УДК 004.72

Жержерунов П. Ю., аспірант,
Національний технічний університет "Харківський політехнічни інститут"
Шматко О. В., к.т.н., доцент,
ТОВ ТУ Метінвест ПОЛІТЕХНІКА

EFFICIENT ZERO-KNOWLEDGE PROOF CIRCUITS FOR THE SM3 HASH FUNCTION IN RESOURCE-CONSTRAINED BLOCKCHAIN SYSTEMS

Modern information systems increasingly rely on distributed infrastructures that enable cooperation between multiple independent organizations. Such environments require mechanisms that guarantee both data integrity and confidentiality. Blockchain technology has emerged as a promising solution for maintaining distributed ledgers and ensuring transparent and tamper-resistant recording of transactions across decentralized networks. However, conventional blockchain architectures are primarily designed to maximize transparency, which may conflict with the confidentiality requirements of corporate information systems.

Zero-Knowledge Proof (ZKP) protocols provide an effective method for privacy-preserving verification of computations. These protocols allow a prover to demonstrate knowledge of a secret value without revealing the value itself. When integrated into blockchain systems, ZKP mechanisms enable validation of transactions while keeping the underlying information confidential. Despite these advantages, practical implementation of ZKP mechanisms often introduces considerable computational overhead, particularly when complex cryptographic primitives such as hash functions are involved.

To address these challenges, this work proposes a privacy-preserving blockchain architecture that combines the Proof of Friendship (PoF) consensus mechanism with optimized Zero-Knowledge Proof circuits based on the SM3 hash function. The proposed approach aims to enable efficient verification of transaction correctness while minimizing computational overhead in distributed enterprise environments.

Experimental evaluation was conducted in a containerized environment that simulates a distributed corporate blockchain network with limited computational resources available to each node. In this architecture, proof generation is performed by an off-chain prover module, while validator nodes verify proofs and participate in the consensus process.

Two circuit construction approaches were analyzed. The first approach corresponds to a direct translation of the SM3 hashing algorithm into a Rank-1 Constraint System without specialized optimization techniques. The second approach implements the optimized SM3-ZKP circuit proposed in this work.

The optimization techniques include bit–arithmetic aggregation, optimized message scheduling, reduction of circuit depth, and the use of lookup tables for nonlinear functions.

The experimental results demonstrate that the optimized SM3-ZKP circuit significantly reduces circuit complexity compared to the naive implementation. The number of arithmetic constraints and intermediate variables required for representing the hash computation decreased by approximately fifty percent. As a result, proof generation time was reduced by more than two times while maintaining constant verification time.

This work presents a privacy-preserving blockchain architecture designed for corporate information systems. By integrating the Proof of Friendship consensus mechanism with optimized SM3-based Zero-Knowledge Proof circuits, the proposed solution enables verification of transaction correctness while maintaining confidentiality of sensitive data. Experimental results demonstrate that the proposed optimization techniques significantly reduce proving complexity and enable practical deployment of ZKP mechanisms in resource-constrained enterprise blockchain environments. The proposed architecture provides a foundation for developing secure distributed information systems that combine blockchain transparency with strong data protection guarantees.

References

1. Chirakarotu N. R., Kumar P. P. Promise of Zero-Knowledge Proofs (ZKPs) for Blockchain Privacy and Security: Opportunities, Challenges, and Future Directions //Security and Privacy. – 2024.

2. Sah C. P., Kaur M., Singh G. Efficiency of zero-knowledge proofs: a through review and analysis //2024 IEEE International conference on public key infrastructure and its applications (PKIA). – IEEE, 2024. – С. 1-7.

3. Yang Y. et al. Implementation and optimization of zero-knowledge proof circuit based on hash function sm3 //Sensors. – 2022. – Т. 22. – №. 16. – С. 5951.

4. Dong J. K. et al. HI-SM3: High-Performance Implementation of SM3 Hash Function on Heterogeneous GPUs //Journal of Computer Science and Technology. – 2025. – Т. 40. – №. 6. – С. 1546-1562.

5. Shmatko O.V. et al. Survey and categorization of blockchain solutions for supply chain management //Системи обробки інформації. – 2024. – №. 3 (178). – С. 84-92.