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 γ to both sides, resulting in the final fundamental equation:

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

While adding the γ 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 ψ and λ 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:

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

By further simplifying and evaluating γ, we derive the final pairing expression:

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

equivalently,

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

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:

$$\pi = Y|D|\Psi|A|B|W|\Lambda. \quad (20)$$

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:

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

Given that a is public and known, we can create a new commitment, C_{r_a}. A Schnorr Σ-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:

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

where r_a is the blinding factor.

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

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

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

$$z = \alpha + c \cdot r_a \quad (24)$$

and verify

$$g^z = g^\alpha \cdot C_{r_a}^c. \quad (25)$$

Since

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

the proof holds.

The prover must provide z in hexadecimal form and g^{α} for the A and B terms. Together with the pairing equation and the two Schnorr Σ-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:

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

3 Analysis

This section contains a completeness, soundness, and zero-knowledge analysis of the zkInterval protocol. It will end with a examination of the efficiency and succinctness of the proofs.

The zkInterval protocol is complete if an honest prover can always generate a valid proof when the secret value d lies between a and b.

Proof 3 (Proof of Completeness)**.** We begin by reformulating the inequality $a \geq d \geq b$ in a polynomial form by defining the auxiliary variables

$$y = a - d \quad \text{and} \quad w = d - b.$$

Then, assuming $a, b, d \geq 0$ and $a \geq b$, it follows that $y, w \geq 0$ and the relation

$$a + b + w = y + 2d$$

holds.

Next, let $C(v, r) = g^r h^v$ denote a Pedersen commitment on a value v with randomness r. We construct commitments so that the underlying arithmetic is preserved homomorphically. In particular, we form the equation

$$C(y, r_y) + 2\,C(d, r_d) + C(0, \psi) = C(a, r_a) + C(b, r_b) + C(w, r_w) + C(0, \lambda),$$

where the randomness is combined as

$$\psi = r_a + r_b + r_w \quad \text{and} \quad \lambda = r_y + 2\,r_d.$$

Suppose the prover computes these commitments honestly (i.e., with $a \geq d \geq b$ so that y and w are nonnegative). In that case, the homomorphic properties of the Pedersen commitments ensure that the commitment equation balances exactly, reflecting the original inequality.

It is important to note that if the inequality does not hold (that is, if $y < 0$ or $w < 0$), then even though negative values can be reduced modulo the field prime, the resulting representation will not correspond to the intended nonnegative values. This misrepresentation will cause the commitment equation to fail, as the finite field arithmetic will not faithfully capture the intended inequality relationship.

We employ the Weil pairing to further validate the arithmetic relation among the committed values. Applying the pairing $e(\cdot, \cdot)$ to both sides yields

$$e\Big(Q,\, C(y, r_y) + C(d, r_d) + C(0, \psi)\Big) = e\Big(Q,\, C(a, r_a) + C(b, r_b) + C(w, r_w) + C(0, \lambda)\Big),$$

where Q is a fixed generator in the $\mathbb{G}_2$ group. The bilinearity, Galois invariance, and identity properties of the Weil pairing ensure that this equation holds if the commitments have been correctly formed according to the intended arithmetic relation.

Additionally, Schnorr Σ-protocols are used to prove that the public endpoints a and b are correctly embedded in the commitments. Since these protocols are complete, an honest execution yields valid proofs for the endpoints.

In summary, the completeness of the overall proof is ensured by:

1. The correct polynomial representation of the inequality $a \geq d \geq b$.
2. The homomorphic properties of Pedersen commitments accurately capture the arithmetic relation.
3. The Weil pairing, whose properties guarantee that the commitment equation holds when formed correctly.
4. The completeness of the Schnorr Σ-protocols that verify the embedding of the endpoints.

Thus, when d lies between a and b and all steps are executed faithfully, every verification check passes, and the verifier accepts the proof.

The zkInterval protocol is sound if a dishonest prover can never produce a valid proof that the secret value d existing outside of a and b actually lies between a and b.

Proof of Soundness. Assume that a dishonest prover produces a proof that convinces the verifier that the secret value d lies in the interval $[b, a]$, while in reality $d \notin [b, a]$. Without loss of generality, suppose that either $d < b$ or $d > a$. Then, at least one of the auxiliary variables

$$y = a - d \quad \text{or} \quad w = d - b$$

must be negative.

In the zkInterval protocol, the prover forms Pedersen commitments to the values y, d, and w (among others). Due to the binding property of Pedersen commitments, once a commitment $C(v, r)$ is published, the prover cannot later claim it opens to a different value x' without breaking the discrete logarithm assumption. Thus, if $y < 0$ or $w < 0$, the corresponding commitment (e.g. $C(y, r_y)$ or $C(w, r_w)$) would need to represent a negative value. Although negative integers can be reduced modulo the field prime, such a reduction does not yield an opening consistent with the intended nonnegative interpretation of y and w in the interval verification.

The protocol enforces the arithmetic relation through the homomorphic property of the commitments:

$$C(y, r_y) + 2\,C(d, r_d) + C(0, \psi) = C(a, r_a) + C(b, r_b) + C(w, r_w) + C(0, \lambda),$$

where the randomness is combined as

$$\psi = r_a + r_b + r_w \quad \text{and} \quad \lambda = r_y + 2\,r_d.$$

This equation holds if and only if the underlying values satisfy the relation

$$a + b + w = y + 2d,$$

which in turn is valid only when $y, w \geq 0$ (i.e., when $a \geq d \geq b$).

Additionally, the verifier uses the Weil pairing:

$$e\Big(Q,\, C(y, r_y) + C(d, r_d) + C(0, \psi)\Big) = e\Big(Q,\, C(a, r_a) + C(b, r_b) + C(w, r_w) + C(0, \lambda)\Big),$$

where Q is a fixed generator in the $\mathbb{G}_2$ group. The bilinearity, Galois invariance, and identity properties of the Weil pairing guarantee that this equation holds if the commitments are formed as prescribed by the correct arithmetic relation.

Finally, the protocol employs Schnorr Σ-protocols to prove that the public endpoints a and b are correctly embedded in the commitments. The soundness of these protocols ensures that no prover can fake valid proofs for the endpoints without knowing their correct discrete logarithms.

In summary, if $d \notin [b, a]$, then either y or w would be negative, and the corresponding commitments would not properly represent the intended values under finite field arithmetic. As a result, the homomorphic and pairing-based checks would fail, and the verifier would detect the inconsistency. Thus, under the binding property of Pedersen commitments and the soundness of the underlying cryptographic assumptions (including the hardness of the discrete logarithm problem and the correctness of the Schnorr Σ-protocols), a dishonest prover cannot produce a valid proof that d lies in $[b, a]$ if it does not, except with negligible probability. □

The zkInterval protocol is zero-knowledge if an honest verifier can only prove the validity of a valid proof without learning the secret value d.

Proof of Zero-Knowledge. We show that an honest verifier learns nothing about the secret value d beyond the fact that it lies in the interval $[b, a]$. This is demonstrated by constructing a simulator that, given only the public values a and b, produces a transcript indistinguishable from one generated by an honest prover.

Simulator Construction:

1. *Simulating Pedersen Commitments:* The simulator chooses random values for the randomness components r_a, r_b, r_y, r_d, r_w and computes the corresponding Pedersen commitments:

$$C(a, r_a), \quad C(b, r_b), \quad C(y, r_y), \quad C(d, r_d), \quad \text{and} \quad C(w, r_w),$$

   where $y = a - d$ and $w = d - b$. Due to the perfect hiding property of Pedersen commitments, these commitments reveal no information about the underlying values. The simulator ensures that the homomorphic relation

$$C(y, r_y) + 2\,C(d, r_d) + C(0, \psi) = C(a, r_a) + C(b, r_b) + C(w, r_w) + C(0, \lambda)$$

   holds by appropriately selecting the combined randomness values $\psi = r_a + r_b + r_w$ and $\lambda = r_y + 2\,r_d$.

2. *Simulating Schnorr Σ-Protocol Transcripts:* The simulator generates transcripts for the Schnorr Σ-protocols that prove the correct embedding of the public endpoints a and b into the commitments. Standard simulation techniques for Schnorr proofs allow the simulator to produce valid-looking responses without knowledge of the discrete logarithms (or the secret d).

3. *Simulating the Pairing Check:* Finally, the simulator produces values that satisfy the Weil pairing equation

$$e\Big(Q,\, C(y, r_y) + C(d, r_d) + C(0, \psi)\Big) = e\Big(Q,\, C(a, r_a) + C(b, r_b) + C(w, r_w) + C(0, \lambda)\Big),$$

   where Q is a fixed generator. Given the bilinear and invariant properties of the pairing, any commitments satisfying the homomorphic relation will also satisfy the pairing equation.

Since the simulated transcript is generated using random values and standard simulation techniques for Schnorr protocols, and because Pedersen commitments are perfectly hiding, the transcript is computationally indistinguishable from one produced by an honest protocol execution. Thus, the verifier gains no knowledge of d other than the fact that the commitments and pairing check validate the arithmetic relation, which implies that $d \in [b, a]$.

Therefore, the zkInterval protocol is zero-knowledge. □

Each proof demostrates that the zkInterval protocol is a zero-knowledge non-interactive proof system.

The zkInterval protocol is fairly succinct. When implemented on the Cardano blockchain, the resulting proof size is 546 bytes for a 64-bit range which is smaller than Bulletproofs in both the 64-bit and 32-bit cases. See Table 4 in [CBC+24]. For the 64-bit case the average prover time is 90ms and verifier time is 2.23ms. The proof generation is slow due to the benchmark being ran with python using the `py_ecc` module for the BLS12-381 curve which is not heavily optmized for performance. The prover time could be decreased significantly with optimal C bindings via rust. The verification is done with the Aiken VM and represents the upperbound on the real computation time required to verify the proof.

In terms of proof size and verification speed when compared to what is consider at the time of this writing to be industry standard, e.g. Bulletproofs, zkInterval is smaller and faster. The zkInterval protocl provides a zero-knowledge range proof that is practical, transparent, and has constant-sized proofs.

4 Discussion

This paper introduced zkInterval, a novel constant-size range-proof protocol that achieves trustlessness and confidentiality without requiring a trusted setup. Our protocol integrates Pedersen commitments, Weil pairings, and Schnorr Σ-protocols to form a robust and efficient proof system. In doing so, zkInterval overcomes several limitations of existing range proofs—most notably the scaling proof sizes seen in schemes such as Bulletproofs **??**—by delivering a proof whose size remains invariant regardless of the interval length.

A key advantage of zkInterval is its elimination of any trusted setup, which minimizes potential vulnerabilities that arise from setup collusion or parameter compromise **??**. This makes it especially attractive for decentralized and blockchain applications where trust minimization is critical. Moreover, by relying on well-established cryptographic assumptions (e.g., the hardness of the discrete logarithm problem) and leveraging the perfect hiding property of Pedersen commitments, the protocol ensures that the secret value remains confidential throughout the proof process.

Our analysis confirms that zkInterval satisfies the standard security properties: completeness, soundness, and zero-knowledge. The completeness proof demonstrates that an honest prover can always generate a valid proof when the secret value d indeed lies within the interval $[b, a]$. The soundness proof ensures that a dishonest prover cannot produce a convincing proof for an invalid claim except with negligible probability. Finally, the zero-knowledge proof shows that an honest verifier learns nothing beyond the claim's validity, ensuring that the secret value is never exposed.

In summary, zkInterval represents a meaningful advancement in the design of range proofs, offering a promising balance between efficiency, security, and practicality. Its constant-size, non-interactive proof system opens new avenues for privacy-preserving technologies in decentralized systems.

5 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.