# zkMIPS: An Advanced Zero-Knowledge Proof Solution for MIPS Architecture

zkMIPS Team

Version 1.1
June 15, 2023

### Abstract

This document introduces zkMIPS, an advanced Zero-Knowledge Protocol (ZKP) system designed for MIPS architecture. zkMIPS aims to provide a verifiable computing solution to trust the computation results generated by untrusted computers. The adoption of the MIPS architecture aligns perfectly with the vision of incorporating zkMIPS into diverse domains such as blockchains and IoT. In the blockchain realm, zkMIPS is seamlessly integrated with Optimism technology, offering a ZKP layer 2 rollup solution specifically tailored for Ethereum. By harnessing the power of ZKP and leveraging the robustness of the MIPS architecture, zkMIPS aims to fulfill its objectives effectively. In particular, Optimism has already established a MIPS platform, providing a strong foundation for the integration of zkMIPS and accelerating the development of Ethereum Layer 2 ZK rollup solutions. In non-blockchain systems including the Internet of Things (IoT), Virtual Reality (VR), wearable devices, and decentralized cloud computing, zkMIPS enables a secure communication channel by trusting devices' computation results. This document serves as a comprehensive introduction, shedding light on the integration of zkMIPS with Optimism's architecture, while offering an overview of the zkMIPS zero-knowledge approach.

# Contents

# 1 Introduction

In recent years, the advancement of verifiable computing techniques, particularly in zero-knowledge proofs (ZKPs), has enabled developers to ensure the trustworthiness of computation results from untrusted parties. Among these achievements, zkMIPS has successfully developed a mechanism to demonstrate the integrity of any MIPS computation. Although initially focused on layer 2 zero-knowledge (ZK) rollup solutions, zkMIPS holds broad applicability, including Internet-of-Things (IoT), wearables, and more. zkMIPS facilitates quick and easy proof of the validity of the computation results performed by untrusted parties, offering a robust solution to ensure computational trust in a wide range of practical applications.

In an interactive proof system, one of the parties, called the Prover, wants to convince the other party, also known as the Verifier, that it possesses specific information [12, 13]. This can involve proving knowledge of a password, a specific solution to a problem, or the ability to execute a particular computation. Although existing methods in the area of ZKP are very promising, applying these techniques to develop a high-performance system requires further innovation and careful consideration, such as computation and storage overhead, to apply a ZKP system. zkMIPS aims to create a cryptographic proof that validates the execution of computations, with several concerns such as proof size, prover time, and verifier time. The size of the generated proof should be succinct to meet application requirements, minimizing storage and transmission overhead. Generating the proof by the Prover and verifying it by the Verifier introduce additional computational overhead, so the time it takes to generate or verify it should align with the application requirements. Balancing these factors requires ongoing innovation to ensure that zkMIPS can be applied effectively while addressing the challenges of proof size, prover time, and verifier time. More importantly, it should be easily integrated with existing applications with minimum effort.

zkMIPS is designed for the stable and well-established MIPS architecture to apply ZKP techniques resulting in offering numerous advantages. The adoption of MIPS architecture brings benefits, such as small instruction set and the simplified design of efficient ZKP circuits. Additionally, due to the stability of the MIPS architecture, integrating zkMIPS does not require significant alterations to its core design, making it compatible with systems that compile computations to MIPS. In the realm of blockchain, Optimism, a key player in Layer 2 Ethereum solutions, recognizes the importance of MIPS. The collaboration between Optimism and zkMIPS to accelerate the development of zkMIPS as a ZKP rollup solution for Ethereum, enhancing scalability and privacy. Furthermore, zkMIPS demonstrates to be a natural choice for IoT applications, as the popularity of MIPS in IoT devices allows for the seamless incorporation of verifiable computing capabilities. In general, zkMIPS takes advantage of the strengths of the MIPS architecture, enabling the widespread implementation of ZKP techniques in domains ranging from blockchain solutions like Optimism to IoT, Virtual Reality (VR), wearable devices, and more applications.

This document serves as an introduction to zkMIPS technology, covering various aspects of its implementation. Section 2 provides a comprehensive review of the applied MIPS architecture within zkMIPS. Section 3 delves into the software system architecture necessary for seamless integration, while also highlighting the integration of Optimism technology for Layer 2 (L2) rollup purposes. The document proceeds to explore ZK protocols in Section 4, explaining how they provide succinct proof through the conversion of computations into high-degree polynomials over a finite field, enabling efficient verifica-