



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

# 29<sup>th</sup> Crypto-Day

06.– 07.09.2018

**Robert Bosch GmbH Zentrum für Forschung und Voraentwicklung  
Robert-Bosch-Campus 1, 71272 Renningen, 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:** [Robert Bosch GmbH](http://www.kryptotag.de) hosts the Crypto-Day 2018 at the research campus in Renningen. On an area of 100ha nearly 1,400 associates work on the many disciplines of science and technology. Humans expect a life in the 'Human-Machine-Society' where smart machines provide ubiquitous and seamless support. Therefore future systems need to be connected, intelligent, autonomous, personalized and organize themselves across domains and applications. Automated driving is only one of the

manifold research highlights at Bosch. The research group Safety, Security and Privacy is interested in all aspects of computer security and privacy, especially when combined with questions regarding safety and efficiency. The goal of security research at Bosch is to enable focal points such as automated, electrified & energy efficient and connected technologies.

**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 August 2018**, by email to [kryptotag@lists.bit.uni-bonn.de](mailto:kryptotag@lists.bit.uni-bonn.de)

**Organisation:** Christopher Huth, Robert Bosch GmbH  
Michael Nüsken, b-it, Universität Bonn  
Frederik Armknecht, Universität Mannheim