zkInterval: Trustless, Confidential, Constant-Size Range Proofs

Quinn Parkinson

Logical Mechanism LLC, USA

Abstract. In this paper, we introduce zkInterval, a novel constant-size range proof protocol that proves a secret value lies within a public interval without revealing the value or requiring a trusted setup. Leveraging Pedersen commitments, Weil pairings, and Schnorr Σ-protocols, zkInterval offers a practical, trustless, and confidential solution with proofs whose size remains invariant regardless of the interval's range. These properties significantly reduce complexity, storage, and communication overhead, making zkInterval particularly well-suited for privacy-focused applications and scenarios with variable interval lengths. Our protocol enhances the efficiency and scalability of cryptographic range proofs, offering a robust solution to a critical challenge in modern cryptography.

1 Introduction

Proving that a value lies within a specific interval while preserving its confidentiality practically and efficiently poses a significant challenge in modern cryptographic range proofs. Many existing methods generate proofs whose size scales with the interval's range, which can severely limit their efficiency, especially in applications that demand a constant proof size across variable interval lengths or must avoid trusted setups, which can introduce vulnerabilities such as collusion-based attacks. This paper introduces zkInterval, a protocol that overcomes these limitations by producing a practical, trustless, and constant-size range proof independent of the interval's range. By integrating Weil pairings [men, pp.62–63], Pedersen commitments [Ped91], and Schnorr Σ-protocols [Tha22, pp.310–311], zkInterval securely demonstrates that a secret value lies within a publicly known interval while keeping the value itself hidden. Our efficient and concise approach makes zkInterval particularly well-suited for privacy-focused applications with variable interval lengths. Since privacy-preserving range proofs play an essential role in private information verification, secure multi-party computation, and confidential transactions, zkInterval addresses a significant need in modern cryptographic systems.

Although some schemes offer constant-size proofs, they often rely on trusted setups or result in verbose proofs [CBC+24]. More recent advancements like Bulletproofs [BBB+18] have reduced proof sizes to sublinear scales, all while being trustless; however, their proof size still depends on the interval's range, which can be a limiting factor in applications with variable interval lengths. zkInterval addresses these challenges by delivering constant-size, scalable range proofs that maintain confidentiality without compromising efficiency. This work fills a critical gap in current cryptographic methods and paves the way for further advancements in range-proof technologies.

The remainder of this paper is as follows. Section 2 presents the derivation of the zkInterval protocol, detailing its mathematical foundation and the integration of Weil pairings, Pedersen commitments, and Schnorr Σ-protocols. Section 3 rigorously examines

E-mail: quinn@logicalmechanism.io (Quinn Parkinson)

Date of this document: 2025-05-08.

the protocol's security properties, establishing its zero-knowledge guarantees and demonstrating that it forms a complete proof system. Finally, Section 4 discusses the practical implementation of zkInterval on the Cardano blockchain, highlighting its performance benefits and suitability for privacy-focused and scalable cryptographic applications.

2 Bibliography

Citing papers is done in the usual way using BibTeX or `biblatex` commands. For example: the RSA paper [**?**].

It is highly encouraged to use CryptoBib from https://cryptobib.di.ens.fr

References

[BBB+18] Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, and Greg Maxwell. Bulletproofs: Short proofs for confidential transactions and more. In *2018 IEEE Symposium on Security and Privacy (SP)*, pages 315–334. IEEE, 2018.

[CBC+24] Miranda Christ, Foteini Baldimtsi, Konstantinos Kryptos Chalkias, Deepak Maram, Arnab Roy, and Joy Wang. SoK: Zero-knowledge range proofs. Cryptology ePrint Archive, Paper 2024/430, 2024. URL: https://eprint.iacr.org/2024/430.

[men]

[Ped91] Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *Annual International Cryptology Conference (CRYPTO)*, pages 129–140. Springer, 1991.

[Tha22] Justin Thaler. *Proofs, Arguments, and Zero-Knowledge*, volume 4 of *Foundations and Trends ® in Privacy and Security*. Now Publishers, 2022.