UNIVERSITÄT MANNHEIM

Group for Theoretical Computer Science und IT-Security

Prof. Dr. Matthias Krause *(Theoretical Computer Science)*	Prof. Dr. Frederik Armknecht *(Cryptography)*
Secretariat	
Karin Teynor	
Researchers	
Matthias Hamann	Angela Jäschke
Alexander Moch	Vasily Mikhalev
	Christian Müller
	Christian Reuter
	Zhi Guan (Guest)
Affiliated PhD Students	
	Yulia Belyaeva
	Benny Fuhry (SAP)
	Avi Mandal (Hochschule Offenburg)
	Tobias Müller (Huawei Technologies)
	Louis Tajan (Hochschule Offenburg)

Our Research

Theoretical Computer Science	IT-Security
Cryptography	
Complexity Theory	Cloud Security
Algorithmics	Embedded Systems
	Mobile Security

Topics (selection):

- Lightweight Cryptography, Hardware Implementation and Verification
- Proofs of Security, Security Models
- Availability of Outsourced Data, Privacy-preserving Data Processing
- Sensor Networks, Privacy Threats in Smart Homes
- Sensor-based Attacks and Security Mechanisms for Mobile Devices

Teaching

Theoretical Computer Science	IT-Security
Lectures	
Algorithmics	Cryptography I & **Cryptography II**
Theoretische Informatik	Selected Topics in IT-Security
Formale Grundlagen der Informatik	**Secure Programming (this term only!)**
Algorithmen und Datenstrukturen	**Data Security (in preparation)**
	Advanced Topics in IT-Security (in preparation)
Seminars	
	Practical IT-Security (Bachelor & **Master**)
Team Projects	
	Attacks on Smart Phones (past)
	A modern cryptanalysis framework using CrypTool 2 (ongoing)

Master Thesis

- **Various topics possible**
- **Can range from theoretical to practical topics**
- **Collaboration with companies possible and welcome**
  - BASF, SAP, NEC, Huawei, ERNW, …
- **Also open for suggestions – simply contact us**