# zkInterval: Trustless Confidential Fixed-Size Range Proofs

Quinn Parkinson

Logical Mechanism LLC, USA Research & Design

**Abstract.** Ensuring that a value falls within a specific interval while keeping the value confidential is a crucial challenge for privacy-preserving technologies. Existing range proof methods often produce proofs whose sizes increase with the interval length, leading to inefficiencies in applications requiring fixed-size proofs. In this paper, we introduce zkInterval, a novel zero-knowledge range proof protocol that delivers fixed-size proofs regardless of the interval size. Combining Pedersen commitments with zero-knowledge proofs, zkInterval securely confirms that a value is within a public interval without revealing it or requiring a trusted setup. The consistent proof size irrespective of the interval length significantly reduces storage, making zkInterval particularly well-suited for privacy-focused applications with variable interval lengths. The zkInterval protocol enhances the efficiency and scalability of cryptographic range proofs, providing a reliable and efficient solution to contemporary cryptographic demands.

**Keywords:** confidentiality · cryptography · information hiding · trustless · zero-knowledge

## 1 Introduction

Proving that a value falls within a specific interval while keeping the value confidential is a significant challenge in cryptographic proofs. Traditional methods produce proofs whose size scales with the interval length, limiting their efficiency, especially in applications requiring a constant proof size across variable intervals. This paper introduces zkInterval, a protocol that overcomes this limitation by delivering fixed-size range proofs regardless of the interval length. By combining Weil pairings [**?**], Pedersen commitments [**?**], and zero-knowledge Schnorr proofs [**?**], zkInterval securely proves that a value lies within a publicly known interval without revealing the value itself. Our results demonstrate that zkInterval reduces storage demands and is well-suited for privacy-focused applications requiring efficient handling of variable interval lengths.

Efficient privacy-preserving range proofs are essential for private information verification, secure multi-party computation, and confidential transactions. Bulletproofs [**?**] improved range proofs significantly by reducing the range proof size to sublinear, yet the proof still scales with the interval length. zkInterval addresses this issue by generating fixed-size range proofs that maintain confidentiality while ensuring scalability, making it ideal for applications like blockchain systems where efficiency and security are paramount. This paper fills a critical gap in current cryptographic methods and opens new avenues for advancing range-proof technologies.

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


Date of this document: 2024-11-02.

## 2 Method

The derivation of zkInterval is practical and systematic, 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 proofs. The resulting proof is a collection of $\mathbb{G}_1$ points of the pairing-friendly curve with two integers for the Schnorr proofs.

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 [**?**].

To facilitate a more sophisticated 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 to reconstitute equation 5 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 of Pedersen Commitment Scheme.* Equation 5 in additive form is:

$$C(y, r_y) + 2C(d, r_d) + C(0, \psi) = C(a, r_a) + C(b, r_b) + C(w, r_w) + C(0, \lambda). \tag{7}$$

The multiplicative form is:

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

Upon aggregation and simplification, the multiplicative form reduces to:

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

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

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

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

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

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

$$h^{a+b+w-y-2d} = h^0 = 1 \tag{12}$$

□

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 2 that the relationship between the variables will hold. However, if we use equation 6, we need additional proofs for 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:

$$e(Q, P) \to e(Q, C), \tag{13}$$

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:

$$e(Q, P)^v = e(Q, vP) \to e(Q, C(v, r_v)), \tag{14}$$

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

$$e(Q, C(v, r_v))^k = 1, \tag{15}$$

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

$$e(Q, C(v, r_v) + C(u, r_u)) = e(Q, C(v, r_v))e(Q, C(u, r_u)), \tag{16}$$

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:

$$e(Q, C(v, r_v))^{y+2d+\gamma-\gamma-a-b-w} = 1. \tag{17}$$

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

$$e(Q, C(y, r_y)+2C(d, r_d)+C(\gamma, \psi))e(-Q, C(a, r_a)+C(b, r_b)+C(w, r_w)+C(\gamma, \lambda)) = 1. \tag{18}$$

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

$$e(Q, Y + D + \Psi)e(-Q, A + B + W + \Lambda) = 1, \tag{19}$$

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 $r_w$.

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:

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

Given that $a$ is public and known, we can create a new commitment, $C_{r_a}$, 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. The Schnorr proof for this commitment proceeds as follows:

*Proof of Schnorr Proof.* 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 proofs, 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 Results

This section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation as well as the experimental conclusions that can be drawn.

# 4 Discussion

Authors should discuss the results and how they can be interpreted from the perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

# 5 Bibliography