Universität Konstanz

Computer and Information Science

Fachbereichs-kolloqium

Summer semester 2024

Cryptography: Formalizing, Proving, and Breaking Security

Speaker and Title

Dr. Patrick Struck (University of Konstanz)
https://www.ccs.uni-konstanz.de/

Time and Room

June 25th (Wednesday)
1:30pm - 3:00pm
ZT 1204 (Data Theatre)

Universität Konstanz

Abstract

Cryptography is an indispensable tool to achieve security and is ubiquitously deployed nowadays. In the first part of the talk, we cover core cryptographic concepts like encryption and authentication of messages. We further discuss how to formalize basic security properties of cryptographic algorithms, e.g., answering the question "what does it mean for an encryption scheme to be secure?" and how to prove and break these properties. The second part of the talk is based on current research, and covers more advanced security properties. These are important when using cryptographic algorithms in larger protocols to protect against more sophisticated attacks.

Speaker's Bio

Patrick Struck joined University of Konstanz in September 2023 as research group leader for the Cryptography and Cyber Security group. Before joining University of Konstanz, he was PostDoc at University of Regensburg and did his PhD at Technical University of Darmstadt. He was also a visiting researcher at University of Maryland in the USA as well as the Centrum Wiskunde & Informatica in the Netherlands. His research interest is provable security of cryptographic algorithms, in particular, in strong attack models, e.g., when considering attackers that have access to quantum computers.