# Post-quantum cryptography QIC 891

**Geovandro C. C. F. Pereira**
Institute for Quantum Computing
University of Waterloo

# Agenda

- Multivariate (quadratic) Public Key Cryptosystems (MPKC)
  - Mathematical Problems: the $\mathcal{MQ}$ and $\mathcal{IP}$ problems
  - Building cryptography from the $\mathcal{IP}$ problem
  - The (yet-successful) UOV and Rainbow signature schemes

# Multivariate quadratic public key cryptosystems (MPKC)

## Motivations of MPKC

- Use systems of (non-linear) equations over finite fields.

# Multivariate quadratic public key cryptosystems (MPKC)

## Motivations of MPKC

- Use systems of (non-linear) equations over finite fields.
- Modern math:

> In contrast, the security of RSA-type cryptosystems relies on the complexity of integer factorization and is based on results in number theory developed in the $17^{\text{th}}$ and $18^{\text{th}}$ centuries. Elliptic curve cryptosystems employ the use of mathematics from the $19^{\text{th}}$ century. This quote is actually from Whitfield Diffie at the RSA Europe conference in Paris in 2002. At least Algebraic Geometry, the mathematics that MPKCs use, is developed in the $20^{\text{th}}$ century.

–**Ding, J.** and Yang, B. [D.J., Buchmann, and Dahmen 2009]

# Multivariate quadratic public key cryptosystems (MPKC)

## Motivations of MPKC

- Use systems of (non-linear) equations over finite fields.
- Modern math:

> In contrast, the security of RSA-type cryptosystems relies on the complexity of integer factorization and is based on results in number theory developed in the 17$^{\text{th}}$ and 18$^{\text{th}}$ centuries. Elliptic curve cryptosystems employ the use of mathematics from the 19$^{\text{th}}$ century. This quote is actually from Whitfield Diffie at the RSA Europe conference in Paris in 2002. At least Algebraic Geometry, the mathematics that MPKCs use, is developed in the 20$^{\text{th}}$ century.

–**Ding, J.** and Yang, B. [D.J., Buchmann, and Dahmen 2009]

- Avoid putting all eggs in one basket.

# Multivariate quadratic public key cryptosystems (MPKC)

## Why **quadratic**?

Given a system of cubic (or higher degree) equations

$$x_1\mathbf{x_2}\mathbf{x_3} + 2x_1x_3 - 3\mathbf{x_2^2}\mathbf{x_3} - 7 = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$-x_1x_2 + x_1x_3 + 6\mathbf{x_3^3} - 7 = 0$$

# Multivariate quadratic public key cryptosystems (MPKC)

## Why **quadratic**?

Given a system of cubic (or higher degree) equations

$$x_1\mathbf{x_2x_3} + 2x_1x_3 - 3\mathbf{x_2^2x_3} - 7 = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$-x_1x_2 + x_1x_3 + 6\mathbf{x_3^3} - 7 = 0$$

One can always perform **degree reduction** or **linearization** by introducing new variables ${\color{red}x_4} = \mathbf{x_2x_3}$ and ${\color{blue}x_5} = \mathbf{x_3}^2$

# Multivariate quadratic public key cryptosystems (MPKC)

## Why **quadratic**?

Given a system of cubic (or higher degree) equations

$$x_1\mathbf{x_2x_3} + 2x_1x_3 - 3\mathbf{x_2^2x_3} - 7 = 0$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$-x_1x_2 + x_1x_3 + 6\mathbf{x_3^3} - 7 = 0$$

One can always perform **degree reduction** or **linearization** by introducing new variables $x_4 = \mathbf{x_2x_3}$ and $x_5 = \mathbf{x_3}^2$

$$x_1x_4 + 2x_1x_3 - 3x_2x_4 - 7 = 0$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$-x_1x_2 + x_1x_3 + 6x_3x_5 - 7 = 0$$

# Multivariate quadratic public key cryptosystems (MPKC)

## Why **quadratic**?

Given a system of cubic (or higher degree) equations

$$x_1\mathbf{x_2x_3} + 2x_1x_3 - 3\mathbf{x_2^2x_3} - 7 = 0$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$-x_1x_2 + x_1x_3 + 6\mathbf{x_3^3} - 7 = 0$$

One can always perform **degree reduction** or **linearization** by introducing new variables $x_4 = \mathbf{x_2x_3}$ and $x_5 = \mathbf{x_3}^2$

$$x_1x_4 + 2x_1x_3 - 3x_2x_4 - 7 = 0$$

$$\dots\dots\dots\dots\dots\dots\dots$$

$$-x_1x_2 + x_1x_3 + 6x_3x_5 - 7 = 0$$

- Solve the quadratic system for the new variables and backtrack.

# Multivariate quadratic public key cryptosystems (MPKC)

## Notation

Let $\mathbb{F}_q$ denote a finite field of $q$ elements where $q$ is a prime power.
A generic quadratic map $\mathcal{P} : (\mathbb{F}_q)^n \to \mathbb{F}_q$ can be represented by a quadratic polynomial

$$p(x_1, \cdots, x_n) = \sum_{1 \le i \le j \le n} \alpha_{ij} x_i x_j + \sum_{1 \le i \le n} \beta_i x_i + \gamma$$

where $\alpha_{ij}, \beta_i, \gamma \in \mathbb{F}_q$.

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Notation

- A purely quadratic map $\mathcal{F} : (\mathbb{F})^n \to \mathbb{F}$ can be written as:

$$f(x_1, \cdots, x_n) = \sum_{1 \le i \le j \le n} \alpha_{ij} x_i x_j$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Notation

- A purely quadratic map $\mathcal{F} : (\mathbb{F})^n \rightarrow \mathbb{F}$ can be written as:

$$f(x_1, \cdots, x_n) = \sum_{1 \leq i \leq j \leq n} \alpha_{ij} x_i x_j$$

- A useful (implementation-friendly) matrix representation is generally used:

$$[x_1, \cdots, x_n] \begin{bmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ 0 & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \sum_{1 \leq i \leq j \leq n} \alpha_{ij} x_i x_j$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## $\mathcal{MQ}$ problem

- Given a system of $m$ **random** quadratic equations in $n$ variables over a finite field $\mathbb{F}_q$ ($q$ is a prime power) of any characteristic:

$$\begin{cases} p_1(x_1, \cdots, x_n) = y_1 \\ p_2(x_1, \cdots, x_n) = y_2 \\ \cdots \cdots \cdots \cdots = \cdots \\ p_m(x_1, \cdots, x_n) = y_m \end{cases}$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## $\mathcal{MQ}$ problem

- Given a system of $m$ **random** quadratic equations in $n$ variables over a finite field $\mathbb{F}_q$ ($q$ is a prime power) of any characteristic:

$$\begin{cases} p_1(x_1, \cdots, x_n) = y_1 \\ p_2(x_1, \cdots, x_n) = y_2 \\ \cdots \cdots \cdots \cdots = \cdots \\ p_m(x_1, \cdots, x_n) = y_m \end{cases}$$

finding a solution $\mathbf{x} \in (\mathbb{F}_q)^n$ is **NP-complete** (a reduction from the 3-SAT to the $\mathcal{MQ}$ problem exists [Patarin and Goubin 1997]).

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## $\mathcal{MQ}$ problem

- Given a system of $m$ **random** quadratic equations in $n$ variables over a finite field $\mathbb{F}_q$ ($q$ is a prime power) of any characteristic:

$$\begin{cases} p_1(x_1, \cdots, x_n) = y_1 \\ p_2(x_1, \cdots, x_n) = y_2 \\ \cdots \cdots \cdots \cdots = \cdots \\ p_m(x_1, \cdots, x_n) = y_m \end{cases}$$

  finding a solution $\mathbf{x} \in (\mathbb{F}_q)^n$ is **NP-complete** (a reduction from the 3-SAT to the $\mathcal{MQ}$ problem exists [Patarin and Goubin 1997]).
- For the **average case**, it is believed to be hard due to experiments although no reduction exist.

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## (Generic) Encryption

- Public key is the system of equations:

$$P = \{p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)\}$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## (Generic) Encryption

- Public key is the system of equations:

$$P = \{p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)\}$$

- To encrypt a document $d_1, \cdots, d_n \in (\mathbb{F}_q)^n$, evaluate

$$(c_1, \cdots, c_m) = (p_1(d_1, \cdots, d_n), \cdots, p_m(d_1, \cdots, d_n))$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## (Generic) Encryption

- Public key is the system of equations:

$$P = \{p_1(x_1, \cdots, x_n), \cdots, p_m(x_1, \cdots, x_n)\}$$

- To encrypt a document $d_1, \cdots, d_n \in (\mathbb{F}_q)^n$, evaluate

$$(c_1, \cdots, c_m) = (p_1(d_1, \cdots, d_n), \cdots, p_m(d_1, \cdots, d_n))$$

- To decrypt, a trapdoor is needed to solve the system for **x**:

$$x_1, \cdots, x_n = P^{-1}(c_1, \cdots, c_m)$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## (Generic) Signature

- Public key is also:

$$P = \{p_1(x_1, \dots, x_n), \cdots, p_m(x_1, \dots, x_n)\}$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## (Generic) Signature

- Public key is also:

$$P = \{p_1(x_1, \ldots, x_n), \cdots, p_m(x_1, \ldots, x_n)\}$$

- Private key: a trapdoor to invert $P$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## (Generic) Signature

- Public key is also:

$$P = \{p_1(x_1, \ldots, x_n), \cdots, p_m(x_1, \ldots, x_n)\}$$

- Private key: a trapdoor to invert $P$
- To sign a document $D \in \{0,1\}^*$, compute the hash $h_1, \ldots, h_m := H(D) \in (\mathbb{F}_q)^m$ solve for $\mathbf{x}$ to get a signature $\sigma$

$$\sigma := (x_1, \ldots, x_n) = P^{-1}(h_1, \ldots, h_m)$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## (Generic) Signature

- Public key is also:

$$P = \{p_1(x_1, \ldots, x_n), \cdots, p_m(x_1, \ldots, x_n)\}$$

- Private key: a trapdoor to invert $P$
- To sign a document $D \in \{0, 1\}^*$, compute the hash $h_1, \ldots, h_m := H(D) \in (\mathbb{F}_q)^m$ solve for $\mathbf{x}$ to get a signature $\sigma$

$$\sigma := (x_1, \ldots, x_n) = P^{-1}(h_1, \ldots, h_m)$$

- To verify $\sigma$, recompute $\{h_1, \cdots, h_m\} \leftarrow H(D)$ and check

$$p_i(\sigma) \stackrel{?}{=} h_i, \quad 1 \leq i \leq m$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map

# Multivariate quadratic Public Key Cryptosystems (MPKC)

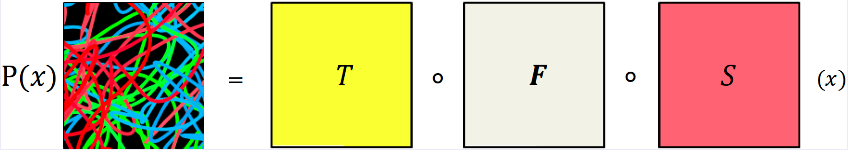
## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map
- The public key is set to $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

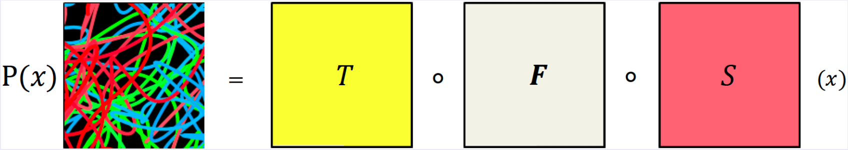
- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map
- The public key is set to $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$



# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map
- The public key is set to $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$

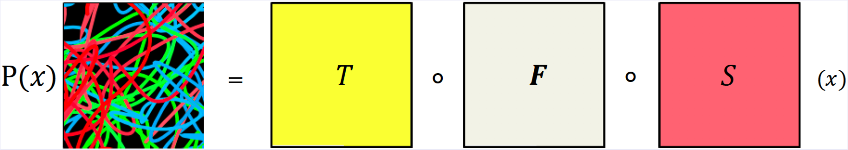



- $\mathcal{P}$ is random-looking and believed to be hard to invert.

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map
- The public key is set to $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$

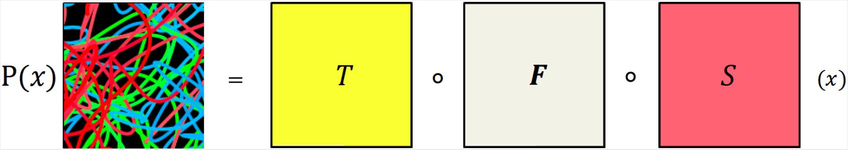



- $\mathcal{P}$ is random-looking and believed to be hard to invert.
  - $\mathcal{S}$ scrambles the variables

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map
- The public key is set to $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$

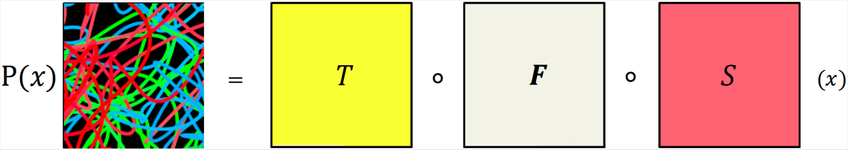



- $\mathcal{P}$ is random-looking and believed to be hard to invert.
  - $\mathcal{S}$ scrambles the variables
  - $\mathcal{F}$ applies $m$ quadratic polynomials in $n$ variables

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map
- The public key is set to $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$

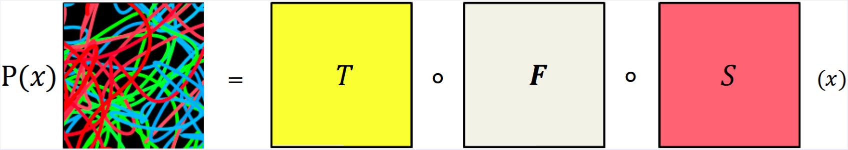



- $\mathcal{P}$ is random-looking and believed to be hard to invert.
  - $\mathcal{S}$ scrambles the variables
  - $\mathcal{F}$ applies $m$ quadratic polynomials in $n$ variables
  - $\mathcal{T}$ mixes the polynomials

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## General **Trapdoor** construction

- Let $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ and $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ be two invertible linear maps
- Let $\mathcal{F} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ an invertible quadratic (central) map
- The public key is set to $\mathcal{P} := \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$




- $\mathcal{P}$ is random-looking and believed to be hard to invert.
  - $\mathcal{S}$ scrambles the variables
  - $\mathcal{F}$ applies $m$ quadratic polynomials in $n$ variables
  - $\mathcal{T}$ mixes the polynomials
- Inverting $\mathcal{P}$ is related to the Isomorphism of Polynomials problem.

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Isomorphism of Polynomials Problem ($\mathcal{IP}$-**problem**)

Two systems of equations/polynomials $\mathcal{U}, \mathcal{V} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ are called **isomorphic** (up to linear transforms) iif $\exists$ linear maps $\mathcal{L}_1, \mathcal{L}_2$ s.t.

$$\mathcal{U} = \mathcal{L}_1 \circ \mathcal{V} \circ \mathcal{L}_2$$

$\mathcal{IP}$ is not **NP-Complete** [Patarin, Goubin, and Courtois 1998]!

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Isomorphism of Polynomials Problem ($\mathcal{IP}$-**problem**)

Two systems of equations/polynomials $\mathcal{U}, \mathcal{V} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ are called **isomorphic** (up to linear transforms) iif $\exists$ linear maps $\mathcal{L}_1, \mathcal{L}_2$ s.t.

$$\mathcal{U} = \mathcal{L}_1 \circ \mathcal{V} \circ \mathcal{L}_2$$

$\mathcal{IP}$ is not **NP-Complete** [Patarin, Goubin, and Courtois 1998]!

- In practice, the security of MPKC rely on a related problem that captures the concept of equivalent keys:

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Isomorphism of Polynomials Problem ($\mathcal{IP}$-**problem**)

Two systems of equations/polynomials $\mathcal{U}, \mathcal{V} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ are called **isomorphic** (up to linear transforms) iif $\exists$ linear maps $\mathcal{L}_1, \mathcal{L}_2$ s.t.

$$\mathcal{U} = \mathcal{L}_1 \circ \mathcal{V} \circ \mathcal{L}_2$$

$\mathcal{IP}$ is not **NP-Complete** [Patarin, Goubin, and Courtois 1998]!

- In practice, the security of MPKC rely on a related problem that captures the concept of equivalent keys:

## Extended Isomorphism of Polynomials (**EIP-problem**)

Given a public key $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$, find a map $\overline{\mathcal{F}}$ isomorphic to $\mathcal{P}$, i.e.,

$$\mathcal{P} = \overline{\mathcal{T}} \circ \overline{\mathcal{F}} \circ \overline{\mathcal{S}}$$

for some invertible $\overline{\mathcal{T}}$ and $\overline{\mathcal{S}}$ s.t. $\overline{\mathcal{F}}$ inherits the trapdoor structure of $\mathcal{F}$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Public key sizes

- Usually, public keys $P$ consist of $m$ quadratic polynomials of shape:

$$p_i(x) = [x_1, \cdots, x_n] \begin{bmatrix} \alpha_{11}^{(i)} & \alpha_{12}^{(i)} & \dots & \alpha_{1n}^{(i)} \\ 0 & \alpha_{22}^{(i)} & \dots & \alpha_{2n}^{(i)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{nn}^{(i)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Public key sizes

- Usually, public keys $P$ consist of $m$ quadratic polynomials of shape:

$$p_i(x) = [x_1, \cdots, x_n] \begin{bmatrix} \alpha_{11}^{(i)} & \alpha_{12}^{(i)} & \ldots & \alpha_{1n}^{(i)} \\ 0 & \alpha_{22}^{(i)} & \ldots & \alpha_{2n}^{(i)} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \alpha_{nn}^{(i)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

- Thus, the number of elements is

$$mn(n+1)/2 \stackrel{m \approx n}{=} O(n^3)$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Public key sizes

- Usually, public keys $P$ consist of $m$ quadratic polynomials of shape:

$$p_i(x) = [x_1, \cdots, x_n] \begin{bmatrix} \alpha_{11}^{(i)} & \alpha_{12}^{(i)} & \dots & \alpha_{1n}^{(i)} \\ 0 & \alpha_{22}^{(i)} & \dots & \alpha_{2n}^{(i)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{nn}^{(i)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

- Thus, the number of elements is

$$mn(n+1)/2 \overset{m \approx n}{=} O(n^3)$$

- In general, for degree $d$ polynomials, the size is $O(n^{d+1})$.

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Public key sizes

- Usually, public keys $P$ consist of $m$ quadratic polynomials of shape:

$$p_i(x) = [x_1, \cdots, x_n] \begin{bmatrix} \alpha_{11}^{(i)} & \alpha_{12}^{(i)} & \dots & \alpha_{1n}^{(i)} \\ 0 & \alpha_{22}^{(i)} & \dots & \alpha_{2n}^{(i)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{nn}^{(i)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

- Thus, the number of elements is

$$mn(n+1)/2 \overset{m \approx n}{=} O(n^3)$$

- In general, for degree $d$ polynomials, the size is $O(n^{d+1})$.
  - $\Rightarrow$ not a good idea to have high degree polynomials.

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Public key sizes

- Usually, public keys $P$ consist of $m$ quadratic polynomials of shape:

$$p_i(x) = [x_1, \cdots, x_n] \begin{bmatrix} \alpha_{11}^{(i)} & \alpha_{12}^{(i)} & \dots & \alpha_{1n}^{(i)} \\ 0 & \alpha_{22}^{(i)} & \dots & \alpha_{2n}^{(i)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \alpha_{nn}^{(i)} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

- Thus, the number of elements is

$$mn(n+1)/2 \overset{m \approx n}{=} O(n^3)$$

- In general, for degree $d$ polynomials, the size is $O(n^{d+1})$.
  - $\Rightarrow$ not a good idea to have high degree polynomials.
  - Stick to $d = 2$.

## Main attacks

- **Direct**: try to solve the public system (invert the quadratic map).

## Main attacks

- **Direct**: try to solve the public system (invert the quadratic map).
  - Encryption: given the ciphertext $c \in \mathbb{F}_q^m$, solve

$$\mathcal{P}(\mathbf{x}) = c$$

for the message $x \in \mathbb{F}_q^n$.

## Main attacks

- **Direct**: try to solve the public system (invert the quadratic map).
  - Encryption: given the ciphertext $c \in \mathbb{F}_q^m$, solve
    $$\mathcal{P}(\mathbf{x}) = c$$
    for the message $x \in \mathbb{F}_q^n$.
  - Signature: given the hash $H(M) = h \in \mathbb{F}_q^m$ solve
    $$\mathcal{P}(\mathbf{x}) = h$$
    for the signature $x \in \mathbb{F}_q^n$.

## Main attacks

- **Direct**: try to solve the public system (invert the quadratic map).
  - Encryption: given the ciphertext $c \in \mathbb{F}_q^m$, solve

    $$\mathcal{P}(\mathbf{x}) = c$$

    for the message $x \in \mathbb{F}_q^n$.
  - Signature: given the hash $H(M) = h \in \mathbb{F}_q^m$ solve

    $$\mathcal{P}(\mathbf{x}) = h$$

    for the signature $x \in \mathbb{F}_q^n$.
  - Best time complexity is exponential when $m \approx n$

## Main attacks

- **Direct**: try to solve the public system (invert the quadratic map).
  - Encryption: given the ciphertext $c \in \mathbb{F}_q^m$, solve
  $$\mathcal{P}(\mathbf{x}) = c$$
  for the message $x \in \mathbb{F}_q^n$.
  - Signature: given the hash $H(M) = h \in \mathbb{F}_q^m$ solve
  $$\mathcal{P}(\mathbf{x}) = h$$
  for the signature $x \in \mathbb{F}_q^n$.
  - Best time complexity is exponential when $m \approx n$
  - Gröbner bases complexity $f(q, m, n)$:
  $$f(q, m, n) = O\left(m \cdot \binom{n + d_{reg} - 1}{d_{reg}}^{\omega}\right)$$
  where $d_{reg}$ is degree of regularity of the system and $2 < \omega \leq 3$.

(cont. $\cdots$)

- **Minrank** attack: find a low rank quadratic map.

### MinRank

Given a set of $m$ matrices $M_i$, find a nontrivial solution $a_1, \cdots a_m$ s.t.

$$\sum_{i=1}^{m} a_i M_i$$

is of minimum rank.

Finding a low rank matrix implies that we have less independent equations $\Rightarrow$ more variables per equation can make the system easier to solve.

# Multivariate quadratic Public Key Cryptosystems (MPKC)

**Encryption**: Requires $\mathbf{m} \geq \mathbf{n}$

- To encrypt a document $\mathbf{d} \in (\mathbb{F}_q)^n$, evaluate

$$\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}_q^m$$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

**Encryption**: Requires $\mathbf{m} \geq \mathbf{n}$

- To encrypt a document $\mathbf{d} \in (\mathbb{F}_q)^n$, evaluate

$$\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}_q^m$$

- To decrypt, compute

# Multivariate quadratic Public Key Cryptosystems (MPKC)

**Encryption**: Requires $\mathbf{m} \geq \mathbf{n}$

- To encrypt a document $\mathbf{d} \in (\mathbb{F}_q)^n$, evaluate

$$\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}_q^m$$

- To decrypt, compute
  - $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{c}) \in \mathbb{F}_q^m$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

**Encryption**: Requires $\mathbf{m} \geq \mathbf{n}$

- To encrypt a document $\mathbf{d} \in (\mathbb{F}_q)^n$, evaluate

$$\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}_q^m$$

- To decrypt, compute
  - $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{c}) \in \mathbb{F}_q^m$
  - $\mathbf{w} = \mathcal{F}^{-1}(\mathbf{x})$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

**Encryption**: Requires $\mathbf{m} \geq \mathbf{n}$

- To encrypt a document $\mathbf{d} \in (\mathbb{F}_q)^n$, evaluate

$$\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}_q^m$$

- To decrypt, compute
  - $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{c}) \in \mathbb{F}_q^m$
  - $\mathbf{w} = \mathcal{F}^{-1}(\mathbf{x})$
  - $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{w})$

# Multivariate quadratic Public Key Cryptosystems (MPKC)

**Encryption**: Requires $\mathbf{m} \geq \mathbf{n}$

- To encrypt a document $\mathbf{d} \in (\mathbb{F}_q)^n$, evaluate

$$\mathbf{c} = \mathcal{P}(\mathbf{d}) \in \mathbb{F}_q^m$$

- To decrypt, compute
  - $\mathbf{x} = \mathcal{T}^{-1}(\mathbf{c}) \in \mathbb{F}_q^m$
  - $\mathbf{w} = \mathcal{F}^{-1}(\mathbf{x})$
  - $\mathbf{z} = \mathcal{S}^{-1}(\mathbf{w})$
- If $m \geq n$ (not undetermined) then we ensure that $\mathcal{F}$ is more or less injective and decryption is not mapped to many different plaintexts.

## **Encryption**: The (MI) Matsumoto and Imai 1988 **trapdoor**

- MI central map $\mathcal{F} : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$ is defined as

$$\mathcal{F} = \phi \circ \overline{\mathcal{F}} \circ \phi^{-1}$$

## **Encryption**: The (MI) Matsumoto and Imai 1988 **trapdoor**

- MI central map $\mathcal{F} : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$ is defined as

$$\mathcal{F} = \phi \circ \overline{\mathcal{F}} \circ \phi^{-1}$$

where $\phi : \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n$ is a coefficient-wise bijection given by

$$a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \mapsto (a_{n-1}, \cdots, a_0)$$

## **Encryption**: The (MI) Matsumoto and Imai 1988 **trapdoor**

- MI central map $\mathcal{F} : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$ is defined as

$$\mathcal{F} = \phi \circ \overline{\mathcal{F}} \circ \phi^{-1}$$

where $\phi : \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n$ is a coefficient-wise bijection given by

$$a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \mapsto (a_{n-1}, \cdots, a_0)$$

with $a_i \in \mathbb{F}_q$ and $\overline{\mathcal{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is a quadratic transform

$$\overline{\mathcal{F}} : X \mapsto X^{q^\theta + 1}$$

## **Encryption**: The (MI) Matsumoto and Imai 1988 **trapdoor**

- MI central map $\mathcal{F} : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$ is defined as

$$\mathcal{F} = \phi \circ \overline{\mathcal{F}} \circ \phi^{-1}$$

where $\phi : \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n$ is a coefficient-wise bijection given by

$$a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \mapsto (a_{n-1}, \cdots, a_0)$$

with $a_i \in \mathbb{F}_q$ and $\overline{\mathcal{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is a quadratic transform

$$\overline{\mathcal{F}} : X \mapsto X^{q^\theta + 1}$$

- Notice that $X^{q^\theta+1}$ is a quadratic transformation since $q^\theta$ is linear ($q^\theta$-Frobenius).

## **Encryption**: The (MI) Matsumoto and Imai 1988 **trapdoor**

- MI central map $\mathcal{F} : (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n$ is defined as

$$\mathcal{F} = \phi \circ \overline{\mathcal{F}} \circ \phi^{-1}$$

where $\phi : \mathbb{F}_{q^n} \to (\mathbb{F}_q)^n$ is a coefficient-wise bijection given by

$$a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \mapsto (a_{n-1}, \cdots, a_0)$$

with $a_i \in \mathbb{F}_q$ and $\overline{\mathcal{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ is a quadratic transform

$$\overline{\mathcal{F}} : X \mapsto X^{q^\theta + 1}$$

- Notice that $X^{q^\theta+1}$ is a quadratic transformation since $q^\theta$ is linear ($q^\theta$-Frobenius).
- The quadratic transformation takes place in the big "hidden field" $\mathbb{F}_{q^n}$ instead of the vector space over the smaller field $(\mathbb{F}_q)^n$.

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Notice that for the quadratic map

$$\overline{\mathcal{F}} : X \mapsto X^{q^\theta+1}$$

to be invertible, ones has to take $q^\theta + 1$-th roots and thus $q^\theta + 1 \in \mathbb{F}_{q^n}$ must invertible

$$(X^{q^\theta+1})^{(q^\theta+1)^{-1}} = X.$$

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Notice that for the quadratic map

$$\overline{\mathcal{F}} : X \mapsto X^{q^\theta+1}$$

to be invertible, ones has to take $q^\theta + 1$-th roots and thus $q^\theta + 1 \in \mathbb{F}_{q^n}$ must invertible

$$(X^{q^\theta+1})^{(q^\theta+1)^{-1}} = X.$$

- The necessary condition for multiplicative inverses in $\mathbb{F}^*_{q^n}$ is

$$GCD(q^\theta + 1, q^n - 1) = 1$$

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Notice that for the quadratic map

$$\overline{\mathcal{F}} : X \mapsto X^{q^\theta + 1}$$

to be invertible, ones has to take $q^\theta + 1$-th roots and thus $q^\theta + 1 \in \mathbb{F}_{q^n}$ must invertible

$$(X^{q^\theta+1})^{(q^\theta+1)^{-1}} = X.$$

- The necessary condition for multiplicative inverses in $\mathbb{F}_{q^n}^*$ is

$$GCD(q^\theta + 1, q^n - 1) = 1$$

- Thus, the quadratic map can be made invertible. The keygen, encryption and decryption for MI can be done as explained before.

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Later, the MI encryption was shown to be insecure using linearization [Patarin 1995].

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Later, the MI encryption was shown to be insecure using linearization [Patarin 1995].
- Some variants were introduced as attempts to recover security.

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Later, the MI encryption was shown to be insecure using linearization [Patarin 1995].
- Some variants were introduced as attempts to recover security.
  - 2000, Patarin suggests **Hidden Field Equations (HFE)** encryption with a slightly modified trapdoor with $\overline{\mathcal{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ redefined to:

$$X \mapsto \sum_{0 \leq i,j \leq d} \mathcal{A}_{ij} X^{q^i + q^j} + \sum_k \mathcal{B}_k X^{q^k} + \gamma$$

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Later, the MI encryption was shown to be insecure using linearization [Patarin 1995].
- Some variants were introduced as attempts to recover security.
  - 2000, Patarin suggests **Hidden Field Equations (HFE)** encryption with a slightly modified trapdoor with $\overline{\mathcal{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ redefined to:

$$X \mapsto \sum_{0 \le i,j \le d} \mathcal{A}_{ij} X^{q^i + q^j} + \sum_k \mathcal{B}_k X^{q^k} + \gamma$$

  - Later, Kipnis and Shamir 1999 showed that degree $d$ cannot be too small otherwise minrank + linearization attacks apply.

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Later, the MI encryption was shown to be insecure using linearization [Patarin 1995].
- Some variants were introduced as attempts to recover security.
  - 2000, Patarin suggests **Hidden Field Equations (HFE)** encryption with a slightly modified trapdoor with $\overline{\mathcal{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ redefined to:

$$X \mapsto \sum_{0 \le i,j \le d} \mathcal{A}_{ij} X^{q^i + q^j} + \sum_k \mathcal{B}_k X^{q^k} + \gamma$$

  - Later, Kipnis and Shamir 1999 showed that degree $d$ cannot be too small otherwise minrank + linearization attacks apply.
  - But if $d$ is increased decryption becomes too slow.

(cont. $\cdots$)

## **Encryption**: The Matsumoto-Imai'88 **trapdoor**

- Later, the MI encryption was shown to be insecure using linearization [Patarin 1995].
- Some variants were introduced as attempts to recover security.
  - 2000, Patarin suggests **Hidden Field Equations (HFE)** encryption with a slightly modified trapdoor with $\overline{\mathcal{F}} : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ redefined to:

$$X \mapsto \sum_{0 \le i,j \le d} \mathcal{A}_{ij} X^{q^i + q^j} + \sum_k \mathcal{B}_k X^{q^k} + \gamma$$

  - Later, Kipnis and Shamir 1999 showed that degree $d$ cannot be too small otherwise minrank + linearization attacks apply.
  - But if $d$ is increased decryption becomes too slow.
  - Finally, Faugere and Joux 2003 improved the attacks using **F4** algorithm which made the system impractical.

# Multivariate quadratic public key cryptosystems (MPKC)

**Signature**: The UOV **trapdoor**, Kipnis, Patarin, and Goubin 1999

- Goal: $\mathcal{F}^{-1}(h) = (x_1, \cdots, x_n)$

# Multivariate quadratic public key cryptosystems (MPKC)

**Signature**: The UOV **trapdoor**, Kipnis, Patarin, and Goubin 1999

- Goal: $\mathcal{F}^{-1}(h) = (x_1, \cdots, x_n)$
- Let $o, v \in \mathbb{N}$, define $n = o + v$ and $m = o$

# Multivariate quadratic public key cryptosystems (MPKC)

**Signature**: The UOV **trapdoor**, Kipnis, Patarin, and Goubin 1999

- Goal: $\mathcal{F}^{-1}(h) = (x_1, \cdots, x_n)$
- Let $o, v \in \mathbb{N}$, define $n = o + v$ and $m = o$
- Write the quadratic polynomials as follows:

$$p(x_1, \cdots, x_n) = \underbrace{\sum_{i=1}^{v}\sum_{j=i}^{v} \alpha_{ij} x_i x_j}_{v \times v \text{ terms}} + \underbrace{\sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{ij} x_i x_j}_{v \times o \text{ terms}} + \sum_{i=1}^{n} \gamma_i x_i + \delta$$

where $(x_1, \cdots, x_v)$ are the vinegar variables and $(x_{v+1}, \cdots, x_n)$ are the *oil* variables.

# Multivariate quadratic public key cryptosystems (MPKC)

**Signature**: The UOV **trapdoor**, Kipnis, Patarin, and Goubin 1999

- Goal: $\mathcal{F}^{-1}(h) = (x_1, \cdots, x_n)$
- Let $o, v \in \mathbb{N}$, define $n = o + v$ and $m = o$
- Write the quadratic polynomials as follows:

$$p(x_1, \cdots, x_n) = \underbrace{\sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ij} x_i x_j}_{v \times v \textit{ terms}} + \underbrace{\sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ij} x_i x_j}_{v \times o \textit{ terms}} + \sum_{i=1}^{n} \gamma_i x_i + \delta$$

  where $(x_1, \cdots, x_v)$ are the vinegar variables and $(x_{v+1}, \cdots, x_n)$ are the *oil* variables.

- Notice *oil* variables are **not mixed** with themselves. // Easier to see using matrix notation, or even easier mixing the ingredients!!

# Multivariate quadratic public key cryptosystems (MPKC)

**Signature**: The UOV **trapdoor**, Kipnis, Patarin, and Goubin 1999

- My attempt to implement $\mathcal{F}$ with **olive oil** and **white vinegar**:

# Multivariate quadratic public key cryptosystems (MPKC)

**Signature**: The UOV **trapdoor**, Kipnis, Patarin, and Goubin 1999

- My attempt to implement $\mathcal{F}$ with **olive oil** and **white vinegar**:

# Multivariate quadratic public key cryptosystems (MPKC)

## How to invert the UOV trapdoor

- To invert guess at random the vinegars $(x_1, \cdots, x_v) \in_R (\mathbb{F}_q)^v$

# Multivariate quadratic public key cryptosystems (MPKC)

## How to invert the UOV trapdoor

- To invert guess at random the vinegars $(x_1, \cdots, x_v) \in_R (\mathbb{F}_q)^v$
- For $1 \leq k \leq o$

$$p_k(x_1, \cdots, x_n) = \underbrace{\sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ij}^{(k)} x_i x_j}_{v \times v \textit{ terms}} + \underbrace{\sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ij}^{(k)} x_i x_j}_{v \times o \textit{ terms}} + \sum_{i=1}^{n} \gamma_i x_i^{(k)}$$

which is a linear system of equations in the *oils*.

# Multivariate quadratic public key cryptosystems (MPKC)

## How to invert the UOV trapdoor

- To invert guess at random the vinegars $(x_1, \cdots, x_v) \in_R (\mathbb{F}_q)^v$
- For $1 \leq k \leq o$

$$p_k(x_1, \cdots, x_n) = \underbrace{\sum_{i=1}^{v} \sum_{j=i}^{v} \alpha_{ij}^{(k)} x_i x_j}_{v \times v \text{ terms}} + \underbrace{\sum_{i=1}^{v} \sum_{j=v+1}^{n} \beta_{ij}^{(k)} x_i x_j}_{v \times o \text{ terms}} + \sum_{i=1}^{n} \gamma_i x_i^{(k)}$$

  which is a linear system of equations in the *oils*.

- Solve the system in at most $O(o^3)$ using Gaussian elimination to find $(x_{v+1}, \cdots, x_n)$.

# Multivariate quadratic public key cryptosystems (MPKC)

## How to invert the UOV trapdoor

- To invert guess at random the vinegars $(x_1, \cdots, x_v) \in_R (\mathbb{F}_q)^v$
- For $1 \leq k \leq o$

$$p_k(x_1, \cdots, x_n) = \underbrace{\sum_{i=1}^{v}\sum_{j=i}^{v} \alpha_{ij}^{(k)} x_i x_j}_{v \times v \ terms} + \underbrace{\sum_{i=1}^{v}\sum_{j=v+1}^{n} \beta_{ij}^{(k)} x_i x_j}_{v \times o \ terms} + \sum_{i=1}^{n} \gamma_i x_i^{(k)}$$

which is a linear system of equations in the *oils*.

- Solve the system in at most $O(o^3)$ using Gaussian elimination to find $(x_{v+1}, \cdots, x_n)$.
- If the system has no solution, guess new vinegars $(x_1, \cdots, x_v)$

## How to invert the UOV trapdoor

- Remaining system $o \times o$ has a solution with very high probability

$$\frac{\left(\prod_{i=0}^{o-1}(q^o - q^i)\right)}{q^{o^2}}$$

## How to invert the UOV trapdoor

- Remaining system $o \times o$ has a solution with very high probability

$$\frac{\left(\prod_{i=0}^{o-1}(q^o - q^i)\right)}{q^{o^2}}$$

- Security note: in practice pick $\mathbf{v} \approx \mathbf{2o}$.

## How to invert the UOV trapdoor

- Remaining system $o \times o$ has a solution with very high probability

$$\frac{\left(\prod_{i=0}^{o-1}(q^o - q^i)\right)}{q^{o^2}}$$

- Security note: in practice pick $\mathbf{v} \approx \mathbf{2o}$.
  - The case where $o \approx v$ (balanced oil and vinegar) was broken by Kipnis and Shamir 1998.

## How to invert the UOV trapdoor

- Remaining system $o \times o$ has a solution with very high probability

$$\frac{\left(\prod_{i=0}^{o-1}(q^o - q^i)\right)}{q^{o^2}}$$

- Security note: in practice pick $\mathbf{v} \approx \mathbf{2o}$.
  - The case where $o \approx v$ (balanced oil and vinegar) was broken by Kipnis and Shamir 1998.
  - For $v > o$ the complexity of the attack becomes $O(q^{v-o} \cdot o^4)$

# UOV parameter sizes [from A. Petzoldt, 2017]

| security level (bit) | scheme | public key size (kB) | private key size (kB) | hash size (bit) | signature (bit) |
|---|---|---|---|---|---|
| 80 | UOV(GF(16),40,80) | 144.2 | 135.2 | 160 | 480 |
| | UOV(GF(256),27,54) | 89.8 | 86.2 | 216 | 648 |
| 100 | UOV(GF(16),50,100) | 280.2 | 260.1 | 200 | 600 |
| | UOV(GF(256), 34,68) | 177.8 | 168.3 | 272 | 816 |
| 128 | UOV(GF(16),64,128) | 585.1 | 538.1 | 256 | 768 |
| | UOV(GF(256),45,90) | 409.4 | 381.8 | 360 | 1,080 |
| 192 | UOV(GF(16),96,192) | 1,964.3 | 1,786.7 | 384 | 1,152 |
| | UOV(GF(256),69,138) | 1,464.6 | 1,344.0 | 552 | 1,656 |
| 256 | UOV(GF(16),128,256) | 4,644.1 | 4,200.3 | 512 | 1,536 |
| | UOV(GF(256),93,186) | 3,572.9 | 3,252.2 | 744 | 2,232 |

## Summary of UOV

- UOV was proposed in 1999 and has not suffured major attacks.
- Faster than ECDSA signature. $2-4\times$ faster to sign, $10-20\times$ faster for verifying.
- Signature sizes are less than $1KiB$
- Public keys are large: tens or hundreds $KiB$
    - Potential topic for research!

# Multivariate quadratic Public Key Cryptosystems (MPKC)

## Rainbow signature

- Proposed by Ding and Schmidt 2005.
- It is a generalization of UOV.
- Idea: split private quadratic maps into layers.
  - Solve more but smaller systems of equations.
  - *Vinegars* for the next layer will be the the *vinegars* + *oils* from the previous one.

# Multivariate quadratic public key cryptosystems (MPKC)

## Rainbow signature

- Assume integer chain $0 < v_1 < \cdots < v_u < v_{u+1} = n$

# Multivariate quadratic public key cryptosystems (MPKC)

## Rainbow signature

- Assume integer chain $0 < v_1 < \cdots < v_u < v_{u+1} = n$
- Let $V_i := \{1, \cdots, v_i\}$ and $O_i := \{v_i + 1, \cdots, v_{i+1}\}$, be sets and $o_i := v_{i+1} - v_i$ the numbers of oils.

# Multivariate quadratic public key cryptosystems (MPKC)

## Rainbow signature

- Assume integer chain $0 < v_1 < \cdots < v_u < v_{u+1} = n$
- Let $V_i := \{1, \cdots, v_i\}$ and $O_i := \{v_i + 1, \cdots, v_{i+1}\}$, be sets and $o_i := v_{i+1} - v_i$ the numbers of oils.
- Central map $\mathcal{F}$ consists of $m = n - v_1$ polynomials $f^{v_1+1}, \cdots, f^n$

$$f^{(k)} = \sum_{i,j \in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} + \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i$$

where $\ell$ is the only integer s.t. $k \in O_\ell$.

# Multivariate quadratic public key cryptosystems (MPKC)

## Rainbow signature

- Assume integer chain $0 < v_1 < \cdots < v_u < v_{u+1} = n$
- Let $V_i := \{1, \cdots, v_i\}$ and $O_i := \{v_i + 1, \cdots, v_{i+1}\}$, be sets and $o_i := v_{i+1} - v_i$ the numbers of oils.
- Central map $\mathcal{F}$ consists of $m = n - v_1$ polynomials $f^{v_1+1}, \cdots, f^n$

$$f^{(k)} = \sum_{i,j \in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} + \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i$$

  where $\ell$ is the only integer s.t. $k \in O_\ell$.
- Choose invertible linear maps $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$

# Multivariate quadratic public key cryptosystems (MPKC)

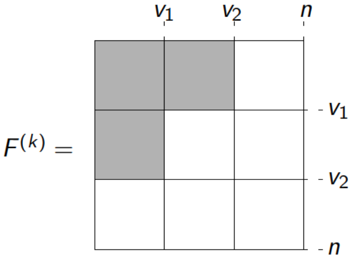
## Rainbow signature

- Assume integer chain $0 < v_1 < \cdots < v_u < v_{u+1} = n$
- Let $V_i := \{1, \cdots, v_i\}$ and $O_i := \{v_i + 1, \cdots, v_{i+1}\}$, be sets and $o_i := v_{i+1} - v_i$ the numbers of oils.
- Central map $\mathcal{F}$ consists of $m = n - v_1$ polynomials $f^{v_1+1}, \cdots, f^n$

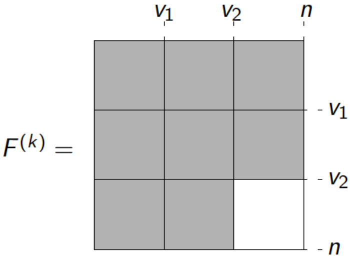
$$f^{(k)} = \sum_{i,j \in V_\ell} \alpha_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell, j \in O_\ell} + \beta_{ij}^{(k)} x_i x_j + \sum_{i \in V_\ell \cup O_\ell} \gamma_i^{(k)} x_i$$

  where $\ell$ is the only integer s.t. $k \in O_\ell$.
- Choose invertible linear maps $\mathcal{T} : \mathbb{F}_q^m \to \mathbb{F}_q^m$ and $\mathcal{S} : \mathbb{F}_q^n \to \mathbb{F}_q^n$
- Public key is $\mathcal{P} = \mathcal{T} \circ \mathcal{F} \circ \mathcal{S}$.

# Rainbow central map with 2 layers



$v_1 + 1 \le k \le v_2$



$v_2 + 1 \le k \le n$

- $x_1, \cdots, x_{v_1}, x_{v_1+1}, \cdots, x_{v_1+o_1}$ will be the vinegars $x_1, \cdots, x_{v_2}$ for the second layer.

## Rainbow (2 layers): Toy example [from A. Petzoldt, 2017]

- $\mathbb{F}_7$, $(v_1, o_1, o_2) = (2, 2, 2)$, $m = n - v_1 = 4$
- Central map $\mathcal{F} = (f^{(3)}, f^{(4)}, f^{(5)}, f^{(6)})$ with

$$
\begin{aligned}
f^{(3)} &= x_1^2 + 3x_1x_2 + 5x_1x_3 + 6x_1x_4 + 2x_2^2 + 6x_2x_3 + 4x_2x_4 + 2x_2 + 6x_3 \\
&\quad + 2x_4 + 5 \\
f^{(4)} &= 2x_1^2 + x_1x_2 + x_1x_3 + 3x_1x_4 + 4x_1 + x_2^2 + x_2x_3 + 4x_2x_4 + 6x_2 + x_4 \\
f^{(5)} &= 2x_1^2 + 3x_1x_2 + 3x_1x_3 + 3x_1x_4 + x_1x_5 + 3x_1x_6 + 6x_1 + 4x_2^2 \\
&\quad + x_2x_3 + 4x_2x_4 + x_2x_5 + 3x_2x_6 + 3x_2 + 3x_3x_4 + x_3x_5 + 2x_3x_6 \\
&\quad + 2x_3 + 3x_4x_5 + x_5 + 6x_6 \\
f^{(6)} &= 2x_1^2 + 5x_1x_2 + x_1x_3 + 5x_1x_4 + 5x_1x_6 + 6x_1 + 5x_2^2 + 3x_2x_3 \\
&\quad + 5x_2x_5 + 4x_2x_6 + x_2 + 3x_3^2 + 5x_3x_4 + 4x_3x_5 + 2x_3x_6 + 4x_3 + x_4^2 \\
&\quad + 6x_4x_5 + 3x_4x_6 + 4x_4 + 4x_5 + x_6 + 2
\end{aligned}
$$

- Goal: Compute the preimage $\mathbf{x} \in \mathbb{F}_7^6$ for $\mathbf{y} = (6, 2, 0, 5)$ under $\mathcal{F}$.

# Rainbow: Toy example [from A. Petzoldt, 2017] (cont. $\cdots$)

- Choose random values for the Vinegar variables $x_1$ and $x_2$, e.g. $(x_1, x_2) = (0, 1)$ and substitute them into the polynomials $f^{(3)}, \ldots, f^{(6)}$.

$$\begin{aligned}
\tilde{f}^{(3)} &= 5x_3 + 6x_4 + 2, \tilde{f}^{(4)} = x_3 + 5x_4, \\
\tilde{f}^{(5)} &= 3x_3x_4 + x_3x_5 + 2x_3x_6 + 3x_3 + 3x_4x_5 + 4x_4 + 2x_5 + 2x_6, \\
\tilde{f}^{(6)} &= 3x_3^2 + 5x_3x_4 + 4x_3x_5 + 2x_3x_6 + x_4^2 + 6x_4x_5 + 3x_4x_6 + 4x_4 + 2x_5 + 5x_6 + 1.
\end{aligned}$$

- Set $\tilde{f}^{(3)} = y_1 = 6$ and $\tilde{f}^{(4)} = y_2 = 2$ and solve for $x_3, x_4$ $\Rightarrow (x_3, x_4) = (3, 4)$
- Substitute into $\tilde{f}^{(5)}$ and $\tilde{f}^{(6)}$ $\Rightarrow \tilde{\tilde{f}}^{(5)} = 3x_5 + x_6 + 5, \tilde{\tilde{f}}^{(6)} = 3x_5 + 2x_6 + 1$
- Set $\tilde{\tilde{f}}^{(5)} = y_3 = 0$ and $\tilde{\tilde{f}}^{(6)} = y_4 = 5$, solve for $x_5$ and $x_6$ $\Rightarrow (x_5, x_6) = (0, 2)$

A pre image of $\mathbf{y} = (6, 2, 0, 5)$ is given by $\mathbf{x} = (0, 1, 3, 4, 0, 2)$.

# Rainbow parameter sizes [from A. Petzoldt, 2017]

(cont. $\cdots$)

| security level (bit) | parameters $\mathbb{F}, v_1, o_1, o_2$ | public key size (kB) | private key size (kB) | hash size (bit) | signature (bit) |
|---|---|---|---|---|---|
| 80 | GF(16),17,20,20 | 33.4 | 22.3 | 160 | 228 |
| | GF(256),19,12,13 | 25.3 | 19.3 | 200 | 352 |
| 100 | GF(16),22,25,25 | 65.9 | 43.2 | 200 | 288 |
| | GF(256), 27,16,16 | 57.2 | 44.3 | 256 | 472 |
| 128 | GF(16),28,32,32 | 136.6 | 87.6 | 256 | 368 |
| | GF(256),36,21,22 | 136.0 | 102.5 | 344 | 632 |
| 192 | GF(16),45,48,48 | 475.9 | 301.8 | 384 | 564 |
| | GF(256),58,33,34 | 523.5 | 385.5 | 536 | 1,000 |
| 256 | GF(16),66,64,64 | 1,194.4 | 763.9 | 512 | 776 |
| | GF(256),86,45,46 | 1,415.7 | 1,046.3 | 728 | 1,416 |

# References I


D.J., Bernstein, Johannes Buchmann, and Erik Dahmen (2009).
*Post-quantum cryptography*.
Springer, Berlin, Heidelberg.

Patarin, Jacques and Louis Goubin (1997).
"Trapdoor one-way permutations and multivariate polynomials".

Patarin, Jacques, Louis Goubin, and Nicolas Courtois (1998).
"Improved algorithms for isomorphisms of polynomials".

Matsumoto, Tsutomu and Hideki Imai (1988).
"Public quadratic polynomial-tuples for efficient signature-verification and message-encryption"

Patarin, Jacques (1995).
"Cryptanalysis of the Matsumoto and Imai public key scheme of Eurocrypt'88".

Kipnis, Aviad and Adi Shamir (1999).
"Cryptanalysis of the HFE public key cryptosystem by relinearization".

Faugere, Jean-Charles and Antoine Joux (2003).
"Algebraic cryptanalysis of hidden field equation (HFE) cryptosystems using Gröbner bases".

# References II


Kipnis, Aviad, Jacques Patarin, and Louis Goubin (1999).
"Unbalanced oil and vinegar signature schemes".

Kipnis, Aviad and Adi Shamir (1998).
"Cryptanalysis of the oil and vinegar signature scheme".

Ding, Jintai and Dieter Schmidt (2005).
"Rainbow, a new multivariable polynomial signature scheme".