# 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 [Men93, 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 Derivation

The derivation of zkInterval is systematic and structured into distinct sections, each addressing a specific aspect of the proof before being integrated into the final result. We begin with the primary inequality and reformulate it into a suitable polynomial representation. Once in polynomial form, we proceed with the Pedersen commitment scheme to demonstrate that the inequality holds at the commitment level. Subsequently, we will incorporate the commitment scheme into a Weil pairing for any pairing-friendly curve, and then we will finalize the proof with two Schnorr Σ-protocols. The resulting proof is a collection of $\mathbb{G}_1$ points of the pairing-friendly curve with two integers for the Schnorr Σ-protocols.

We begin the derivation by stating the fundamental inequality that establishes the existence of a value $d$ between $a$ and $b$,

$$a \geq d \geq b, \tag{1}$$

where $a \geq b$ and $a, b, d \in \mathbb{Z}^+$. We will introduce two auxiliary variables that quantify the differences between the extremal values $a$ and $b$ and the intermediate value $d$ to reformulate the inequality into a polynomial. The first variable, $y$, is defined as:

$$a - d = y, \tag{2}$$

and the second variable, $w$, is defined as:

$$d - b = w. \tag{3}$$

By subtracting equation 3 from equation 2 and reorganizing the terms, we obtain the following equation:

$$a + b + w = y + 2d. \tag{4}$$

Next, we introduce an additional term $\gamma$ to both sides, resulting in the final fundamental equation:

$$\gamma + a + b + w = y + 2d + \gamma. \tag{5}$$

While adding the $\gamma$ terms might initially appear redundant, it plays a crucial role when incorporating Pedersen commitments. This inclusion allows us to commit to a value of $\gamma = 0$ while still encapsulating the randomness from the commitment process, thus balancing the randomness by making the blinding factors of the other commitments act like secret keys [Jed16].

To facilitate a more familiar exposition of the commitment proof, we shall express the Pedersen commitment scheme in its multiplicative formulation, denoted as $C(v, r) = g^r h^v$, where $g$ and $h$ are designated generators within the $\mathbb{G}_1$ group of our pairing-friendly elliptic curve. We will use the additive formulation, $C(v, r) = [r]g + [v]h$, to reconstitute equation 5 for the derivation in the following manner:

$$C(y, r_y) + 2C(d, r_d) + C(\gamma, \psi) = C(a, r_a) + C(b, r_b) + C(w, r_w) + C(\gamma, \lambda), \tag{6}$$

wherein $\psi = r_a + r_b + r_w$ and $\lambda = r_y + 2r_d$. By imposing $\gamma = 0$, equation 6 reaches a state of equilibrium in its commitment form, thereby enabling each component of equation 5 to be encapsulated within a commitment while preserving the requisite algebraic integrity.

**Proof 1** (Proof of Pedersen Commitments)**.** The proof of the Pedersen commitment scheme is as follows. Start with Equation 6 in multiplicative form.

$$g^{r_y} h^y g^{2r_d} h^{2d} g^{\psi} = g^{r_a} h^a g^{r_b} h^b g^{r_w} h^w g^{\lambda}. \tag{7}$$

Upon aggregation and simplification, the multiplicative form reduces to:

$$g^{r_y+2r_d+\psi} h^{y+2d} = g^{r_a+r_b+r_w+\lambda} h^{a+b+w}. \tag{8}$$

Recall that $\psi = r_a + r_b + r_w$ and $\lambda = r_y + 2r_d$ which further simplifies the equation to:

$$g^{\lambda+\psi} h^{y+2d} = g^{\psi+\lambda} h^{a+b+w}. \tag{9}$$

The definitions of $\psi$ and $\lambda$ allow the $g$ terms to cancel out.

$$h^{y+2d} = h^{a+b+w} \tag{10}$$

We know from equation 4 that $a + b + w - y - 2d = 0$ thus

$$h^{a+b+w-y-2d} = h^0 = 1 \tag{11}$$

The prover must possess comprehensive knowledge of all blinding factors and their aggregate sums and is responsible for constructing the proof with the necessary mathematical rigor. Their key responsibility is to ensure that the commitment form reaches a state of equilibrium and that each component of equation 5 is encapsulated within a commitment.

Now that we have equation 5 and equation 6, we know by proof 1 that the relationship between the variables will hold. However, if we use equation 6, we need additional proofs to open each commitment. One way to address this problem is using Weil pairings, which enable global verification, verifying that all the relationships among the commitments hold as expected without having to prove each commitment individually.

The last part of the proof derivation relies on the identity, Galois invariant, and bilinear properties of a Weil pairing. Without loss of generality, we will use the following notation for a Weil pairing:

$$e(Q, P) \to e(Q, C), \tag{12}$$

where $Q$ is a fixed $\mathbb{G}_2$ point and $C$ is a Pedersen commitment as a $\mathbb{G}_1$ point on pairing friendly curve. The Galois invariant property is:

$$e(Q, P)^v = e(vQ, P) = e(Q, vP) \to e(Q, C(v, r_v)), \tag{13}$$

where $r_v$ is a random blinding factor for the scalar $v$. The identity property is:

$$e(Q, C(v, r_v))^k = 1, \tag{14}$$

when $k = 0$. The bilinear property is:

$$e(Q, C(v, r_v) + C(u, r_u)) = e(Q, C(v, r_v))e(Q, C(u, r_u)), \tag{15}$$

We start with equation 5 and will work our way into the Weil pairing commitment form similar to equation 6. First, rewrite equation 5 in standard form and substitute the expression for $k$ using the identity property of a Weil pairing. The resulting equation is:

$$e(Q, C)^{y+2d+\gamma-\gamma-a-b-w} = 1. \tag{16}$$

Expand, group terms, and simplify using the invariant and bilinear properties:

$$e(Q, C(y, r_y)+2C(d, r_d)+C(\gamma, \psi))e(-Q, C(a, r_a)+C(b, r_b)+C(w, r_w)+C(\gamma, \lambda)) = 1. \tag{17}$$

By further simplifying and evaluating $\gamma$, we derive the final pairing expression:

$$e(Q, Y + D + \Psi)e(-Q, A + B + W + \Lambda) = 1, \tag{18}$$

equivalently,

$$e(Q, Y + D + \Psi) = e(Q, A + B + W + \Lambda). \tag{19}$$

Here, the variables are defined as follows:

- $\Psi = C(0, \psi)$ and $\Lambda = C(0, \lambda)$, where $\psi = r_a + r_b + r_w$ and $\lambda = r_y + 2r_d$ represent linear combinations of the blinding factors,
- $Y = C(y, r_y)$ denotes the commitment associated with the scalar $y$ and its corresponding blinding factor $r_y$,
- $D = 2C(d, r_d)$ represents a doubled commitment to the scalar $d$, with $r_d$ as its blinding factor,
- $A = C(a, r_a)$ and $B = C(b, r_b)$ are commitments to the scalars $a$ and $b$ respectively, with $r_a$ and $r_b$ as their respective blinding factors,
- $W = C(w, r_w)$ corresponds to the commitment associated with the scalar $w$ and its blinding factor $r_w$.

A compact form of the proof of the Weil pairing is the hexadecimal string:

$$\pi = Y|D|\Psi|A|B|W|\Lambda. \tag{20}$$

To complete the proof, we must show that we have correctly included the interval endpoints $a$ and $b$ because, in the current form, nothing proves that the public endpoints are inside the proof. The commitment for an endpoint in multiplicative form:

$$A = C(a, r_a) = g^{r_a} h^a, \tag{21}$$

Given that $a$ is public and known, we can create a new commitment, $C_{r_a}$. A Schnorr $\Sigma$-protocol can be used to prove knowledge of the randomness $r_a$, thus proving $A$ does indeed use the endpoint $a$. The commitment $C_{r_a}$ expresses itself as:

$$C_{r_a} = A - C(a, 0) = g^{r_a}. \tag{22}$$

where $r_a$ is the blinding factor.

**Proof 2** (Proof of a Schnorr $\Sigma$-protocol)**.** Select a random value $\alpha$, where $\alpha \in \mathbb{Z}^+$. Compute a challenge value

$$c = H(g^\alpha | g^{r_a}), \tag{23}$$

using the Fiat-Shamir heuristic and a public hash function $H$. Then compute

$$z = \alpha + c \cdot r_a \tag{24}$$

and verify

$$g^z = g^\alpha \cdot C_{r_a}^c. \tag{25}$$

Since

$$g^z = g^{\alpha + c \cdot r_a} = g^\alpha \cdot g^{c \cdot r_a} = g^\alpha \cdot (g^{r_a})^c = g^\alpha \cdot C_{r_a}^c, \tag{26}$$

the proof holds.

The prover must provide $z$ in hexadecimal form and $g^{\alpha}$ for the $A$ and $B$ terms. Together with the pairing equation and the two Schnorr $\Sigma$-protocols, this constitutes a complete zero-knowledge proof system for demonstrating that the value $d$ lies between $a$ and $b$. The final proof is the hexadecimal string:

$$\pi = Y|D|\Psi|A|B|W|\Lambda|g^{r_a}|g^{r_b}|Z_a|Z_b. \tag{27}$$

# 3 Bibliography

## 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.

[Jed16] Tom Elvis Jedusor. Mimblewimble. https://scalingbitcoin.org/papers/mimblewimble.txt, 2016. Unpublished whitepaper.

[Men93] Alfred Menezes. *Elliptic Curve Public Key Cryptosystems*. Kluwer Academic Publishers, 1993.

[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.