The interest group Angewandte Kryptographie of Gesellschaft für Informatik e.V. hosts

27th Crypto-Day

7.-8. December 2017
Im Technologiepark 25, 15236 Frankfurt (Oder), Germany

Ambition and Program: The Crypto-Day aims at providing an opportunity for early-stage researchers in the field of cryptography and IT-security to exchange knowledge and establish networks to universities as well as to industry (e.g. for collaboration across Germany, or to find out about research internships and post-doc positions). Therefore, we invite students, doctoral candidates, and experienced researchers to present their research results or research ideas in the form of 20 minute presentations on this upcoming Crypto-Day.

Schedule (tentative)

Thu 13:00-17:00	Talks
Thu 17:10-17:55	GI Fachgruppentreffen "Angewandte Kryptographie"
Thu 18:00-22:00	Social event
Fri 09:00-13:00	Talks

Host: The IHP is an institute of the Leibniz Association and conducts research and development of silicon-based systems and ultra high-frequency circuits and technologies including new materials. It develops innovative solutions for application areas such as wireless and broadband communication, security, medical technology, industry 4.0, automotive industry, and aerospace. The sensor networks group is working in the field of hardware accelerators for cryptographic operations for more than 10 years. Its research is embedded into national and international projects. The recent focus is on tamper resistant design approaches especially for elliptic curve cryptography. As part of the Kryptotag we will offer the opportunity of guided tours "through" our class1 clean room, HW crypto lab, focused ion beam station and test laboratory.

Topics: The presented talks shall cover a broad spectrum from the field of cryptography or IT-security. We invite presentations of work-in-progress, contributions, which may be submitted to a conference, or summarize findings from a thesis or dissertation.
Submitted articles corresponding to the presentations will be arranged in a technical report. Therefore, submissions will be quotable publications and will be published on the web page. Observe that this does not forbid the publication of the result at other conferences or journals.

Attendance: There are **no participation fees**.

Submission: Please submit an abstract of your talk (**one DIN A4 page**). To simplify generation of the technical report, we request you to only use the LaTeX template of the cryptography group and to provide the PDF file additionally to the LaTeX sources.

Further Information (Program, Venue, LaTeX-template): http://www.kryptotag.de/

Submission/Registration:	Until **15 November 2017**, per email at kryptotag@lists.bit.uni-bonn.de
Organisation:	Zoya Dyka, IHP GmbH Michael Nüsken, b-it, Universität Bonn Frederik Armknecht, Universität Mannheim