Karlsruhe Institute of Technology

KASTEL

Institute for Automation and Applied Informatics (IAI)
Karlsruhe Institute of Technology (KIT)
Campus North, Hermann-von-Helmholtz-Platz 1
76344 Eggenstein Leopoldshafen

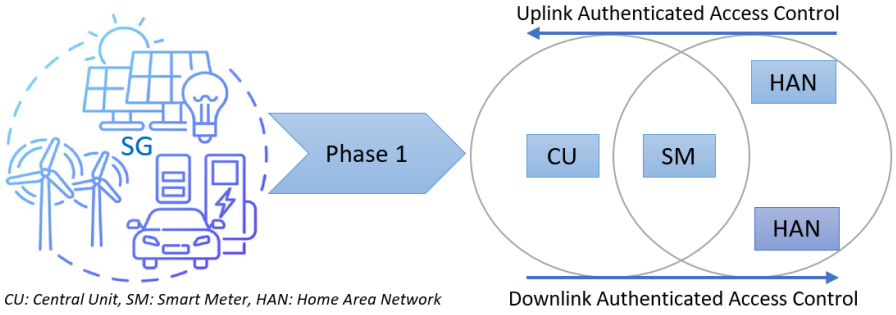
Master / Bachelor Thesis
Authenticated Access Control Cryptosystem for Smart Grids

Starting: ASAP

❖ Description:

Secure Energy Systems (SES) is a working group within Institute for Automation and Applied Informatics (IAI). SES covers a broad area in energy systems and smart grids (SG) including cybersecurity, information security, cryptography, machine learning, communication structure, etc.

The research topic "Zero-trust Malleable Cryptosystem for Smart Grids (ZMC-SG)" aims to develop secure, efficient, and flexible crypto-algorithms that are compatible with SG. Phase 1 in this research topic is to provide an authenticated access control cryptosystems for SG and advanced metering infrastructure (AMI), and it is a combination of authentication, authorization, and data integrity cryptographic algorithm under the zero-trust concept (zero trust for grid entities, connections, and data) using some advanced digital signature schemes (DSS) and also to design a provably secure lightweight public-key cryptographic scheme (PKC) for AMI utilizing the idea of verifiable random functions (VRF) and verifiable delay functions (VDF).



CU: Central Unit, SM: Smart Meter, HAN: Home Area Network

➢ Main Tasks:

- Literature review on PKC, advanced DSS, attribute-based access control (ABAC), VRF, and VDF.
- Design of PKC crypto-algorithms, e.g., ABAC for authorization and access control.
- Design of a lightweight PKC identity-based/certificateless authentication scheme.
- Provide security models, definitions, and formal/informal security analysis.
- Implementation of the authenticated access control phase.
- Performance and complexity evaluation of the cryptosystems using network simulators.
- Reliability and compatibility evaluation using KASTEL Security Lab Energy.

» *The above tasks are flexible and will be adapted to whether is a bachelor's or master's thesis.*

➢ Requirements:

- Majoring in Computer Science, Informatics, or any related major.
- Good knowledge of MATLAB and/or OPNET.
- Familiar or motivated to work within cryptography (PKC).
- Hands-on experience, presentation, and academic writing skills.

➢ **If interested, please send your C.V. and most recent transcript to the contact person. Also, we are glad to answer any questions or queries you might have.**

Dr. Mohammed Ramadan, Ph.D.
Email: mohammed.ramadan@kit.edu
Phone: +49 721 608-25737