# Multivariate-quadratic signatures

## Definitions and basic concepts

Tanja Lange

Eindhoven University of Technology

SAC – Post-quantum cryptography

# Multivariate-quadratic equations

We consider a system of $m$ equations in $n$ variables over $\mathbf{F}_q$.

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(k)} x_i x_j + \sum_{1 \le i \le n} b_i^{(k)} x_i + c^{(k)}$$

with coefficients $a_{i,j}^{(k)}, b_i^{(k)}, c^{(k)} \in \mathbf{F}_q$.

# Multivariate-quadratic equations

We consider a system of $m$ equations in $n$ variables over $\mathbf{F}_q$.

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(k)} x_i x_j + \sum_{1 \le i \le n} b_i^{(k)} x_i + c^{(k)}$$

with coefficients $a_{i,j}^{(k)}, b_i^{(k)}, c^{(k)} \in \mathbf{F}_q$.

## Hard problem:

Given $(y_1, y_2, \ldots, y_m) \in \mathbf{F}_q^m$, find $(x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$ with

$$f_k(x_1, x_2, \ldots, x_n) = y_k \text{ for } 1 \le k \le m$$

if they exist.

# Multivariate-quadratic equations

We consider a system of $m$ equations in $n$ variables over $\mathbf{F}_q$.

$$f_k(x_1, x_2, \ldots, x_n) = \sum_{1 \le i \le j \le n} a_{i,j}^{(k)} x_i x_j + \sum_{1 \le i \le n} b_i^{(k)} x_i + c^{(k)}$$

with coefficients $a_{i,j}^{(k)}, b_i^{(k)}, c^{(k)} \in \mathbf{F}_q$.

## Hard problem:

Given $(y_1, y_2, \ldots, y_m) \in \mathbf{F}_q^m$, find $(x_1, x_2, \ldots, x_n) \in \mathbf{F}_q^n$ with

$$f_k(x_1, x_2, \ldots, x_n) = y_k \text{ for } 1 \le k \le m$$

if they exist.

For systems of *linear* equations (all $a_{i,j}^{(k)} = 0$) this is easy

Code-based crypto and lattice-based crypto add constraints to the solutions or errors to the equations ("noisy linear algebra').

Multivariate systems typically stop with degree 2.
$m(n(n+1)/2 + n + 1) = m(n+1)(n+2)/2$ coefficients is big enough.

# MQ signatures (typical case)

Take $F = (f_1, f_2, \ldots, f_m)$ as public key.

Let $H : \{0,1\}^* \times \{0,1\}^r \to \mathbf{F}_q^m$ be a hash function.

## Signature:

Signature on $M \in \{0,1\}^*$ is $(\mathbf{X}, R)$ with

- $\mathbf{X} = (X_1, X_2, \ldots, X_n) \in \mathbf{F}_q^n$
- $R \in \{0,1\}^r$

satisfying

$$f_k(X_1, X_2, \ldots, X_n) = h_k$$

for all $1 \leq k \leq m$ and $H(M, R) = (h_1, h_2, \ldots, h_m)$.

The inclusion of $R$ is necessary because not every system has a solution.

Notation: using bold face to indicate vectors.

# How to sign?

# How to sign?

There are 3 types of constructions:

- Hidden large field
  Construct the polynomials in $F$ with some secret structure hiding a large finite field $\mathbf{F}_{q^n}$.
  Examples are HFE, HFEv−, GeMSS.
- Oil-and-vinegar construction
  Construct the polynomials in $F$ with some secret structure by adding and removing variables.
  Examples are Rainbow.
- Transformation of identification system
  Use random equations, build an interactive identification scheme around that and then replace challenges by hashes (Fiat-Shamir transform).
  Examples are MQDSS, SOFIA.