Optimized ZK verification of ECDSA signature with partially outsourced computations

Distributed Lab

Distributed Lab

1 Introduction

The Elliptic Curve Digital Signature Algorithm (ECDSA) is one of the most widely adopted signature schemes, particularly in blockchain systems. However, when it comes to zero-knowledge proof systems, verifying ECDSA signatures presents significant computational challenges.

Current implementations of ECDSA signature verification in zero-knowledge circuits face several limitations. The primary challenge lies in the computational complexity of the verification process, which requires numerous elliptic curve operations and modular arithmetic calculations. These operations translate into a large number of constraints when expressed in arithmetic circuits, making the proof generation process computationally intensive and time-consuming.

We propose to ousource part of computations to a verification party, while still preserving user's privacy.

2 Optimization

Let PK be a public key, (r, s) - signature, m - message, G - base point (generator of EC group), R - point, where $R.x == r$. Then to verify an ECDSA signature, the following equation must hold:

$$m \cdot s^{-1} \cdot G + r \cdot s^{-1} \cdot PK = R \tag{1}$$

Let $\mathcal{B}$ be random value selected uniformly from range $[0, 2^c)$, where c is security parameter; $\mathbb{B} = [\mathcal{B}]G$