As distributed systems are becoming more ubiquitous, privacy is and will be an important concern. Applying state estimation techniques like a Kalman filter while ensuring that sensor data remain private is a challenging task. In this thesis, you will investigate techniques that enable us to implement an in-network processing of private sensor data. Two directions can be pursued: First, specific cryptosystems can be employed to implement encrypted signal processing algorithms and to define secure protocols. Second, information-theoretic models enable us to achieve differential privacy, which is useful to protect the individual sensor outputs in a networked multi-sensor system.

The focus area of this thesis is in line with our joint research project "SeReMo: Secure Remote Monitoring" in cooperation with our industrial partner.

Within the scope of this work, the following research questions can be addressed:

- Derivation of specific state estimation algorithms using homomorphic encryption schemes
- Processing of multi-sensor data by means of differential privacy to protect sensor outputs
- Fundamental research on privacy-preserving techniques tailored to state estimation

Requirements:
Students with a background in computer science, mathematics, electrical engineering, or other engineering majors. Pre-knowledge in state estimation, sensor data fusion, as well as cryptography is welcome. Strong self-motivation, reliability, and critical mind are expected.

Emphasis:

Theoretical Study
Software Implementation
Hardware Implementation

We offer:
- excellent support and advice
- highend infrastructure
- contact to industry and research partners

Contact:
Dr.-Ing. Benjamin Noack
E-Mail: noack@kit.edu