Frobenius-UOV (FUOV)

A Very Efficient Multivariate Public Key Signature Scheme

Gilles Macario-Rat, Orange Research

May 29, 2026

Background: Digital Signatures and UOV

- **Signature scheme (high-level):**
  - **KeyGen:** outputs a public key pk and a secret key sk.
  - **Sign:** uses sk to produce a signature σ on a message m.
  - **Verify:** uses pk to check that σ matches m.
- **Goal:** fast verification and **EUF-CMA** security (unforgeability under chosen-message attacks).
- **Multivariate signatures:** the public key is a system of quadratic polynomials $F : \mathbb{F}^n \to \mathbb{F}^m$.
- **UOV trapdoor:** split variables into **Vinegar** (public randomness) and **Oil** (hidden); with the right basis, signing reduces to solving a **linear** system.

Background: Hash-and-Sign, the Standard Pattern

- **Why hash?** compress arbitrary-length messages into a fixed-size digest.
- **Hash-and-sign workflow:**
  1. Compute a digest $d = H(m)$ (often with domain separation / context).
  2. Map to a signing target (e.g., $y = \mathrm{Encode}(d) \in \mathbb{F}^m$).
  3. Produce a signature $\sigma \leftarrow \mathrm{Sign}(sk, y)$.
  4. Verification recomputes y from m and checks $\mathrm{Verify}(pk, y, \sigma) = 1$.
- **In multivariate schemes:** signing typically means finding x such that $F(x) = y$ (using the trapdoor), and σ contains x (plus optional salt).

1. FUOV vs. Traditional UOV

- **Standard UOV:** Relies on a quadratic system over a base field F_p with many variables and equations. Uses a special subspace on which the quadratic system vanishes.
- **FUOV Innovation:** Leverages a **field extension** $F_q = F_{p^e}$ and **Frobenius forms** $(x_i^{p^a} x_j^{p^b})$.
- **Structure:** Stable under linear change of variables, preserving the trapdoor while drastically reducing the public variable count.
- **Oil subspace:** Uses a secret subspace of dimension o=1.
- **Parameters:** FUOV uses only **one equation** $(m = 1)$ and 5 variables $(n = 5)$ over F_q.

2. Frobenius forms (FUOV core ingredient)

Let $\mathbb{F}_q = \mathbb{F}_{p^e}$ and $x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$. Define the Frobenius twist

$$x^{[a]} := (x_1^{p^a}, \ldots, x_n^{p^a}).$$

- A **Frobenius (bi-)form** of type (a, b) is

$$f(x) := \sum_{i,j} A_{ij}\, x_i^{p^a} x_j^{p^b} \;=\; x^{[a]} A\, (x^{[b]})^{\mathsf{T}}, \quad A \in \mathbb{F}_q^{n \times n}.$$

- **Matrix view:** the public map is a collection of such matrices $(A_k)_{k=1}^m$, i.e., $F_k(x) = x^{[a]} A_k (x^{[b]})^{\mathsf{T}}$.
- **Multi-degree property:** f has *bi-degree* (p^a, p^b): it is linear in $x^{[a]}$ and linear in $x^{[b]}$ (but not a standard degree-2 monomial over $\mathbb{F}_q$).

3. FUOV equations (toy example: $o = 1$, $v = 2$, $\ell = 2$)

- secret equations:

$$\Lambda^{[a_1]} A_1 (\Lambda^{[b_1]})^{\mathsf{T}} = 0 \quad \Lambda^{[a_2]} A_2 (\Lambda^{[b_2]})^{\mathsf{T}} = 0$$

  Λ and A_i are random, except one coefficient of each A_i, which are computed as to satisfy the corresponding equation. Equivalently, in a change of coordinates, matrices have a square 'zero' part.

- public equation:

$$X^{[a_1]} A_1 (X^{[b_1]})^{\mathsf{T}} + X^{[a_2]} A_2 (X^{[b_2]})^{\mathsf{T}} = H$$

  Can easily be solved as $f(x\Lambda + V) = H$ where V is random, and the equation is linear in x.

Conjecture : Solving degree (up to conversion into MQ system over Fp) is highly dependent on the multi-degree.

4. Arithmetic Optimizations

Fast resolution of the linear system $M \cdot X = \Gamma$ during signing:

- F_q **Representation:** Uses basis $(1, \xi, \ldots, \xi^{e-1})$ to treat F_q as an F_p^e vector space [14].
- **Precomputations:** Storage of Frobenius powers ξ^{ip^r} and basis products $\xi^i \xi^j$ to avoid redundant calculations.
- L **Matrices:** Pre-calculates L_{ark} and L_{brk} to quickly transform Frobenius forms into an F_p linear system.
- **Linearization:** Efficiently converts $x \mapsto \alpha x^{p^a}$ into $e \times e$ matrices over F_p to build system matrix M.

5. Analysis of Known Attacks

- **Direct Attack:** Solving $Pub(X) = h$. Becomes an $e \times ne$ quadratic system over F_p. Complexity $\approx 2^{154}$ for Level I.
- **Kipnis-Shamir:** Not directly applicable on F_q (lacks standard matrix representation). On F_p, complexity bounded by $O(p^{e(v-o)}) > 2^{151}$.
- **MinRank:** On F_q, fails as subspace intersections are likely null. On F_p, prohibitive complexity (2^{336} for Level I).
- **Wedge Attack:** Infeasible; dimensions $\binom{en}{ev}$ are too large to process.

6. FUOV Specific Attacks and Open Problems

- **Univariate "DO" Polynomials ($x^{p^a+p^b} = h$):**
  - Polynomial-time solvable when converted to F_p system (since $a \neq b$).
  - Complexity $CP(m, p, e)$ estimated at $O(\binom{e+e/2}{e}^2)$ for $m \geq 3$ monomials.
- **Key Recovery:**
  - Finding the secret "Oil" subspace.
  - On F_p, adding $o(e-1)$ linear equations ensures solutions convert back to F_q.
  - Complexity $CI(s, t, p, e, n)$ is exponential if $s(t+1) > n$.

7. Key and Signature Size Advantages

FUOV achieves extreme compactness compared to current standards:

NIST Level	Signature	Public Key	Secret Key
I (AES-128)	223 bytes	207 bytes	32 bytes
III (AES-192)	366 bytes	350 bytes	32 bytes
V (AES-256)	509 bytes	493 bytes	32 bytes

Table: Comparative Sizes

- **Compactness:** Public key is smaller than RSA-2048.
- **Compression:** Uses seeds to generate A^* matrices, explicitly storing only derived coefficients.

Thank you for your attention.