SUOV: Sedenionic Unbalanced Oil and Vinegar Post-Quantum Signatures over $\mathbb{GF}(p)$

Aaron M. Schutza

February 24, 2026

Abstract

Multivariate Quadratic (MQ) signature schemes, such as Unbalanced Oil and Vinegar (UOV), offer robust resistance against quantum cryptanalysis via Shor's algorithm. However, standard MQ schemes suffer from prohibitively large public key sizes, often exceeding 50 KB, limiting their viability in bandwidth-constrained environments. This paper introduces Sedenionic Unbalanced Oil and Vinegar (SUOV), a novel signature scheme that maps the MQ problem onto the non-associative topological lattice of the 16-dimensional Sedenion algebra over a finite Galois Field $\mathbb{GF}(p)$. By leveraging the fixed Cayley-Dickson algebraic tensor to enforce quadratic mixing, SUOV successfully compresses the public key into a single 16×16 affine transformation matrix (≈ 1 KB). We formalize the SUOV trapdoor generation routine, the $O(1)$ signing algorithm, and demonstrate Existential Unforgeability under Chosen Message Attacks (EUF-CMA) via a strict Hash-to-Sedenion embedding.

1 Introduction

The impending realization of cryptanalytically relevant quantum computers poses an existential threat to signature schemes reliant on the discrete logarithm and integer factorization problems (e.g., ECDSA, RSA). Post-Quantum Cryptography (PQC) standards have heavily investigated Multivariate Quadratic (MQ) systems, whose security reduces to the NP-Hard problem of solving systems of quadratic equations over finite fields.

While MQ schemes like UOV execute rapidly, they require the public key to contain the entire set of random quadratic polynomial coefficients. Sedenionic Unbalanced Oil and Vinegar (SUOV) resolves this structural bottleneck. Instead of generating random polynomials, SUOV utilizes the natively fixed, strictly non-associative geometry of the Rank-5 Sedenion algebra. The quadratic mixing is offloaded to the algebra itself, reducing the public key to a simple linear basis translation matrix that obscures a hidden isotropic subspace.

2 Mathematical Foundation: Discrete Sedenions

SUOV operates within the Sedenion algebra ($\mathbb{S}$) mapped over a large cryptographic prime field $\mathbb{GF}(p)$. A Sedenion S is represented as a 16-dimensional vector. The multiplication of two Sedenions $X = (x_a, x_b)$ and $Y = (y_a, y_b)$ modulo p is defined recursively via the Cayley-Dickson construction:

$$X \times Y \equiv (x_a y_a - y_b^* x_b,\ y_b x_a + x_b y_a^*) \pmod{p} \tag{1}$$

Because the algebra is non-associative ($A(BC) \neq (AB)C$), the expression $(S \times P) \times (\mathcal{M}S)$ cannot be linearly factored, naturally yielding a dense system of 16 multivariate quadratic equations.

3 The SUOV Signature Scheme

3.1 Key Generation & The Secret Subspace

The trapdoor relies on creating a **Totally Isotropic Subspace**, dividing the 16 dimensions of $\mathbb{S}$ into v Vinegar variables and o Oil variables (where $v + o = 16$). The core mechanic dictates that Oil variables must never multiply with other Oil variables within the central map.

1. **The Secret Central Map ($\mathcal{M}_{sec}$):** The signer constructs a 16×16 central matrix over $\mathbb{GF}(p)$ such that evaluating $(S \times P) \times (\mathcal{M}_{sec}S)$ yields no quadratic $o_i o_j$ cross-terms.
2. **The Secret Basis (T):** The signer generates a dense, randomly invertible 16×16 matrix $T \in GL_{16}(\mathbb{GF}(p))$. This matrix maps the public coordinate system into the signer's secret Oil-Vinegar subspace.
3. **The Public Key ($\mathcal{M}_{pub}$):** The signer obfuscates the central map by conjugating it with the secret basis:
$$\mathcal{M}_{pub} \equiv T \cdot \mathcal{M}_{sec} \cdot T^{-1} \pmod{p} \tag{2}$$

The Private Key is the tuple $(T, \mathcal{M}_{sec})$. The Public Key is strictly the matrix $\mathcal{M}_{pub}$.

3.2 The Hash-to-Sedenion Paradigm

To achieve Existential Unforgeability, raw data is never signed directly. A message M is hashed using a pre-image resistant function (e.g., SHA3-256) and deterministically mapped to a 16-dimensional vector over $\mathbb{GF}(p)$:

$$P_{geom} = \text{HashToSedenion}(M) \tag{3}$$

3.3 The $O(1)$ Signing Algorithm

To sign a message M, the signer utilizes their hidden knowledge of T to bypass the NP-Hardness of the public quadratic system.

Algorithm 1 SUOV Signing Algorithm

1: $P_{geom} \leftarrow \text{HashToSedenion}(M)$
2: **Translate to Secret Basis:** Evaluate equations in the domain of $S' = T^{-1}S$
3: **Vinegar Randomization:** Randomly assign values in $\mathbb{GF}(p)$ to the v Vinegar variables.
4: **Linear Collapse:** Substitute Vinegar values. The absence of $o_i o_j$ terms instantly reduces the MQ system to 16 linear equations with o unknowns.
5: **Solve:** Execute Gaussian elimination to solve for the remaining Oil variables. (If singular, return to Step 3).
6: **Basis Reversion:** Reassemble $S' = [v_1 \dots v_v, o_1 \dots o_o]^T$.
7: **Output Signature:** $S \equiv TS' \pmod{p}$.

3.4 Verification

Any verifier possessing $\mathcal{M}_{pub}$, the signature S, and the message M evaluates the trapdoor in $O(1)$ time:

$$(S \times \text{HashToSedenion}(M)) \times (\mathcal{M}_{pub}S) \equiv 0 \pmod{p} \tag{4}$$

If the product is the absolute zero vector, the signature is geometrically valid.

4 Security Analysis

4.1 Existential Unforgeability under Chosen Message Attacks (EUF-CMA)

An adversary attempting to forge a signature for a chosen message M_{evil} must solve for S such that $(S \times P_{evil}) \times (\mathcal{M}_{pub} S) \equiv 0 \pmod{p}$. Because $P_{evil} = \text{HashToSedenion}(M_{evil})$, the adversary cannot work backwards from a known zero-divisor trajectory to find a readable message. The payload collision resistance reduces entirely to the cryptographic collision resistance of the underlying hash function.

4.2 MQ-Hardness and The Isomorphism of Polynomials

For an adversary lacking the secret basis T, the Vinegar and Oil variables are indistinguishably entangled across all 16 Sedenionic dimensions. Evaluating the public trapdoor equation yields a dense, pseudo-random system of 16 multivariate quadratic polynomials. Recovering the signature S without T directly requires solving the NP-Hard MQ problem. Furthermore, recovering the private key $(T, \mathcal{M}_{sec})$ from $\mathcal{M}_{pub}$ requires solving the Isomorphism of Polynomials (IP) problem, which remains classically and quantumly intractable.

5 Conclusion

By offloading the combinatorial complexity of quadratic mixing to the intrinsic non-associative geometry of the Sedenions, SUOV provides a highly secure, post-quantum signature scheme. It achieves the execution speed and security bounds of traditional UOV architectures while severely compressing the public key footprint, positioning it as an optimal primitive for next-generation distributed networks and embedded systems.