A Hybrid Zero-Knowledge Proof Framework: Integrating zk-SNARK, zk-STARK and zk-Rollup

Amara Jaya Sri Varshini
Department of CSE SRM University-AP, Amaravati, Andhra Pradesh, India

Meghana Nangireddy
Department of CSE SRM University-AP, Amaravati, Andhra Pradesh, India

Chekuri Harshitha
Department of CSE SRM University-AP, Amaravati, Andhra Pradesh, India

Chandana Gorantla
Department of CSE SRM University-AP, Amaravati, Andhra Pradesh, India

KC Deepthi Kakumani
Department of CSE SRM University-AP, Amaravati, Andhra Pradesh, India

Abstract

The increasing dependence on digital financial and identity verification systems has amplified concerns surrounding user privacy and data exposure. Traditional verification mechanisms require complete disclosure of sensitive attributes such as credit score, salary, account balance, age, and nationality, creating significant risks related to misuse, profiling, and unauthorized access. Zero-Knowledge Proofs (ZKPs) provide a transformative approach by enabling users to prove compliance with eligibility conditions without revealing their underlying data. In this research, we present a hybrid ZKP framework that integrates three complementary zero-knowledge paradigms—zk-SNARK, zk-STARK, and zk-Rollup—to achieve a balanced combination of privacy, transparency, and scalability. The proposed system uses constraint-based logic to validate financial and demographic attributes through private inputs, producing verifiable proofs using SNARK, transparent post-quantum-secure proofs using STARK, and highly scalable proof aggregation through Rollups. A programmable verification engine simulates trusted-setup workflows, FRI-based STARK execution, Merkle-tree batching, fraud detection, and blockchain-style on-chain confirmation. Experimental execution demonstrates that invalid proofs are correctly rejected based on predefined eligibility thresholds, while valid proofs are efficiently generated and verified. Performance evaluation shows that SNARK proofs remain compact (~25 KB) with sub-millisecond on-chain verification, STARK proofs offer full transparency without setup requirements, and Rollups reduce verification gas by approximately 97% when aggregating batches of ten users. The hybrid design highlights strong applicability in privacy-preserving fintech verification, identity validation, compliance auditing, and decentralized Web3 services.

Keywords

Zero-Knowledge Proofs, zk-SNARK, zk- STARK, zk-Rollup, Privacy-Preserving Verification, Blockchain.