The Octonionic Associator Verifiable Delay Function

Breaking Artin's Theorem via Rotational Injection in $\mathbb{Z}_{2^{64}}$

Aaron M. Schutza

February 18, 2026

Abstract

We propose a novel post-quantum Verifiable Delay Function (VDF) based on the non-associative algebra of Octonions over the integer ring $\mathbb{Z}_{2^{64}}$. Standard algebraic iterations in alternative algebras suffer from Artin's Theorem, which forces trajectories generated by two elements into an associative subalgebra, rendering the Associator term zero. We introduce a *Rotational Injection* mechanism that introduces a third independent generator at every step, effectively breaking Artin's Theorem and forcing the trajectory into the non-associative bulk. Empirical benchmarks demonstrate that this construction resists parallelization (*Speedup* $\approx 1.0x$) and operates deterministically without floating-point arithmetic.

1 Introduction

Verifiable Delay Functions (VDFs) are cryptographic primitives that require a specified amount of sequential time to evaluate, but whose output can be efficiently verified. Current state-of-the-art VDFs, such as those by Wesolowski and Pietrzak, rely on squaring in groups of unknown order (typically RSA groups). While efficient, these are vulnerable to quantum attacks (Shor's algorithm) and rely on the associativity of the underlying group.

We propose a VDF that derives its sequential hardness not from number-theoretic assumptions (like factoring), but from *Topological Impedance* inherent in non-associative algebras. By operating over the Octonions ($\mathbb{O}$), we exploit the computational cost of resolving the order of operations in a chaotic trajectory.

2 Mathematical Foundations

2.1 The Ring $\mathbb{O}_{2^{64}}$

We define the computational domain as the Octonions with coefficients in the ring of unsigned 64-bit integers, $\mathbb{Z}_{2^{64}}$. An element $X \in \mathbb{O}_{2^{64}}$ is represented as:

$$X = \sum_{i=0}^{7} x_i e_i, \quad x_i \in \mathbb{Z}_{2^{64}}$$

Arithmetic operations (addition and multiplication) are performed modulo 2^{64}. This ensures deterministic behavior across hardware platforms, avoiding the non-determinism of floating-point arithmetic.

2.2 The Associator

The defining feature of the Octonions is non-associativity. For elements $A, B, C \in \mathbb{O}$, the associative law fails: $(AB)C \neq A(BC)$. We define the **Associator** as the error term:

$$[A, B, C] = (AB)C - A(BC)$$

In a cryptographic context, this term represents a hazard or impedance that prevents algebraic simplification (linearization) of the delay function.

3 The Construction

3.1 The Failure of Standard Iteration (Artin's Trap)

A naive attempt to construct an Octonionic VDF might use the iteration:

$$Z_{n+1} = Z_n^2 + C$$

where Z_0 is the seed and C is a constant. However, **Artin's Theorem** states that in any alternative algebra, the subalgebra generated by any two elements is associative. Since every Z_n is formed strictly from combinations of Z_0 and C, the entire trajectory lies within an associative subalgebra (isomorphic to the Quaternions or Complex numbers). **Consequence:** The Associator $[Z_n, Z_{n-1}, C]$ vanishes to zero, destroying the unique security property of the Octonions.

3.2 The Solution: Rotational Injection

To break Artin's Theorem, we must introduce a third independent generator into the recurrence relation that does not commute or associate with the subalgebra $\langle Z_n, C \rangle$. We achieve this via a bitwise/coefficient rotation operator.

Let $\mathrm{Rot}(X)$ be the operation that cyclically shifts the 8 coefficients of octonion X:

$$\mathrm{Rot}(\sum x_i e_i) = \sum x_i e_{(i+1) \pmod 8}$$

We define the **Synergeia Iteration** as:

$$Z_{n+1} = Z_n^2 + C + [Z_n, C, \mathrm{Rot}(Z_n)] \qquad (1)$$

The term $[Z_n, C, \mathrm{Rot}(Z_n)]$ is the *Associator Hazard*. By injecting $\mathrm{Rot}(Z_n)$, we ensure that the three inputs to the associator are linearly independent generators, forcing a non-zero result that perturbs the trajectory into the non-associative bulk.

4 Algorithm

Algorithm 1: Octonionic Associator VDF Evaluation

```
Input: Seed $S$, Iterations $T$
Output: Final State $Z_T$
$C \leftarrow \mathrm{Derive}(S)$;
$Z_0 \leftarrow \mathrm{Derive}(S \oplus \mathrm{0xDEADBEEF})$;
for $i \leftarrow 0$ to $T$ do
    $Sq \leftarrow Z_i \times Z_i$;
    $R \leftarrow \mathrm{Rot}(Z_i)$;
    $A \leftarrow (Z_i \times C) \times R - Z_i \times (C \times R)$;
    $Z_{i+1} \leftarrow Sq + C + A \pmod{2^{64}}$;
end
return $Z_T$;
```

5 Experimental Validation

We implemented the proposed VDF in Rust using ‘u64‘ arithmetic. We benchmarked the system on a multi-core processor to test for sequential hardness.

5.1 Test 1: Associator Hazard Verification

We verified that the Associator term does not vanish in the new construction.

- **Naive Iteration ($Z^2 + C$):** Associator Hazard $= 0$ (Artin's Trap confirmed).
- **Synergeia Iteration:** Associator Hazard $\neq 0$. The trajectory successfully utilizes the full 8-dimensional manifold.

5.2 Test 2: Sequentiality & Parallel Resistance

We simulated a parallel attack where an adversary attempts to compute the second half of the chain ($T/2 \to T$) simultaneously with the first half.

Mode	Iterations	Time (s)	Throughput
Sequential	1,000,000	0.5700s	1.75 M/ops
Parallel (2 Threads)	1,000,000	0.5722s	-

Table 1: Benchmark Results

Result: The effective speedup was **0.9961x**. This confirms that the VDF is strictly sequential; adding threads provided no advantage because Z_{n+1} strongly depends on the specific, non-associative perturbation of Z_n.

6 Security Analysis

6.1 Post-Quantum Hardness

Unlike group-based VDFs, the security of this construction does not rely on the Hidden Subgroup Problem (HSP). Shor's algorithm, which solves HSP for finite abelian groups, does not apply to the non-associative structure of $\mathbb{O}_{2^{64}}$. The best known quantum attack against unstructured non-associative mapping is Grover's algorithm, which provides only a quadratic speedup ($O(\sqrt{N})$), leaving the system secure with 256-bit entropy.

6.2 Topological Impedance

The hardness of the delay is geometric. An attacker trying to shortcut the computation $Z_0 \to Z_T$ must solve a system of equations where the parentheses cannot be removed or reordered. The number of possible bracketing orders for a sequence of length N grows according to the Catalan numbers, creating an exponential barrier to algebraic simplification.

7 Conclusion

We have presented the first VDF construction that explicitly leverages the failure of associativity as a cryptographic primitive. By identifying and bypassing Artin's Theorem via rotational injection, we created a strictly sequential, integer-based function that resists parallelization. This opens a new avenue for post-quantum time-lock puzzles and randomness beacons based on hypercomplex algebra.