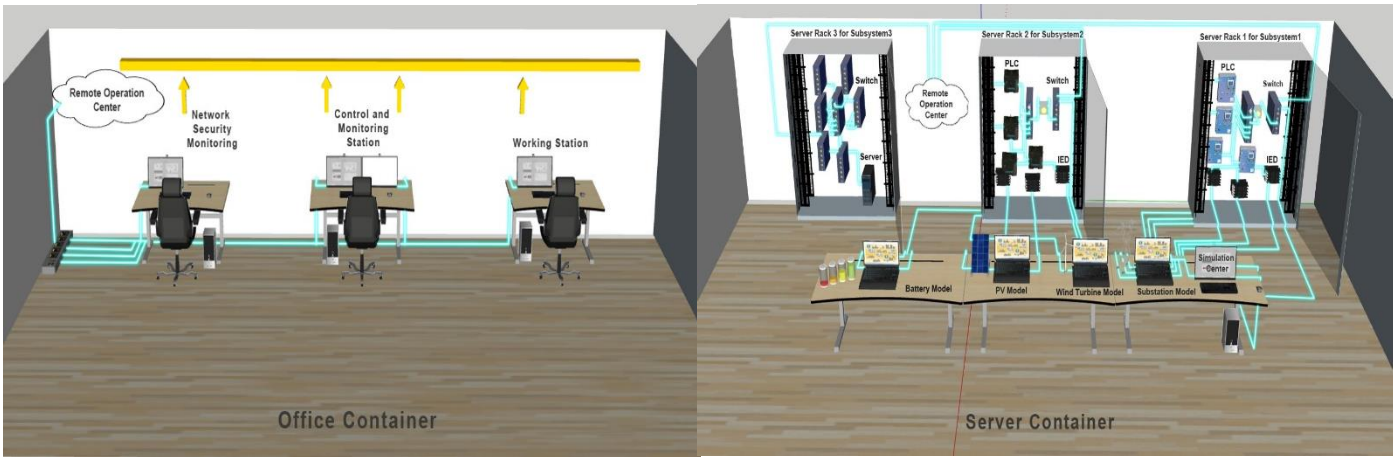
Institute for Automation und Applied Informatics (IAI),
Karlsruhe Institute of Technology, Campus North
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein Leopoldshafen

# Design and Implementation of Crypto-algorithms for Energy Systems

## ➢ 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.
Our goal is to design and implement flexible Public-key Cryptography (PKC) algorithms for Distributed Energy Systems (DES) and Advanced Metering Infrastructure (AMI) within Smart Grids (SG). These energy systems involve power-constrained infrastructure and entities (e.g., sensors - WSN) that required lightweight cryptosystems. Thus, our targeted topic for this position is applied cryptography, design, and implementation of provable secure lightweight public-key cryptosystems.



## ➢ Main Tasks:

- Implementation of crypto-algorithms, e.g., Public-key Cryptography (PKC), Pairing-based Cryptography, Identity-based Cryptography (IBC), Certificateless (CL-PKC), and Attribute-based Cryptography (AB-PKC) for access control.
- Performance and complexity evaluation of cryptosystems using network simulators.
- Reliability and compatibility evaluation using KASTEL Security Lab Energy.
- Some writing tasks for the research findings.

## ➢ Requirements:

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

## ➢ There is an opportunity to pursue your bachelor/master thesis within the project.

## ➢ If you are interested, please send your C.V. and your most recent transcript to the contact person.

Dr. Mohammed Ramadan
E-mail: mohammed.ramadan∂kit.edu
Phone: +49 721 608-25737