OctoSTARK: A Post-Quantum Verifiable Delay Function via Non-Associative Algebras and STARKs

Aaron M. Schutza

February 20, 2026

Abstract

We propose *OctoSTARK*, a novel post-quantum Verifiable Delay Function (VDF) combining the non-associative hypercomplex algebra of the Octonions with Scalable Transparent ARguments of Knowledge (zk-STARKs). Current state-of-the-art VDFs rely on sequential squaring in commutative groups of unknown order, rendering them vulnerable to quantum adversaries via Shor's algorithm. By operating over the Octonions defined over a STARK-friendly prime field ($\mathbb{O}_p$), OctoSTARK derives its strict sequentiality from *Topological Impedance*—the mathematical inability to apply associative tensor shortcuts to multivariate polynomial recurrences. To prevent the state trajectory from collapsing into associative subalgebras, we dynamically bypass Artin's Theorem by injecting an algebraic hash as a third independent generator at every step. Finally, to bridge the verifiability gap inherent in non-associative structures, we embed the execution trace within a Fast Reed-Solomon Interactive Oracle Proof of Proximity (FRI) based STARK protocol, achieving $\mathcal{O}(\log^2 T)$ asymmetric verification time.

1 Introduction

Verifiable Delay Functions (VDFs) are cryptographic primitives that guarantee a computation requires a prescribed amount of sequential wall-clock time T to evaluate, while remaining exponentially faster to verify, typically requiring time $t = \mathcal{O}(\text{polylog}(T))$ [BBBF18]. They serve as critical components in decentralized randomness beacons, proofs of history, and leader election protocols, ensuring fairness by mitigating front-running and manipulation.

The dominant paradigm for constructing VDFs, instantiated by Wesolowski [Wes19] and Pietrzak [Pie18], relies on repeated squaring in groups of unknown order (such as RSA groups or ideal class groups). While mathematically elegant, these constructions suffer from two fundamental vulnerabilities:

1. **Quantum Vulnerability:** The underlying security assumption reduces to the Hidden Subgroup Problem (HSP) for abelian groups, which is solvable in polynomial time by Shor's algorithm on a quantum computer.

2. **Associative Reliance:** The verification protocols inherently depend on the associativity of the underlying group (i.e., $(g^a)^b = g^{ab}$) to facilitate recursive halving or quotient proofs.

In this paper, we introduce a paradigm shift: deriving sequential delay from the geometric and structural obstructions found in non-associative algebras, specifically the Octonions ($\mathbb{O}$). By pairing an inherently sequential non-associative evaluation over a prime field with modern STARK proof systems [BSBHR18], we achieve the requisite asymmetric verifiability while establishing a rigorously secure, post-quantum VDF.

2 Mathematical Foundations

2.1 The Octonions over Prime Fields ($\mathbb{O}_p$)

The computational domain of OctoSTARK is the Octonion algebra defined over a large, cryptographic prime field $\mathbb{F}_p$, denoted as $\mathbb{O}_p = \mathbb{O} \otimes_{\mathbb{R}} \mathbb{F}_p$. For optimal integration with the zero-knowledge verification circuit, we require a STARK-friendly field such as the Goldilocks prime ($p = 2^{64} - 2^{32} + 1$) or BabyBear ($p = 15 \times 2^{27} + 1$).

An element $X \in \mathbb{O}_p$ is represented as an 8-dimensional vector:

$$X = \sum_{i=0}^{7} x_i e_i, \quad x_i \in \mathbb{F}_p \tag{1}$$

where e_0 is the scalar identity, and $e_1, \ldots, e_7$ are imaginary basis vectors satisfying $e_i^2 = -1$. Multiplication is governed by the Fano plane and is strictly non-commutative and non-associative [Bae02].

2.2 The Associator

The defining feature of $\mathbb{O}_p$ is its failure to obey the associative law: $(AB)C \neq A(BC)$. We define the *Associator* as the multilinear alternating error term measuring this failure:

$$[A, B, C] = (AB)C - A(BC) \tag{2}$$

The non-zero behavior of this associator creates *Topological Impedance*. It acts as an irreducible geometric hazard that prevents an adversary from unrolling a sequence of multiplications into a single, easily computable matrix exponentiation.

2.3 Artin's Theorem

However, alternative algebras (like the Octonions) are subject to **Artin's Theorem**:

Theorem 2.1 (Artin)**.** *In any alternative algebra, the subalgebra generated by any two elements is strictly associative.*

Consequently, for any two elements $X, Y \in \mathbb{O}_p$, the associator $[X, Y, X] = [X, Y, Y] = 0$. This poses a profound threat to any simple iterated delay function (e.g., $Z_{n+1} = Z_n^2 + C$). Because every state Z_n is formed strictly from the genesis seed Z_0 and the constant C, the entire trajectory lies within an associative subalgebra (isomorphic to the Complex or Quaternionic planes). The associator term permanently vanishes, exposing the sequence to parallel algebraic shortcuts.

3 The OctoSTARK Construction

To overcome Artin's trap, the step function must continuously inject a strictly independent third generator into the computation to force the trajectory into the non-associative 8-dimensional bulk.

3.1 Dynamic Injection via Algebraic Hashing

If a static geometric operator (such as a basis rotation or coefficient shift) is used to perturb the sequence, an adversary can select isotropic genesis seeds that align with the rotational symmetry, keeping the trajectory trapped in an associative subspace.

To definitively break Artin's Theorem, we inject a third generator dynamically using a cryptographic pseudo-random oracle. Let $\mathcal{H} : \mathbb{O}_p \to \mathbb{O}_p$ be an algebraic, STARK-friendly hash function, such as Poseidon [GKR+20], acting over the 8 field elements.

3.2 The Recurrence Relation

Given a target delay of T sequential iterations, a verifiable public constant $C \in \mathbb{O}_p$, and a genesis seed $Z_0 \in \mathbb{O}_p$, the OctoSTARK state evolution is defined as:

$$Z_{n+1} = Z_n^2 + C + \left[Z_n, C, \mathcal{H}(Z_n)\right] \pmod{p} \tag{3}$$

By utilizing the non-linear expansion of $\mathcal{H}(Z_n)$, we guarantee with overwhelming cryptographic probability that the three inputs to the associator $\{Z_n, C, \mathcal{H}(Z_n)\}$ are linearly independent. This continuously perturbs the state Z_{n+1} out of any associative plane, ensuring a persistent, non-zero *Associator Hazard* at every step.

Algorithm 1 OctoSTARK Evaluation Phase

Require: Seed state $Z_0 \in \mathbb{O}_p$, Constant $C \in \mathbb{O}_p$, Time parameter T
Ensure: Final state $Z_T \in \mathbb{O}_p$ and STARK Trace Tr

```
Initialize Trace Tr ← [Z_0]
for n = 0 to T − 1 do
    S ← Z_n × Z_n (mod p)
    E_n ← H(Z_n)
    A ← (Z_n × C) × E_n − Z_n × (C × E_n) (mod p)
    Z_{n+1} ← S + C + A (mod p)
    Append Z_{n+1} to Tr
end for
return Z_T, Tr
```

4 Security Analysis

4.1 Cycle Bounds and Field Selection

A critical aspect of the OctoSTARK construction is the strict adherence to a prime field $\mathbb{F}_p$. Polynomial mappings over local rings such as $\mathbb{Z}_{2^{64}}$ built from addition and multiplication suffer from 2-adic nilpotent collapse. Over such power-of-two rings, the Jacobian modulo 2 vanishes, leading to rapid state space collapse and $\mathcal{O}(1)$ cycle-finding attacks via Hensel lifting.

By operating over a large prime field (e.g., $p \approx 2^{64}$), 2-adic nilpotency is mathematically eliminated. The state transition graph acts as a pseudo-random permutation over an 8-dimensional vector space. By the Birthday Paradox, the expected Rho-cycle bound is $\mathcal{O}(\sqrt{p^8}) = p^4$. For a 64-bit prime, this yields a cycle length of $\approx 2^{256}$, offering 128 bits of collision resistance and safely preventing tortoise-and-hare shortcut attacks.

4.2 Resistance to Tensor Unrolling

The standard algebraic attack against custom polynomial iterations is linearization via tensor products. Suppose an attacker attempts to lift the recurrence into a higher-dimensional associative matrix algebra using the left/right multiplication operators L_x, R_x of the octonions.

Because Equation 3 is a Multivariate Quadratic (MQ) relation, unrolling T steps requires lifting the state into the symmetric tensor algebra $\mathrm{Sym}(\mathbb{O}_p) \cong \bigoplus_{d=0}^{2^T} S^d(\mathbb{F}_p^8)$. The dimension of the required linear operator matrices grows double-exponentially as $\mathcal{O}(8^{2^T})$. This "Curse of Dimensionality" renders $\mathcal{O}(\log T)$ repeated matrix squaring algebraically and physically impossible.

4.3 Post-Quantum Hardness

Because $\mathbb{O}_p$ is not a commutative group, the Hidden Subgroup Problem does not apply. The security of the sequential delay reduces to evaluating a system of Multivariate Quadratic (MQ) equations over a non-associative structure. The best known quantum attack is Grover's algorithm applied to collision finding, which provides only a generic polynomial speedup ($\mathcal{O}(\sqrt{N})$), well within the safety margins of standard symmetric parameterization.

5 Asymmetric Verification via STARKs

A VDF must possess a verification protocol vastly faster than the time parameter T. Wesolowski-style proofs rely on exponentiation homomorphisms ($x^{ab} = (x^a)^b$), which are strictly invalid in $\mathbb{O}_p$. Therefore, an algebraic quotient proof of exponentiation is impossible.

We bridge this "Verifiability Gap" by turning to Zero-Knowledge Scalable Transparent ARguments of Knowledge (zk-STARKs) [BSBHR18].

5.1 The Algebraic Execution Trace (AET)

The OctoSTARK iteration is exquisitely optimized for arithmetization. The step function consists entirely of low-degree polynomial operations:

- Octonionic multiplication requires exactly 64 field multiplications and 56 additions.
- The Poseidon hash $\mathcal{H}$ is natively designed to minimize multiplicative complexity within arithmetic circuits.
- The Associator computation requires 128 field multiplications.

Thus, the transition polynomial $P(Z_n, Z_{n+1}) = 0$ has a low algebraic degree with absolutely no complex control flow or bitwise operations, making it an ideal Algebraic Intermediate Representation (AIR).

5.2 Protocol Complexity

- **Prover (Evaluator):** The Evaluator computes the T sequential iterations to construct the trace. They then run the FRI (Fast Reed-Solomon Interactive Oracle Proof of Proximity) protocol over the trace. The proving overhead is highly parallelizable and executes in $\mathcal{O}(T \log^2 T)$ wall-clock time.
- **Verifier:** The Verifier receives the VDF output payload (Z_T, π). They check the FRI proximity proofs and a logarithmic number of Merkle paths. The verification time is strictly asymmetric: $\mathcal{O}(\log^2 T)$.

This isolates the sequential hardness of the non-associative algebra while outsourcing the asymmetric succinctness requirement to a zero-knowledge circuit, yielding a fully compliant VDF.

6 Conclusion

OctoSTARK introduces the first mathematically sound Verifiable Delay Function grounded in the non-associativity of the Octonions over prime fields. By strategically bypassing Artin's Theorem using an algebraic random oracle, we construct an impenetrable sequence of topological impedance resistant to tensor linearization and subspace trapping. Fused with modern STARK proof systems, this architecture yields a robust, transparent, and post-quantum primitive for timing assumptions in decentralized networks.

References

[Bae02] John C Baez. The octonions. *Bulletin of the American Mathematical Society*, 39(2):145–205, 2002.

[BBBF18] Dan Boneh, Joseph Bonneau, Benedikt Bünz, and Ben Fisch. Verifiable delay functions. In *Advances in Cryptology–CRYPTO 2018*, pages 757–788. Springer, 2018.

[BSBHR18] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable, transparent, and post-quantum secure computational integrity. IACR Cryptology ePrint Archive, Report 2018/046, 2018.

[GKR+20] Lorenzo Grassi, Dmitry Khovratovich, Christian Rechberger, Arnab Roy, and Markus Schofnegger. Poseidon: A new hash function for zero-knowledge proof systems. In *USENIX Security Symposium*, 2020.

[Pie18] Krzysztof Pietrzak. Simple verifiable delay functions. In *Innovations in Theoretical Computer Science (ITCS)*, 2018.

[Wes19] Benjamin Wesolowski. Efficient verifiable delay functions. In *Advances in Cryptology–EUROCRYPT 2019*, pages 379–407. Springer, 2019.