Dissertation Topic: Feasibility Analysis of Zero Knowledge Proof Authentication in Internet Of Vehicles

By Hanna Foerster

Project description: Traditional anonymous authentication methods are currently not suitable for the Internet Of Vehicles (IoV) due to their computation or communication costs and problems with maintaining anonymity. So, in my dissertation I explore the practicality of a new anonymous mutual authentication protocol called "A ZKP-based Anonymous Mutual Authentication Scheme (ZAMA)", which is designed for the IoV using Zero-Knowledge Proof (ZKP) and Elliptic Curve Cryptography (ECC). ZAMA mitigates the problem of identity leakage and ensures robust user anonymity via the utilization of ZKP.

Analysis methodology: Analyse the ZAMA protocol from a security and efficiency perspective. Explain the proofs of the security guarantees (anonymity, revocability, unlinkability, traceability, forward secrecy and replay attack resistance) that are found in the original paper to clarify how ZAMA achieves these security properties and to be able to assess its suitability for IoV authentication in terms of security and privacy. Test the efficiency by a simulation and an additional computational and communication overhead analysis. Compare the results obtained in the ZAMA paper with my efficiency analysis and evaluate ZAMA in the context of related works on the overall efficiency and security guarantees.

Project outcomes: While the efficiency of the simulation that is presented in the original paper cannot be achieved in our simulation, the computational and communication overhead analysis reveals that ZAMA is superior to many of its peer authentication protocols. Additionally, the security goals of mutual authentication, user anonymity, replay attack resistance, forward security, unlinkability, and traceability are met, which highlights its advantage in the aspects of security compared to many related works.

Project objectives: The aim through this is to show that ZKP authentication methods are efficient with a strong anonymity and security guarantee and therefore a more viable solution for authentication in IoV compared to other methods. The effectiveness of ZAMA highlights the potential for the application of ZKPs in other authentication systems including systems with any type of moving smart device such as drones or wearable technology devices.