# Not Easy to Prepare a Pesto: Cryptanalysis of a Multivariate Public-Key Scheme

**Ottawa**, August 26, 2026

C.Beierle[1], P. Felke[2]

[1]Ruhr-University Bochum, [2]University of Applied Sciences Emden/Leer

# Preliminaries

- $\mathbb{F}_q$ denotes a finite field, i.e. $q = p^m, p$ prime, $\mathbb{F}_q^n$ the vector space of dimension $n$.
- The canonical unit basis of $\mathbb{F}_q^n$ is denoted with $e_1 = (1, 0, \ldots, 0)^T, \ldots, e_n = (0, \ldots, 0, 1)^T$.
- The subspace generated $v_1, \ldots, v_l \in \mathbb{F}_q^n$ is denoted by $< v_1, \ldots, v_l >$.
- Matrices are denoted by capital letters and $Id$ denotes the identity matrix in case of $n = m$.

# Preliminaries

- Any function $F$ can be represented as $F = (f_1, \ldots, f_m)$ with $f_i \colon \mathbb{F}_q^n \to \mathbb{F}_q, 1 \leq i \leq m$.
- Any function $f \colon \mathbb{F}_q^n \to \mathbb{F}_q$ has a unique representation of the form $f(x) = \sum_{u \in \mathbb{N}^n} a_u x_1^{u_1} \cdots x_n^{u_n} \bmod (x_1^q - x_1, \ldots, x_n^q - x_n)$ with $a_u \in \mathbb{F}_q$ and all $u_1, \ldots, u_n$ less than $q$, called the *ANF*.
- It can be extended vectorially by setting $F(x) = \sum_{u \in \{0,\ldots,q-1\}^n} a_u x_1^{u_1} \cdots x_n^{u_n}$ with $a_u \in \mathbb{F}_q^m$.
- Define $\deg(F) := \max\{\sum_{i=1}^n u_i \mid u \in \{0, \ldots, q-1\}^n, a_u \neq 0\}$. We call $F$ *quadratic* if $\deg(F) = 2$.
- If all terms have the same degree then $F$ is called *homogeneous*.

# Basic Principle

$$\begin{array}{lccc} \text{Encryption (public):} & m \in \mathbb{F}_q^n & \xrightarrow{G_{\text{pub}} = A_1 \circ G \circ A_2} & c \in \mathbb{F}_q^m \\ \text{Decryption (secret):} & \uparrow A_2^{-1} & & \downarrow A_1^{-1} \\ & m' \in \mathcal{M}' & \xleftarrow{G^{-1}} & c' \end{array}$$

- $G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is equipped with a trapdoor to invert it and $\deg(G) \geq 2$.
- $A_1, A_2$ are affine mappings.
- $(G, A_1, A_2)$ is the secret key. $G_{\text{pub}} = A_1 \circ G \circ A_2$ the public key.

# Basic Principle

$$\begin{array}{lccc} \text{Encryption (public):} & m \in \mathbb{F}_q^n & \xrightarrow{G_{\text{pub}} = A_1 \circ G \circ A_2} & c \in \mathbb{F}_q^m \\ \text{Decryption (secret):} & \uparrow A_2^{-1} & & \downarrow A_1^{-1} \\ & m' \in \mathcal{M}' & \xleftarrow{G^{-1}} & c' \end{array}$$

- $G : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is equipped with a trapdoor to invert it and $\deg(G) \geq 2$.
- $A_1, A_2$ are affine mappings.
- $(G, A_1, A_2)$ is the secret key. $G_{\text{pub}} = A_1 \circ G \circ A_2$ the public key.

If given a ciphertext $c = (c_1, \ldots, c_n)$ the system of equations

$$\begin{aligned} G\text{pub}_1(x_1, \ldots, x_n) &= c_1 \\ &\vdots \\ G\text{pub}_n(x_1, \ldots, x_n) &= c_n \end{aligned}$$

can be solved efficiently over $\mathbb{F}_q$ the system is broken.

# Security Assumption

## The MQ Problem

Finding a solution to a system of multivariate quadratic equations over a finite field $\mathbb{F}_q$ is NP-hard.

# Security Assumption

## The MQ Problem

Finding a solution to a system of multivariate quadratic equations over a finite field $\mathbb{F}_q$ is NP-hard.

☞Any system of multivariate equations of degree $\geq 3$ can be transformed into a system of quadratic equations.

# Security Assumption

## The MQ Problem

Finding a solution to a system of multivariate quadratic equations over a finite field $\mathbb{F}_q$ is NP-hard.

☞Any system of multivariate equations of degree $\geq 3$ can be transformed into a system of quadratic equations.

- Systems of degree $\geq 3$ are motivated by the idea to get particular hard to solve instances of multivariate equations and in particular of the MQ problem more easily.
- While lots of proposed schemes were broken a few systems based on the so-called unbalanced Oil&Vinegar principle to build a trapdoored $G$ of degree 2 survived until today.
- Pesto, the system attacked in this talk, employs the OV principle to get public keys of degree 4.

# Unbalanced Oil & Vinegar (UOV)

Partition $\{z_1, \ldots, z_n\}$ variables into $v$ *Vinegar* variables $V$ and $n - v$ *Oil* variables $O$.

## OV Polynomial

An OV polynomial $P_{OV}$ has the form:

$$\sum_{i,j \in V} \alpha_{ij} z_i z_j + \sum_{i \in V, j \in O} \beta_{ij} z_i z_j + \sum_{k=1}^{n} \gamma_k z_k + \delta.$$

# Unbalanced Oil & Vinegar (UOV)

Partition $\{z_1, \ldots, z_n\}$ variables into $v$ *Vinegar* variables $V$ and $n - v$ *Oil* variables $O$.

## OV Polynomial

An OV polynomial $P_{OV}$ has the form:

$$\sum_{i,j \in V} \alpha_{ij} z_i z_j + \sum_{i \in V, j \in O} \beta_{ij} z_i z_j + \sum_{k=1}^{n} \gamma_k z_k + \delta.$$

- **Crucial property:** There are no Oil $\times$ Oil terms.

# Unbalanced Oil & Vinegar (UOV)

Partition $\{z_1, \ldots, z_n\}$ variables into $v$ *Vinegar* variables $V$ and $n - v$ *Oil* variables $O$.

## OV Polynomial

An OV polynomial $P_{OV}$ has the form:

$$\sum_{i,j \in V} \alpha_{ij} z_i z_j + \sum_{i \in V, j \in O} \beta_{ij} z_i z_j + \sum_{k=1}^{n} \gamma_k z_k + \delta.$$

- **Crucial property:** There are no Oil $\times$ Oil terms.
- **The trapdoor:** The system becomes linear when fixing the Vinegar variables with random values. ☞Gaussian elimination.
- **Unbalanced:** $v > n - v$. The original proposal by Patarin (1997) was balanced, i.e. $n = 2v$ and broken by Kipnis and Shamir (1998).

# The Pesto Encryption/Signature Scheme

- Proposed by Calderini, Caminata and Villa (J. Cryptol. 2025).
- Pesto combines the Oil&Vinegar approach with the so-called CCZ equivalence to build systems with public keys of degree 4. As CCZ equivalence is neither required to understand Pesto nor has any influence on its security we skip the details.
- In 2026 it was shown that the degree-4 system can be reduced to a quadratic system (Caminata et al., 2026). The authors did not outline an actual attack.

# The Pesto Encryption/Signature Scheme

- Proposed by Calderini, Caminata and Villa (J. Cryptol. 2025).
- Pesto combines the Oil&Vinegar approach with the so-called CCZ equivalence to build systems with public keys of degree 4. As CCZ equivalence is neither required to understand Pesto nor has any influence on its security we skip the details.
- In 2026 it was shown that the degree-4 system can be reduced to a quadratic system (Caminata et al., 2026). The authors did not outline an actual attack.

☞We present a full attack breaking all proposed instances of Pesto in practical time by recovering an equivalent key.

# The Central Map $G$

Let $t \leq \min(n, m)$ and $s \leq n - t$. The input variables are partitioned into $x = (x_1, \ldots, x_t)$ and $y = (y_1, \ldots, y_{n-t})$.
The central map $G(x, y) = \big(G_Q(x, y), G_U(x, y)\big)$ is defined by:

**A quadratic map (top $t$ components):**

- $G_Q(x, y) := x - \mathfrak{q}(y)$,
  where $\mathfrak{q} : \mathbb{F}_q^{n-t} \to \mathbb{F}_q^t$ is a randomly chosen quadratic mapping.

**An OV map (bottom $m - t$ components):**

- $G_U(x, y) := U\big(x - \mathfrak{q}(y), y\big)$,
  where $U : \mathbb{F}_q^n \to \mathbb{F}_q^{m-t}$ and its components are OV polynomials with
  - Vinegar variables: $V = \{x_1, \ldots, x_t, y_1, \ldots, y_s\}$.
  - Oil variables: $O = \{y_{s+1}, \ldots, y_{n-t}\}$.

☞$V$ contains variables in $y$ as otherwise the system becomes insecure.

# The Pesto Encryption/Signature Scheme

**Public key:** $G_{\text{pub}} = A_1 \circ G \circ A_2$,
$A_1(x) = S(x) + c, A_2(x) = T(x) + d$ affine bijections
**Secret key:** $(G, A_1, A_2)$.
As an example decryption of a ciphtertext $c$ is shown:

1. From $c \in \mathbb{F}_q^m$ compute $c' = A_1^{-1}(c)$.
2. Set $z' = A_2(z)$, where $z$ is the plaintext. It is $c' = G(z')$, $c' = (c'_Q, c'_U) \in \mathbb{F}_q^t \times \mathbb{F}_q^{m-t}$ and $z' = (x', y') \in \mathbb{F}_q^t \times \mathbb{F}_q^{n-t}$, where $c'_Q = x' - \mathfrak{q}(y'), c'_U = U(c'_Q, y')$.
   For fixed values $y'_1, \ldots, y'_s$, the system of equations $c'_U = U(c'_Q, y')$ becomes linear in $y'_{s+1}, \ldots, y'_{n-t}$. By exhaustive search a set of values $\mathcal{Y}' \subset \mathbb{F}_q^{n-t}$ is computed.
3. For all $y \in \mathcal{Y}'$, a value $x'$ is computed from $x' - \mathfrak{q}(y')$ and finally $z = A_2^{-1}(z') = A_2^{-1}((x', y'))$.

# The Attack - Recovering an equivalent Key

## Equivalent Key

An equivalent key is a triple $(G', A_1', A_2')$ such that

$$G_{\text{pub}} = A_1 \circ G \circ A_2 = A_1' \circ G' \circ A_2',$$

where $A_1', A_2'$ are affine and $G'$ can be inverted with the same asymptotic complexity as $G$.

- The goal of the attack is to recover an equivalent key $G_{\text{pub}} = A_1' \circ G' \circ A_2'$, where $G' = (G'_Q, G'_U) = (\mathfrak{l}(x) - \mathfrak{q}'(y), U'(\mathfrak{l}(x) - \mathfrak{q}'(y), y)$, $\mathfrak{l}$ a linear map over $\mathbb{F}_q^t$ and $U'$ consists of OV polynomials with $O, V$ as in $U$.

- The designers proposed a compressed variant of Pesto, with $A_1(x) = S(x) + c$ and $S = \begin{pmatrix} A & 0 \\ B & C \end{pmatrix}$, i.e. the submap $G_U$ is only mixed with itself.
- Any public key $G_{\text{pub}}$ can be transformed into compressed variant with complexity $\mathcal{O}(m^2n^4)$ (already observed by the designers).
- For simplicity we restrict to show the attack for the compressed version. By a slight abuse of notation the first $t$ components of $G_{\text{pub}}$ are equal to $A_1 \circ G_Q \circ A_2 = A_1 \circ (x - \mathfrak{q}(y)) \circ A_2$.
- We denote these upper $t$ components by $\mathfrak{q}'_1, \ldots, \mathfrak{q}'_t$.

The attack is based on the theory of quadratic forms.

# Quadratic Forms

## Radicals, Isometry and Isotropy

1. A quadratic form $\mathfrak{q}$ is either zero or its ANF is a homogeneous quadratic polynomial (set $x_i = x_i^2$ for $\mathbb{F}_q = \mathbb{F}_2$).
2. For a quadratic form $\mathfrak{q}$, its associated symmetric bilinear form is $\mathfrak{B}_\mathfrak{q}(u, v) = \mathfrak{q}(u + v) - \mathfrak{q}(u) - \mathfrak{q}(v)$. The radical is:

$$\mathrm{rad}(\mathfrak{B}_\mathfrak{q}) = \{v \in \mathbb{F}_q^n \mid \mathfrak{B}_\mathfrak{q}(u, v) = 0 \text{ for all } u \in \mathbb{F}_q^n\}.$$

3. A vector $v$ with $\mathfrak{q}(v) = 0$ is called isotropic.
4. Two quadratic forms $\mathfrak{q}, \mathfrak{q}'$ over $\mathbb{F}_q^n$ are called isometric if there exists a bijective linear mapping $L$ with $\mathfrak{q}(x) = \mathfrak{q}'(L(x))$. $L$ maps radicals onto radicals and isotropic vectors onto isotropic vectors.

# Step 1: Transform $\mathfrak{q}'_i$ into $\mathfrak{l}_i(x) - \mathfrak{q}''_i(y)$

Recall $A_2(x) = T(x) + d$.

1. In $x - \mathfrak{q}(y)$ the variables $x_1, \ldots, x_t$ appear only linearly and $\mathfrak{q}(y)$ is random. Let $\mathfrak{q}_{h,i}(y)$ denote the homogeneous part of $(x - \mathfrak{q}(y))_i$. It is expected that $\bigcap_{i=1}^{t} \mathrm{rad}(\mathfrak{B}_{\mathfrak{q}_{h,i}}) = \langle e_1, \ldots, e_t \rangle$ with high probability.
2. Let $\mathfrak{q}'_{h,i}$ denote the homogeneous part of $\mathfrak{q}'_i$. By isometry, $\bigcap_{i=1}^{t} \mathrm{rad}(\mathfrak{B}_{q'_{h,i}}) = \langle T^{-1}(e_1), \ldots, T^{-1}(e_t) \rangle$.
3. Generate a matrix $T'^{-1}$, where the first $t$ columns are a basis $t'_1, \ldots, t'_t$ of the above space and the last $n - t$ columns $t'_{t+1}, \ldots, t'_n$ extend it to a basis of $\mathbb{F}_q^n$. Then
$$TT'^{-1} = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}.$$
4. Then the composition $G' := G_{\mathsf{pub}} \circ T'^{-1}$ yields the transformation into $g'_i = \mathfrak{l}_i(x) - \mathfrak{q}''_i(y)$.

# Step 2: Retrieve $U'$ and $G'_U$

- We have
  $g'_l = \sum_{1 \le j \le k \le t} \alpha'_{jkl} g'_j g'_k + \sum_{j \in \{1,\dots,t\}, k \in \{1,\dots,n-t\}} \beta'_{jkl} g'_j y_k + \sum_{1 \le i \le j \le n-t} \gamma'_{ijl} y_i y_j + \sum_{i=1}^{t} \delta'_{il} g'_i + \sum_{j=1}^{n-t} \nu'_{jl} y_j + \mu'_l,$
  for $l = t+1, \dots, m$ and unique $\alpha'_{jkl}, \beta'_{jkl}, \gamma'_{ijl}, \delta'_{il}, \nu'_{jl}, \mu'_l$, if uninteresting exceptional cases over $\mathbb{F}_2$ are excluded.
- $\alpha'_{jkl}, \beta'_{jkl}, \gamma'_{ijl}, \delta'_{il}, \nu'_{jl}, \mu'_l$ can be efficiently computed with Gaussian elimination.
- Note, that these coefficients almost yield $U'$ and $G'_U$ except for $\sum_{1 \le i \le j \le n-t} \gamma'_{ijl} y_i y_j$.

# Step 3: Retrieve $U'$ and $G'_U$ from the lower Part of $G'$

- $$\sum_{1 \le i \le j \le n-t} \gamma'_{ijl} y_i y_j$$

  can be transformed into OV polynomials with $\#V = s$ by another transformation

  $$C'^{-1} = \begin{pmatrix} E_t & 0 \\ 0 & \widetilde{C}^{-1} \end{pmatrix} \in M(n \times n, \mathbb{F}_q),$$

  where $E_t$ is the $t \times t$ identity matrix.
- For practical parameters of Pesto, e.g. $s = 2$, this is most efficiently done by a simple probabilistic search algorithm for isotropic vectors, which recovers the oil space and finally the whole OV polynomial.

# Finally: The equivalent key

Composing $C'^{-1}$ with $G'$ yields $m - t$

$$
\begin{array}{ll}
U'_l = & G'_{Ul} = \\
\sum_{1\le j\le k\le t} \alpha''_{jkl} x_j x_k + & \sum_{1\le j\le k\le t} \alpha''_{jkl} g''_j g''_k + \\
\sum_{j\in\{1,\dots,t\},k\in\{1,\dots,n-t\}} \beta''_{jkl} x_j y_k + & \sum_{j\in\{1,\dots,t\},k\in\{1,\dots,n-t\}} \beta''_{jkl} g''_j y_k + \\
\sum_{1\le i\le j\le s} \gamma''_{ijl} y_i y_j + & \sum_{1\le i\le j\le s} \gamma''_{ijl} y_i y_j + \\
\sum_{1\le i\le s} y_i \ell_{il}(y_{s+1},\dots,y_{n-t}) & \sum_{1\le i\le s} y_i \\
\ell_{il}(y_{s+1},\dots,y_{n-t}) & \\
\sum_{i=1}^{t} \delta''_{il} x_i + & \sum_{i=1}^{t} \delta''_{il} g''_i + \\
 & \\
\sum_{j=1}^{n-t} \nu''_{jl} y_j + \mu''_l & \sum_{j=1}^{n-t} \nu''_{jl} y_j + \mu''_l,
\end{array}
$$

$l = t+1,\dots,m$ and
$G'_{Q_l} = \mathfrak{l}_l(x) - \mathfrak{q}'''_l(y), l = 1,\dots,t.$

- These together with $A'_2 := T'^{-1} C'^{-1}$ (and $A'_1 = Id$) yield the equivalent key.

# Attacking the proposed Parameters

- The designers proposed parameters for signature schemes for NIST I,III and V referring to the security level defined by NIST within the PQC standardization process.

Table: Execution times (Magma, 40-core Xeon @ 2.20GHz, 20 threads)

| **Sec. Level** | $n, m, t, s, q$ | **Equiv. Key** | **Forg./Dec.** |
|---|---|---|---|
| NIST I | $27, 25, 10, 2, 2^6$ | $\approx$ 3.5 min | $<$ 1 min |
| NIST III | $40, 38, 14, 2, 2^6$ | $\approx$ 40.0 min | $\approx$ 2 min |
| NIST V | $57, 55, 20, 2, 2^6$ | $\approx$ 11.0 hrs | $\approx$ 30 min |

- proof-of-concept implementation in Magma available at *doi.org/10.5281/zenodo.21642070*.
- A careful theoretical complexity analysis is given in the paper.

# Conclusion

- **Status of `Pesto`:** We presented an equivalent key recovery attack against `Pesto` and broke all proposed NIST parameters in feasible time.
- **Lessons learned:** Separation of variables as employed in $x - \mathfrak{q}(y)$ again turned out to be bad design decision. Designing practical multivariate cryptosystems of degree $> 2$ is tempting as it seems to be easy to get hard to break systems. Until today it turned out to be an illusion (only acadamic proposals exist, e.g. Ariande Thread by Micario-Rat et al.).
- **Future Work:** As most systems considered to be secure are based on the UOV approach new ideas to design practical schemes in particular of degree $> 2$ might yield a new cornerstone. In other words make the illusion disappear...

# Thank you!
# Any Questions?