight) cryptographic primitives often implemented as application-specific hardware blocks aiming at minimizing area, energy, etc.. Security functions in hardware to which a potential attacker has direct access makes them vulnerable to a range of physical attacks, including (passive) side-channel analysis and fault-injection attacks.

We report on AutoFault, a prototypic framework to quickly evaluate the resistance of security-critical hardware blocks to fault attacks. AutoFault can be employed for three main tasks in the course of cipher design and analysis: pre-silicon analysis, postsilicon analysis, and analysis of countermeasures. The framework takes as inputs solely the circuit description of the cipher and the fault(s) and produces an algebraic formula that can be handed over to an external (SAT-)solver. We demonstrate successful application of AutoFault (in pre-silicon mode) to LED-64 and to small-scale AES. To the best of our knowledge, this is the first time that a state-of-the-art cipher (LED-64) was broken by a fault attack with no prior manual cryptanalysis whatsoever. We also present first results on the performance of AutoFault using the data of physical fault injections on an FPGA board.

連絡先： 温暁青
九州工業大学大学院情報工学研究院
情報創成工学研究系
Tel: 0948-29-7891
Email: wen@cse.kyutech.ac.jp

平成３０年１月２４日

# 講師プロフィール

**Bernd Becker** is a Full Professor at the Faculty of Engineering, University of Freiburg, Germany.

The research activities of Bernd Becker have been primarily in the area of computer-aided design, test and verification of (digital) circuits and systems (VLSI CAD). A focus of his research is the development and analysis of efficient data structures and algorithms in VLSI CAD. More recently, he has been working on security and verification methods for embedded systems and test techniques for nanoelectronic circuitry.

He has published more than 300 papers in peer-reviewed conferences and journals and has been the holder of several research grants from DFG, BMBF and industry as well. In particular, he has been the Co-Speaker of the DFG Transregional Collaborative Research Center "Automatic Analysis and Verification of Complex Systems (AVACS)" with project partners from University of Freiburg, University of Saarland, University of Oldenburg and Max Planck Institute of Computer Science. Currently, he is a director of the Freiburg Center for Security and Society

Bernd Becker is a fellow of IEEE and a member of Academia Europaea.