SQE: Sedenionic Quadratic Encapsulation
A Zero-Noise Post-Quantum KEM over $\mathbb{GF}(p)$

Aaron M. Schutza

February 24, 2026

Abstract

Current Post-Quantum Key Encapsulation Mechanisms (KEMs) standardizing on lattice-based Learning With Errors (LWE) suffer from inherent decryption failure rates due to probabilistic noise vectors. Multivariate Quadratic (MQ) encryption schemes theoretically bypass this limitation but have historically fallen to linearization attacks due to the commutative nature of the underlying finite fields. This paper introduces Sedenionic Quadratic Encapsulation (SQE), a deterministic, zero-noise KEM that leverages the strictly non-associative geometry of the Sedenion algebra over $\mathbb{GF}(p)$. By masking a native $O(1)$ Sedenion square root trapdoor behind random affine transformations, SQE achieves perfect decryption reliability while presenting an NP-Hard multivariate quadratic system to observers.

1 Introduction

The cryptographic challenge of Multivariate Public Key Cryptography (MPKC) lies in designing a central map $F(X)$ that is efficiently invertible by the private key holder but computationally intractable to reverse when obscured by affine transformations. Historic implementations, such as the Matsumoto-Imai C^* scheme, utilized finite field exponentiation but were broken by linear algebraic modeling.

SQE mitigates these vulnerabilities by transitioning the central map into a non-division, strictly non-associative algebra: the 16-dimensional Sedenions ($\mathbb{S}$). Because Sedenionic multiplication enforces extreme topological impedance, linearization attacks shatter. SQE utilizes the simplest possible non-linear map—Sedenionic Squaring ($X \times X$)—creating a perfectly deterministic trapdoor with zero reliance on noise variables.

2 The Sedenion Square Root Trapdoor

Let $X \in \mathbb{S}$ over a finite field $\mathbb{GF}(p)$. X can be decomposed into a real scalar x_0 and a 15-dimensional imaginary vector $\vec{v}$. Sedenionic squaring simplifies geometrically:

$$X^2 = (x_0^2 - ||\vec{v}||^2) + 2x_0\vec{v}$$

If an entity knows the squared ciphertext $C = c_0 + \vec{c}$, reversing the operation to find X is an $O(1)$ procedure. Substituting $\vec{v} = \frac{\vec{c}}{2x_0}$ into the real component yields:

$$c_0 \equiv x_0^2 - \frac{||\vec{c}||^2}{4x_0^2} \pmod{p}$$

Rearranging to isolate x_0^2 yields the core trapdoor equation:

$$4(x_0^2)^2 - 4c_0(x_0^2) - ||\vec{c}||^2 \equiv 0 \pmod{p}$$

The private key holder applies the standard quadratic formula and the Tonelli-Shanks algorithm to solve for x_0, subsequently recovering $\vec{v}$.

3 The SQE Protocol

3.1 Key Generation

The receiver (Alice) generates two secret, randomly invertible 16×16 matrices $L_1, L_2 \in GL_{16}(\mathbb{GF}(p))$. The public key $\mathcal{P}$ evaluates as:

$$\mathcal{P}(X) \equiv L_1 \cdot ((L_2 \cdot X) \times (L_2 \cdot X)) \pmod{p}$$

The private key is the tuple (L_1, L_2).

3.2 Encapsulation

To transmit a symmetric session key, the sender (Bob) executes the following:

1. Generate a random 16-dimensional vector $R \in \mathbb{GF}(p)^{16}$.
2. Derive the session key: $Key = \text{Hash}(R)$.
3. Encapsulate R using Alice's public affine transformations:

$$C \equiv L_1 \cdot ((L_2 \cdot R) \times (L_2 \cdot R)) \pmod{p}$$

4. Transmit C and a 1-bit parity hint (to resolve the $\pm X$ sign ambiguity of square roots).

3.3 Decapsulation

Alice receives C and executes her trapdoor:

1. Strip the outer mask: $C' \equiv L_1^{-1} \cdot C \pmod{p}$.
2. Execute the Sedenion Square Root algorithm on C' to recover the intermediate vector X.
3. Strip the inner mask: $R \equiv L_2^{-1} \cdot X \pmod{p}$.
4. Verify the parity hint to select the correct root, and derive $Key = \text{Hash}(R)$.

4 Security Analysis

To an observer without L_1 and L_2, the public key $\mathcal{P}(X)$ expands into a dense system of 16 multivariate quadratic polynomials. Reversing this map without the secret basis directly reduces to the NP-Hard MQ Problem. Because Sedenion multiplication is non-associative, algebraic attempts to factor or isolate the inner transformation L_2 inherently fail.