

## **System for a user authentication according to a zero-knowledge proof protocol**

### **Abstract**

This paper presents the design and implementation of a user authentication system based on the Zero-Knowledge Proof (ZKP) protocol.

The study addresses the limitations of traditional authentication methods such as password-based, digital signature, and two-factor authentication systems which often compromise user privacy by requiring the transmission or storage of sensitive data. The proposed solution demonstrates how ZKP technology can enable secure and private user verification without revealing personal information. The system was developed using a modular architecture that integrates cryptographic components for proof generation and verification, ensuring anonymity and resistance to common cyberattacks. Functional testing confirmed that the ZKP-based approach maintains strong authentication accuracy while effectively protecting against data leakage and impersonation threats. The results of the comparative analysis highlight the superiority of ZKP-based authentication in terms of privacy, anonymity, and security, making it a promising direction for modern applications such as secure electronic voting and digital identity systems. The proposed implementation serves as a practical example of how advanced cryptographic mechanisms can enhance trust and confidentiality in digital interactions.