I was thinking about opening an EIP about a precompiled contract that verifies ZKProofs. The contract takes two parameters: p

, the proof, v_k

the verification key and x

, the public input. the contract then proves p

and x

using v_k

. This is already done in Zokrates's Verifier contract. However, given the steady increase in gas price and the consequent increase in the popularity of ZkProofs in verifying transactions with the minimum amount of gas, I think it would be beneficial for simplifying the process of verification (solidity-development-side) and make it more efficient so that we could save some gas in the process of verification.

The code of the precompiled will be pretty much the same as the one in the Zokrates Verifier contract so it's not something that is to be started from scratch.

Any thoughts?