Zero-Knowledge Proofs and Assurance for Autonomous System Communications

Edward Griffor, Ph.D.

Bio

Dr. Edward Griffor is the Associate Director for Cyber-Physical Systems and Internet of Things in NIST's Smart Connected Systems Division. He brings a decade of experience as chief scientist in the automotive sector, where he led autonomous vehicle technology development. He is currently an adjunct professor at Wayne State University and the University of Grenoble Alpes. Dr. Griffor holds a Ph.D. in mathematics from MIT and a European habilitation in electrical engineering from the University of Oslo, and is a recipient of the NATO–NSF Postdoctoral Fellowship in Engineering and Science. He has authored multiple handbooks, including works on system safety and security, computability theory, and mathematical domain theory published by Elsevier and Cambridge University Press. His research integrates physics, computing, mathematics, and biosciences to advance the security and assurance of cyber-physical and IoT systems, spanning automated driving, reactor protection, and biomedical applications.

Abstract

The application of zero-knowledge proofs (ZKPs) in autonomous systems is an emerging area of research, motivated by the growing need for regulatory compliance, transparent auditing, and trustworthy operation in decentralized environments. zk-SNARK is a powerful cryptographic tool that allows a party (the prover) to prove to another party (the verifier) that a statement about its own internal state is true, without revealing sensitive or proprietary data about that state. This paper proposes Hermes' Seal: a zk-SNARK-based ZKP framework for enabling privacy-preserving, verifiable communication in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) networks. The framework allows autonomous systems to generate cryptographic proofs of perception and decision-related computations without revealing proprietary models, sensor data, or internal system states, thereby supporting interoperability across heterogeneous autonomous systems. We present two real-world case studies implemented and empirically evaluated within our framework, demonstrating a step toward verifiable autonomous system information exchanges. The first demonstrates real-time proof generation and verification, achieving 8ms proof generation and 1ms verification on a GPU, while the second evaluates the performance of an autonomous vehicle perception stack, enabling proof of computation without exposing proprietary or confidential data. Furthermore, the framework can be integrated into autonomous system perception stacks to facilitate verifiable interoperability and privacy-preserving cooperative perception. The demonstration code for this project is open source, available on GitHub.