# Privacy-Preserving Vehicle Renting in VANETs

Mahdi Akil
Karlstad University
mahdi.akil@kau.se

## 1 Abstract

The rapid increase in urbanization has led to several transportation challenges, such as traffic congestion, accidents, and pollution caused by vehicles.These issues not only degrade urban living standards but also create economical and environmental costs. To address these issues, Vehicular Ad-Hoc Networks (VANETs) have emerged as a pivotal technological innovation to redefine vehicular traffic management through enhanced safety and efficiency.

VANETs are critical for future Intelligent Transportation Systems, enhancing communications between vehicles and infrastructure. Even though there are significant advancements in ensuring anonymous and secure communication within VANETs, the integration of privacy-preserving vehicle rentals remains a challenge. In this presentation, we will introduce a novel rental protocol within VANETs, employing delegatable anonymous credentials and Non-Interactive Zero-Knowledge (NIZK) proofs. Our approach allows drivers to securely delegate credentials to vehicles, ensuring that each vehicle broadcasts authenticated messages verified through NIZK proofs while maintaining the driver's privacy. An inspector can reveal the identity of the actual driver in cases of abuse, adding accountability to the system. This protocol addresses trust issues in previous systems by providing a robust mechanism for privacy-preserving, accountable vehicle rentals in VANETs.

Our protocol allows drivers to securely delegate their credentials to vehicles, ensuring that the messages broadcasted are verified through NIZK proofs. This mechanism not only preserves the anonymity of drivers but also achieves direct accountability into the system. An inspector within the network has the capability to decrypt the identity of the driver, if necessary, to address potential abuses.

The proposed approach addresses the inherent trust issues in previous systems and provides a comprehensive solution that enhances both the privacy and the accountability in the system. This dual enhancement is crucial for the acceptance and effectiveness of VANETs in real-world applications, where both security and privacy are required. The implementation of our protocol aims to redefine the standards of privacy and security in vehicular communications, promoting a safer and more efficient transportation environment. This work not only advances the field of vehicular networks but also sets a precedent for future research in secure and privacy-preserving communication protocols in Intelligent Transportation Systems.