Zero-Knowledge Proof (ZKP) technology marks a revolutionary advancement in the field of cryptography, enabling the verification of certain information ownership without revealing any specific details. This technology, with its paradoxical yet powerful characteristics, provides a solid foundation for a wide range of applications, especially in enhancing the privacy and security of blockchain technology and other cryptographic systems. As ZKP technology increasingly becomes a part of the blockchain infrastructure, its importance for security and integrity becomes more pronounced. However, the complexity of ZKP implementation and the rapid iteration of the technology introduce various vulnerabilities, challenging the privacy and security it aims to offer.

This study bases on the integrity, soundness, and zero-knowledge properties of ZKP to meticulously classify existing vulnerabilities and deeply explores multiple categories of vulnerabilities, including integrity issues, soundness problems, information leakage, and non-standardized cryptographic implementations. Furthermore, we propose a set of defense strategies that include a rigorous security audit process and a robust distributed network security ecosystem. This audit strategy employs a divide-and-conquer approach, segmenting the project into different levels, from the application layer to the platform-nature infrastructure layer, using threat modeling, linear code checking, and internal cross-review, among other means, aimed at comprehensively identifying vulnerabilities in ZKP circuits, revealing design flaws in ZKP applications, and accurately identifying inaccuracies in the integration process of ZKP primitives.

Read More

https://eprint.iacr.org/2024/514