



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

31st Crypto-Day

17/18 October 2019

Qualcomm CDMA GmbH, Kurfürstendamm 21, 10719 Berlin, Germany

Ambition and Program: 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 and connections 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

Thu	13:00-18:00	Talks (incl. coffee break)
Thu	18:30-23:00	Social event (incl. dinner)
Fri	09:00-13:00	Talks (incl. lunch)

Host: Qualcomm invents breakthrough technologies that transform how the world connects, computes and communicates. Qualcomm is an R&D engine, and our foundational technologies have connected billions of people for more than 30 years. Our technology is in nearly every smartphone in the world. We invented CDMA, pioneered 3G and 4G, and are leading the way to 5G and a new era of intelligent, connected devices. QPSI is the product security initiative within Qualcomm responsible for improving security of our products throughout all stages of the product development lifecycle. In order to do so, QPSI employs a strong group of security researchers working from many countries. We work in vari-

ous teams to research the latest security technologies and develop solutions that focus both on hardening the security foundations of our products and on vulnerability detection and mitigations. QPSI hosts a vulnerability rewards program and is responsible for Qualcomm's product security incident response. We regularly issue security bulletins to our customers and later to the public to increase transparency and public awareness.

Topics: Presented talks should cover a broad spectrum from the field of cryptography or IT-security. We invite presentations of work-in-progress, contributions that may be submitted to a security conference, or a summary of findings from a thesis or dissertation. A technical report will be arranged from the submitted articles corresponding to the presentations. Therefore, submissions will be quotable publications and will be published on the web page. Please note that this does not forbid the publication of presentations or papers at other conferences or journals.

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

Submission: Please submit an abstract of your talk (**one DIN A4 page**) along with the granting of rights form for consideration. 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.

Further Information (Program, Venue, LaTeX-template): http://www.kryptotag.de/	
Submission / Registration:	Until 22 September 2019 , per email at kryptotag@lists.bit.uni-bonn.de
Organisation:	Marcel Selhorst, Qualcomm CDMA GmbH Daniel Loebenberger, Fraunhofer AISEC, Weiden i.d.Opf. Michael Nüsken, b-it, Universität Bonn Frederik Armknecht, Universität Mannheim