S-VDF: Sedenionic Verifiable Delay Functions Pure Topological Impedance via Degree-3 STARKs

Aaron M. Schutza

February 24, 2026

Abstract

Verifiable Delay Functions (VDFs) mandate a strict, un-acceleratable passage of time in cryptographic protocols. While recent constructions like OctoSTARK leverage non-associative geometry to prevent parallel loop unrolling, their reliance on alternative algebras (such as the Octonions) necessitates the injection of algebraic hash oracles to prevent associative collapse. This inflates the STARK algebraic intermediate representation (AIR) to a degree-8 polynomial, severely bottlenecking the Prover. This paper introduces the Sedenionic VDF (S-VDF). By transitioning to the strictly non-alternative 16-dimensional Sedenion algebra, we eliminate the hash oracle entirely. The resulting "Chaotic Walk" reduces the STARK transition constraint to a purely geometric degree-3 polynomial. Benchmarks over the BabyBear prime field demonstrate an 78% reduction in Prover overhead compared to legacy 8-dimensional architectures.

1 Introduction

A robust Proof-of-Sequential-Work (PoSW) must guarantee that no accumulation of parallel parallel processors (ASICs or GPUs) can compute a future state faster than a single sequential processor. The defense against such hardware acceleration is "Topological Impedance"—the utilization of non-associative algebras where $(A \times B) \times C \neq A \times (B \times C)$, strictly preventing matrix linearizations and algorithmic shortcuts.

Previous implementations utilizing the Octonions ($\mathbb{O}$) fell victim to Artin's Theorem: any subalgebra generated by two elements in an alternative algebra is associative. To break these 2D associative planes, Octonionic VDFs dynamically injected a Poseidon hash evaluation ($\mathcal{H}(Z_n)$) into the delay loop. While secure, modeling a symmetric hash function inside a STARK polynomial elevated the constraint degree to 8, forcing the Fast Reed-Solomon IOP of Proximity (FRI) to expand the execution trace by a massive blowup factor, suffocating the Prover.

2 The Sedenionic Chaotic Walk

The Sedenions ($\mathbb{S}$) are a 16-dimensional algebra constructed via the Cayley-Dickson process. Crucially, they are *not* an alternative algebra. The non-associativity is so pervasive that even localized operations twist out of 2D planes, rendering Artin's Theorem inapplicable. This allows the S-VDF to completely discard the cryptographic hash oracle.

We define the **Chaotic Walk** over a finite Galois Field $\mathbb{GF}(p)$. Let $X_0 \in \mathbb{S}$ be the starting seed vector. Let $G_t \in \mathbb{S}$ be a periodically rotating orthogonal generator vector (e.g., the canonical basis $e_{t \pmod{16}}$). The delay function is strictly evaluated as:

$$X_{t+1} \equiv (X_t \times G_t) \times X_t \pmod{p} \tag{1}$$

Because the evaluation bounds a rotating orthogonal generator between the state vector, the computation violently mixes across all 16 dimensions. The absence of an alternative structure

guarantees that no algebraic reduction can bridge X_t to X_{t+k} without sequentially evaluating the intermediate steps.

3 STARK Arithmetization and FRI Optimization

The execution trace of the S-VDF is arithmetized into a table of width 32 (16 columns mapping the state X_t, and 16 columns mapping the rotating generator G_t).

Because the transition constraint $X_{t+1} = (X_t \times G_t) \times X_t$ involves exactly two multiplications of the state variable X_t, the highest algebraic degree of the polynomial constraint is **Degree 3**.

In STARK protocols (such as Plonky3), the polynomial degree dictates the required Low Degree Extension (LDE) rate. Dropping from a degree-8 constraint (OctoSTARK) to a degree-3 constraint allows the Prover to utilize a drastically smaller Reed-Solomon interpolation domain, preserving RAM and minimizing cryptographic latency without compromising the geometric time-lock.

4 Performance Characteristics

The S-VDF engine was implemented in Rust utilizing the Plonky3 framework, operating over the 31-bit BabyBear prime field ($p = 15 \times 2^{27} + 1$).

For a target delay of approximately 2.5 seconds, the S-VDF was configured for $T = 2^{22}$ $(4,194,304)$ discrete sequential steps, tested on consumer hardware.

- **Evaluator (Time-Lock):** 2,515.4 ms
- **Prover (Work Phase):** 21,466.9 ms
- **Verifier (Succinct Argument):** $\approx$ 15.0 ms

Compared to the 96.7-second Prover time recorded for the same 2^{22} steps in the degree-8 OctoSTARK architecture, the S-VDF achieves a nearly 80% reduction in Prover overhead. The system successfully generates a verifiable receipt of the 4.19 million-step chaotic walk in ~ 21 seconds, yielding a 1403$\times$ asymmetric speedup between the Prover and Verifier.

5 Conclusion

By migrating the VDF time-lock up the Cayley-Dickson construction to the 16-dimensional Sedenions, we successfully decouple geometric impedance from symmetric hash oracles. The resulting S-VDF provides an un-acceleratable, purely algebraic delay function that can be arithmetized as a minimal degree-3 STARK polynomial, effectively neutralizing the Prover bottleneck in decentralized verifiable networks.