Multivariate cryptography – Intro and classic designs

SLMath summer school:
Introduction to Quantum-Safe Cryptography (IBM Zurich)

Simona Samardjiska

1-5 July, 2024

Institute for Computing and Information Sciences
Radboud University

Schedulle (tentative)

- **Monday - Designs**
  - General
  - Classic designs
- **Tuesday - Design and general MQ solving techniques**
  - Key size optimization techniques
  - Algorithms for solving the MQ problem
- **Wednesday - Cryptanalysis**
  - MinRank
  - Equivalent keys attacks
- **Thursday - Cryptanalysis and provably secure designs**
  - Attacks on UOV
  - Fiat-Shamir signatures I
- **Friday - Provably secure designs**
  - Fiat-Shamir signatures II

Notations

- $\mathbb{F}_q$ – finite field of q elements,
- $\mathbb{F}_q^m$ – vector space of vectors $(u_1, u_2, \ldots, u_m)$ over $\mathbb{F}_q$
- $\mathbb{F}_{q^m}$ – extension field of $\mathbb{F}_q$ of degree m
- $\mathbb{F}_q[x_1, \ldots, x_n]$ – ring of polynomials over $\mathbb{F}_q$ in the variables $x_1, \ldots, x_n$
- polynomial ideal - subset of $\mathbb{F}_q[x_1, \ldots, x_n]$ closed under linear combination with polynomial coefficients
- $\mathrm{GL}_n(\mathbb{F}_q)$ – general linear group of degree n over $\mathbb{F}_q$.
- $\mathbf{x} = (x_1, \ldots, x_n)$ – row vectors in $\mathbb{F}_q^n$, $\mathbf{x}^\top = (x_1, \ldots, x_n)^\top$ – column vectors in $\mathbb{F}_q^n$
- $p(x_1, \ldots, x_n) = \sum\limits_{1 \leq i \leq j \leq n} \alpha_{ij} x_i x_j$ – quadratic form
    - matrix form $\bar{\mathbf{P}} = \mathbf{P} + \mathbf{P}^\top$, where $\mathbf{P}_{ij} = \alpha_{ij}/2$ over char $\neq 2$ or $\mathbf{P}_{ij} = \alpha_{ij}$ over char $= 2$

Multivariate cryptography

- Cryptosystems whose security is based on the MQ-**problem** over $\mathbb{F}_q$
  - MQ stands for **M**ultivariate **Q**uadratic
  - Finding a solution to a system of m quadratic equations over a finite field in n variables
  - Decisional variant is **NP-complete problem**
- More general PoSSo problem for higher degree equations

Multivariate cryptography

- Cryptosystems whose security is based on the **MQ-problem** over $\mathbb{F}_q$
  - MQ stands for **M**ultivariate **Q**uadratic
  - Finding a solution to a system of m quadratic equations over a finite field in n variables
  - Decisional variant is **NP-complete problem**
- More general PoSSo problem for higher degree equations

Multivariate cryptography

- Cryptosystems whose security is based on the **MQ-problem** over $\mathbb{F}_q$
  - MQ stands for **M**ultivariate **Q**uadratic
  - Finding a solution to a system of m quadratic equations over a finite field in n variables
  - Decisional variant is **NP-complete problem**
- More general PoSSo problem for higher degree equations

Multivariate cryptography

- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem

Multivariate cryptography

- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem

Multivariate cryptography

- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem

Multivariate cryptography

- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem

Multivariate cryptography

- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem

Multivariate cryptography

- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem

Multivariate cryptography

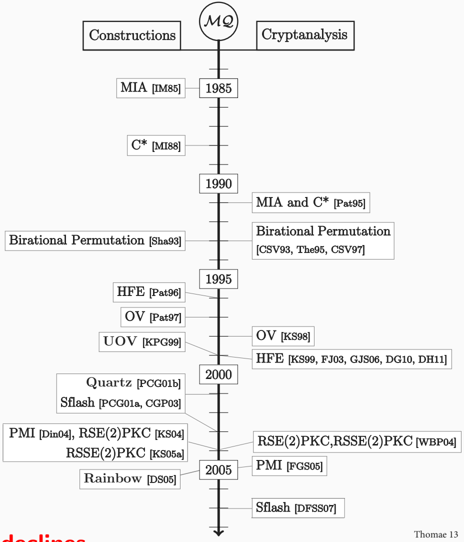
- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem

Multivariate cryptography

- Symmetric (stream cipher QUAD) but mostly public key designs
- Mostly signatures
- Mostly ad-hoc designs, but there are also provably secure ones
- **Shaky history due to break and patch approach**
  - ETSI finalist SFLASH was broken
- NIST submissions:
  - LUOV, Rainbow, GeMSS – short signatures, big keys, ad-hoc
    - all broken! GeMSS severely, Rainbow as finalist
  - MQDSS – short keys, big signatures, provably secure
- **Additional NIST round ongoing**
  - many UOV variants! - UOV, MAYO, TUOV, PROV, VOX, etc.
  - also some Fiat-Shamir signatures - MQOM, ALTEQ*, MEDS*

* - based on variants of the Isomorphism of Polynomials problem



Interest seriously declines

The MQ problem

Computational MQ problem

Given: m multivariate polynomials $p_1, p_2, \dots, p_m \in \mathbb{F}_q[x_1, \dots, x_n]$ of degree 2

Find: (if any) a vector $(u_1, \dots, u_n) \in \mathbb{F}_q^n$ such that

$$\begin{cases} p_1(u_1, \dots, u_n) = & 0 \\ p_2(u_1, \dots, u_n) = & 0 \\ \quad \dots & \\ p_m(u_1, \dots, u_n) = & 0 \end{cases}$$

How hard is it actually?

- **Easy** when $m >$ number of monomials of degree 2
  - linearize and solve as a system of linear equations
- hardest case $n \approx m$
- Complexity well understood for "random" systems (correct: systems without structure)
  - Gröbner bases, XL, Joux-Vitse algorithms

The MQ problem

Computational MQ problem

Given: m multivariate polynomials $p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree 2

Find: (if any) a vector $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ such that

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

How hard is it actually?

- **Easy** when $m >$ number of monomials of degree 2
  - linearize and solve as a system of linear equations
- hardest case $n \approx m$
- Complexity well understood for "random" systems (correct: systems without structure)
  - Gröbner bases, XL, Joux-Vitse algorithms

Computational MQ problem

Given: m multivariate polynomials $p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree 2

Find: (if any) a vector $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ such that

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

How hard is it actually?

- **Easy** when $m >$ number of monomials of degree 2
  - linearize and solve as a system of linear equations
- hardest case $n \approx m$
- Complexity well understood for "random" systems (correct: systems without structure)
  - Gröbner bases, XL, Joux-Vitse algorithms

Computational MQ problem

Given: m multivariate polynomials $p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree 2

Find: (if any) a vector $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ such that

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

How hard is it actually?

- **Easy** when $m >$ number of monomials of degree 2
  - linearize and solve as a system of linear equations
- hardest case $n \approx m$
- Complexity well understood for “random” systems (correct: systems without structure)
  - Gröbner bases, XL, Joux-Vitse algorithms

The MQ problem

Computational MQ problem

Given: m multivariate polynomials $p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree 2

Find: (if any) a vector $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ such that

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

How hard is it actually?

- **Easy** when $m >$ number of monomials of degree 2
  - linearize and solve as a system of linear equations
- hardest case $n \approx m$
- Complexity well understood for "random" systems (correct: systems without structure)
  - Gröbner bases, XL, Joux-Vitse algorithms

The MQ problem

Computational MQ problem

Given: m multivariate polynomials $p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree 2

Find: (if any) a vector $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ such that

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

How hard is it actually?

- **Easy** when $m >$ number of monomials of degree 2
    - linearize and solve as a system of linear equations
- hardest case $n \approx m$
- Complexity well understood for "random" systems (correct: systems without structure)
    - Gröbner bases, XL, Joux-Vitse algorithms

The MQ problem

Computational MQ problem

Given: m multivariate polynomials $p_1, p_2, \ldots, p_m \in \mathbb{F}_q[x_1, \ldots, x_n]$ of degree 2

Find: (if any) a vector $(u_1, \ldots, u_n) \in \mathbb{F}_q^n$ such that

$$\begin{cases} p_1(u_1, \ldots, u_n) = & 0 \\ p_2(u_1, \ldots, u_n) = & 0 \\ \quad \ldots & \\ p_m(u_1, \ldots, u_n) = & 0 \end{cases}$$

How hard is it actually?

- **Easy** when $m >$ number of monomials of degree 2
  - linearize and solve as a system of linear equations
- hardest case $n \approx m$
- Complexity well understood for "random" systems (correct: systems without structure)
  - Gröbner bases, XL, Joux-Vitse algorithms

MQ problem: numerical example

- Example parameters: $n = m = 3$, $\mathbb{F}_q = \mathbb{F}_5$
- Random system of polynomials $\mathcal{F}$:

$$y_1 = 4x_1x_1 + 3x_1x_2 + 0x_1x_3 + x_2x_2 + 2x_2x_3 + x_3x_3 + 0x_1 + 2x_2 + 2x_3$$
$$y_2 = x_1x_1 + 2x_1x_2 + x_1x_3 + 0x_2x_2 + 3x_2x_3 + 4x_3x_3 + 0x_1 + 3x_2 + 2x_3$$
$$y_3 = 0x_1x_1 + x_1x_2 + 4x_1x_3 + 3x_2x_2 + 0x_2x_3 + x_3x_3 + 4x_1 + x_2 + 0x_3$$

- 'Secret' input $\mathbf{x} = (1, 4, 3)$

$$y_1 = 4 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot 4 + 4 \cdot 4 + 2 \cdot 4 \cdot 3 + 3 \cdot 3 + 2 \cdot 4 + 2 \cdot 3 = 79 = 4$$
$$y_2 = 1 \cdot 1 + 2 \cdot 1 \cdot 4 + 1 \cdot 3 + 3 \cdot 4 \cdot 3 + 4 \cdot 3 \cdot 3 + 3 \cdot 4 + 2 \cdot 3 = 102 = 2$$
$$y_3 = 1 \cdot 4 + 4 \cdot 1 \cdot 3 + 3 \cdot 4 \cdot 4 + 3 \cdot 3 + 4 \cdot 1 + 4 = 81 = 1$$

- 'Public' output $\mathbf{y} = (4, 2, 1)$

MQ **problem: numerical example**

- Example parameters: $n = m = 3$, $\mathbb{F}_q = \mathbb{F}_5$
- Random system of polynomials $\mathcal{F}$:

$$y_1 = 4x_1x_1 + 3x_1x_2 + 0x_1x_3 + x_2x_2 + 2x_2x_3 + x_3x_3 + 0x_1 + 2x_2 + 2x_3$$
$$y_2 = x_1x_1 + 2x_1x_2 + x_1x_3 + 0x_2x_2 + 3x_2x_3 + 4x_3x_3 + 0x_1 + 3x_2 + 2x_3$$
$$y_3 = 0x_1x_1 + x_1x_2 + 4x_1x_3 + 3x_2x_2 + 0x_2x_3 + x_3x_3 + 4x_1 + x_2 + 0x_3$$

- 'Secret' input $\mathbf{x} = (1, 4, 3)$

$$y_1 = 4\cdot1\cdot1 + 3\cdot1\cdot4 + 4\cdot4 + 2\cdot4\cdot3 + 3\cdot3 + 2\cdot4 + 2\cdot3 = 79 = 4$$
$$y_2 = 1\cdot1 + 2\cdot1\cdot4 + 1\cdot3 + 3\cdot4\cdot3 + 4\cdot3\cdot3 + 3\cdot4 + 2\cdot3 = 102 = 2$$
$$y_3 = 1\cdot4 + 4\cdot1\cdot3 + 3\cdot4\cdot4 + 3\cdot3 + 4\cdot1 + 4 = 81 = 1$$

- 'Public' output $\mathbf{y} = (4, 2, 1)$

MQ problem: numerical example

- Example parameters: $n = m = 3$, $\mathbb{F}_q = \mathbb{F}_5$
- Random system of polynomials $\mathcal{F}$:

$$y_1 = 4x_1x_1 + 3x_1x_2 + 0x_1x_3 + x_2x_2 + 2x_2x_3 + x_3x_3 + 0x_1 + 2x_2 + 2x_3$$
$$y_2 = x_1x_1 + 2x_1x_2 + x_1x_3 + 0x_2x_2 + 3x_2x_3 + 4x_3x_3 + 0x_1 + 3x_2 + 2x_3$$
$$y_3 = 0x_1x_1 + x_1x_2 + 4x_1x_3 + 3x_2x_2 + 0x_2x_3 + x_3x_3 + 4x_1 + x_2 + 0x_3$$

- 'Secret' input $\mathbf{x} = (1, 4, 3)$

$$y_1 = 4 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot 4 + 4 \cdot 4 + 2 \cdot 4 \cdot 3 + 3 \cdot 3 + 2 \cdot 4 + 2 \cdot 3 = 79 = 4$$
$$y_2 = 1 \cdot 1 + 2 \cdot 1 \cdot 4 + 1 \cdot 3 + 3 \cdot 4 \cdot 3 + 4 \cdot 3 \cdot 3 + 3 \cdot 4 + 2 \cdot 3 = 102 = 2$$
$$y_3 = 1 \cdot 4 + 4 \cdot 1 \cdot 3 + 3 \cdot 4 \cdot 4 + 3 \cdot 3 + 4 \cdot 1 + 4 = 81 = 1$$

- 'Public' output $\mathbf{y} = (4, 2, 1)$

MQ problem: numerical example

- Example parameters: $n = m = 3$, $\mathbb{F}_q = \mathbb{F}_5$
- Random system of polynomials $\mathcal{F}$:

$$y_1 = 4x_1x_1 + 3x_1x_2 + 0x_1x_3 + x_2x_2 + 2x_2x_3 + x_3x_3 + 0x_1 + 2x_2 + 2x_3$$
$$y_2 = x_1x_1 + 2x_1x_2 + x_1x_3 + 0x_2x_2 + 3x_2x_3 + 4x_3x_3 + 0x_1 + 3x_2 + 2x_3$$
$$y_3 = 0x_1x_1 + x_1x_2 + 4x_1x_3 + 3x_2x_2 + 0x_2x_3 + x_3x_3 + 4x_1 + x_2 + 0x_3$$

- 'Secret' input $\mathbf{x} = (1, 4, 3)$

$$y_1 = 4 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot 4 + 4 \cdot 4 + 2 \cdot 4 \cdot 3 + 3 \cdot 3 + 2 \cdot 4 + 2 \cdot 3 = 79 \equiv 4$$
$$y_2 = 1 \cdot 1 + 2 \cdot 1 \cdot 4 + 1 \cdot 3 + 3 \cdot 4 \cdot 3 + 4 \cdot 3 \cdot 3 + 3 \cdot 4 + 2 \cdot 3 = 102 \equiv 2$$
$$y_3 = 1 \cdot 4 + 4 \cdot 1 \cdot 3 + 3 \cdot 4 \cdot 4 + 3 \cdot 3 + 4 \cdot 1 + 4 = 81 \equiv 1$$

- 'Public' output $\mathbf{y} = (4, 2, 1)$

MQ problem: numerical example

- Example parameters: $n = m = 3$, $\mathbb{F}_q = \mathbb{F}_5$
- Random system of polynomials $\mathcal{F}$:

$$y_1 = 4x_1x_1 + 3x_1x_2 + 0x_1x_3 + x_2x_2 + 2x_2x_3 + x_3x_3 + 0x_1 + 2x_2 + 2x_3$$
$$y_2 = x_1x_1 + 2x_1x_2 + x_1x_3 + 0x_2x_2 + 3x_2x_3 + 4x_3x_3 + 0x_1 + 3x_2 + 2x_3$$
$$y_3 = 0x_1x_1 + x_1x_2 + 4x_1x_3 + 3x_2x_2 + 0x_2x_3 + x_3x_3 + 4x_1 + x_2 + 0x_3$$

- 'Secret' input $\mathbf{x} = (1, 4, 3)$

$$y_1 = 4 \cdot 1 \cdot 1 + 3 \cdot 1 \cdot 4 + 4 \cdot 4 + 2 \cdot 4 \cdot 3 + 3 \cdot 3 + 2 \cdot 4 + 2 \cdot 3 = 79 \equiv 4$$
$$y_2 = 1 \cdot 1 + 2 \cdot 1 \cdot 4 + 1 \cdot 3 + 3 \cdot 4 \cdot 3 + 4 \cdot 3 \cdot 3 + 3 \cdot 4 + 2 \cdot 3 = 102 \equiv 2$$
$$y_3 = 1 \cdot 4 + 4 \cdot 1 \cdot 3 + 3 \cdot 4 \cdot 4 + 3 \cdot 3 + 4 \cdot 1 + 4 = 81 \equiv 1$$

- 'Public' output $\mathbf{y} = (4, 2, 1)$

Multivariate signatures – the ad-hoc construction

- Start with a structured central map **that is easily invertible**

$$\mathcal{F} : (x_1, \ldots, x_n) \in \mathbb{F}_q^n \to \big(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\big) \in \mathbb{F}_q^m,$$

- Hide the structured central map, using two bijective linear maps $\mathcal{S}$ and $\mathcal{T}$
- The public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is then obtained as

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

- and basically looks like $\mathcal{P}(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$ where $p_s(x_1, \ldots, x_n) = \sum\limits_{1 \le i \le j \le n} \alpha_{ij}^{(s)} x_i x_j + \sum_{i=1}^n \beta_i^{(s)} x_i + \gamma^{(s)}$ for some coefficients $\alpha_{ij}^{(s)}, \beta_i^{(s)}, \gamma^{(s)} \in \mathbb{F}_q$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\text{private key}", "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

Multivariate signatures – the ad-hoc construction

- Start with a structured central map **that is easily invertible**

$$\mathcal{F} : (x_1, \ldots, x_n) \in \mathbb{F}_q^n \to \big(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\big) \in \mathbb{F}_q^m,$$

- Hide the structured central map, using two bijective linear maps $\mathcal{S}$ and $\mathcal{T}$
- The public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is then obtained as

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

- and basically looks like $\mathcal{P}(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$ where $p_s(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} \alpha_{ij}^{(s)} x_i x_j + \sum_{i=1}^n \beta_i^{(s)} x_i + \gamma^{(s)}$ for some coefficients $\alpha_{ij}^{(s)}, \beta_i^{(s)}, \gamma^{(s)} \in \mathbb{F}_q$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\text{private key}", "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

Multivariate signatures – the ad-hoc construction

- Start with a structured central map **that is easily invertible**

$$\mathcal{F} : (x_1, \ldots, x_n) \in \mathbb{F}_q^n \to \big(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\big) \in \mathbb{F}_q^m,$$

- Hide the structured central map, using two bijective linear maps $\mathcal{S}$ and $\mathcal{T}$
- The public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is then obtained as

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

- and basically looks like $\mathcal{P}(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$ where $p_s(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} \alpha_{ij}^{(s)} x_i x_j + \sum_{i=1}^n \beta_i^{(s)} x_i + \gamma^{(s)}$ for some coefficients $\alpha_{ij}^{(s)}, \beta_i^{(s)}, \gamma^{(s)} \in \mathbb{F}_q$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[rr, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[rr, "\text{private key}", "\mathcal{F}"'] & & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

Multivariate signatures – the ad-hoc construction

- Start with a structured central map **that is easily invertible**

$$\mathcal{F} : (x_1, \ldots, x_n) \in \mathbb{F}_q^n \to \big(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\big) \in \mathbb{F}_q^m,$$

- Hide the structured central map, using two bijective linear maps $\mathcal{S}$ and $\mathcal{T}$
- The public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is then obtained as

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

- and basically looks like $\mathcal{P}(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$ where $p_s(x_1, \ldots, x_n) = \sum\limits_{1 \le i \le j \le n} \alpha_{ij}^{(s)} x_i x_j + \sum_{i=1}^n \beta_i^{(s)} x_i + \gamma^{(s)}$ for some coefficients $\alpha_{ij}^{(s)}, \beta_i^{(s)}, \gamma^{(s)} \in \mathbb{F}_q$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\text{private key}", "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

Multivariate signatures – the ad-hoc construction

- Start with a structured central map **that is easily invertible**

$$\mathcal{F} : (x_1, \ldots, x_n) \in \mathbb{F}_q^n \to \big(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)\big) \in \mathbb{F}_q^m,$$

- Hide the structured central map, using two bijective linear maps $\mathcal{S}$ and $\mathcal{T}$
- The public key $\mathcal{P} : \mathbb{F}_q^n \to \mathbb{F}_q^m$ is then obtained as

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

- and basically looks like $\mathcal{P}(x_1, \ldots, x_n) = (p_1(x_1, \ldots, x_n), \ldots, p_m(x_1, \ldots, x_n))$ where $p_s(x_1, \ldots, x_n) = \sum_{1 \le i \le j \le n} \alpha_{ij}^{(s)} x_i x_j + \sum_{i=1}^n \beta_i^{(s)} x_i + \gamma^{(s)}$ for some coefficients $\alpha_{ij}^{(s)}, \beta_i^{(s)}, \gamma^{(s)} \in \mathbb{F}_q$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\text{private key}", "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

- **To sign a message m**,
  - hash the message $H(\mathbf{m})$
  - apply the inverses of the secret maps $\mathcal{T}$, $\mathcal{F}$, $\mathcal{S}$

$$\sigma = \mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1}(H(\mathbf{m}))$$

- **To verify a signature** σ,
  - evaluate the polynomials $\mathcal{P}$ at σ and
  - check if it matches $H(\mathbf{m})$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\text{private key}", "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{Verification}"'] & \mathbb{F}_q^m \arrow[d, "\mathcal{T}^{-1}"] \\
\mathbb{F}_q^n \arrow[u, "\mathcal{S}^{-1}"] & \mathbb{F}_q^m \arrow[l, "\text{Signing}"', "\mathcal{F}^{-1}"]
\end{tikzcd}$$

Signing/Verification

Multivariate signatures – the ad-hoc construction

- **To sign a message $\mathbf{m}$,**
  - hash the message $H(\mathbf{m})$
  - apply the inverses of the secret maps $\mathcal{T}$, $\mathcal{F}$, $\mathcal{S}$

$$\sigma = \mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1}(H(\mathbf{m}))$$

- **To verify a signature σ,**
  - evaluate the polynomials $\mathcal{P}$ at σ and
  - check if it matches $H(\mathbf{m})$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\text{private key}", "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}", "\text{Verification}"'] & \mathbb{F}_q^m \arrow[d, "\mathcal{T}^{-1}"] \\
\mathbb{F}_q^n \arrow[u, "\mathcal{S}^{-1}"] & \mathbb{F}_q^m \arrow[l, "\text{Signing}"', "\mathcal{F}^{-1}"]
\end{tikzcd}$$

Signing/Verification

Multivariate signatures – the ad-hoc construction

- **To sign a message $\mathbf{m}$**,
  - hash the message $H(\mathbf{m})$
  - apply the inverses of the secret maps $\mathcal{T}$, $\mathcal{F}$, $\mathcal{S}$

$$\sigma = \mathcal{S}^{-1} \circ \mathcal{F}^{-1} \circ \mathcal{T}^{-1}(H(\mathbf{m}))$$

- **To verify a signature σ**,
  - evaluate the polynomials $\mathcal{P}$ at σ and
  - check if it matches $H(\mathbf{m})$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[rr, "\mathcal{P}", "\text{public key}"'] \arrow[d, "\mathcal{S}"'] & & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[rr, "\text{private key}", "\mathcal{F}"'] & & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"']
\end{tikzcd}$$

Key generation

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[rr, "\mathcal{P}", "\text{Verification}"'] & & \mathbb{F}_q^m \arrow[d, "\mathcal{T}^{-1}"] \\
\mathbb{F}_q^n \arrow[u, "\mathcal{S}^{-1}"] & & \mathbb{F}_q^m \arrow[ll, "\text{Signing}"', "\mathcal{F}^{-1}"]
\end{tikzcd}$$

Signing/Verification

The ad-hoc construction - Signature and key sizes

- **Signature** $\in \mathbb{F}_q^n$ - hence only $\log q \cdot n$ bits
- **Private key** - can be generated from seed - hence only store a small seed (ex. 256 bits)
- **Public key** typically can't be compressed
  - m degree 2 homogeneous polynomials in n over $\in \mathbb{F}_q$ - hence $\log q \cdot \binom{n+1}{2}$ bits
  - there are some optimization techniques we discuss later

Families of ad-hoc multivariate signatures

- **Mixed-field schemes**
  - Secret key defined over extension field, and transformed in the ground field
  - C^*, HFE variants including GeMSS
- **Single field schemes**
  - Defined over and all operations in a single field
  - Oil and vinegar schemes (UOV, LUOV, MAYO, Rainbow)
  - Step-wise triangular schemes (TTS, TTM, MQQ-sig, Rainbow)

Families of ad-hoc multivariate signatures

- **Mixed-field schemes**
  - Secret key defined over extension field, and transformed in the ground field
  - C^*, HFE variants including GeMSS
- **Single field schemes**
  - Defined over and all operations in a single field
  - Oil and vinegar schemes (UOV, LUOV, MAYO, Rainbow)
  - Step-wise triangular schemes (TTS, TTM, MQQ-sig, Rainbow)

Mixed-field schemes

General principle of mixed-field schemes

- Central map $\mathcal{F}$ constructed in extension field $\mathbb{F}_{q^n}$ as a univariate map $\widetilde{\mathcal{F}}$.
  - ($\mathbb{F}_{q^n}$ constructed as quotient ring $\mathbb{F}_q[X]/g(X)$ for irreducible $g(X)$ of degree n)
- Then mapped bijectively to the ground field using $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ defined by:

$$\phi(\sum_0^{n-1} u_i X_i) = (u_1, \ldots, u_n)$$

for a basis $(1, X \ldots, x^{n-1}) \in \mathbb{F}_{q^n}^n$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$

- Public key $\mathcal{P}$ then obtained by masking over the ground field with $\mathcal{S}$ and $\mathcal{T}$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}"] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"'] \arrow[d, "\phi^{-1}"] \\
\mathbb{F}_{q^n} \arrow[u, "\phi"] \arrow[r, "\widetilde{\mathcal{F}}"'] & \mathbb{F}_{q^m}
\end{tikzcd}$$

General principle of mixed-field schemes

- Central map $\mathcal{F}$ constructed in extension field $\mathbb{F}_{q^n}$ as a univariate map $\widetilde{\mathcal{F}}$.
  - ($\mathbb{F}_{q^n}$ constructed as quotient ring $\mathbb{F}_q[X]/g(X)$ for irreducible $g(X)$ of degree n)
- Then mapped bijectively to the ground field using $\phi : \mathbb{F}_{q^n} \to \mathbb{F}_q^n$ defined by:

$$\phi(\sum_0^{n-1} u_i X_i) = (u_1, \ldots, u_n)$$

for a basis $(1, X \ldots, x^{n-1}) \in \mathbb{F}_{q^n}^n$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$

- Public key $\mathcal{P}$ then obtained by masking over the ground field with $\mathcal{S}$ and $\mathcal{T}$

$$\begin{tikzcd}
\mathbb{F}_q^n \arrow[r, "\mathcal{P}"] \arrow[d, "\mathcal{S}"'] & \mathbb{F}_q^m \\
\mathbb{F}_q^n \arrow[r, "\mathcal{F}"'] & \mathbb{F}_q^m \arrow[u, "\mathcal{T}"'] \arrow[d, "\phi^{-1}"] \\
\mathbb{F}_{q^n} \arrow[u, "\phi"] \arrow[r, "\widetilde{\mathcal{F}}"'] & \mathbb{F}_{q^m}
\end{tikzcd}$$

C* [Matsumoto and Imai '85]

- Central map over extension field extremely simple – permutation monomial of algebraic degree 2:

$$\widetilde{\mathcal{F}}(X) = X^{q^t+1}$$

  where $\gcd(q^t + 1, q^n - 1) = 1$ (condition for bijectivity). Secret key is t.
- The inverse can be computed as

$$\widetilde{\mathcal{F}}^{-1}(Y) = Y^h$$

  where h is the multiplicative inverse of $q^t + 1$ modulo $q^n - 1$.
- **Very easy to break!** [Message recovery attack Patarin '95]
  - input X and the output Y of the map connected as

$$\begin{aligned} Y^{q^t-1}XY &= (X^{q^t+1})^{q^t-1}XY \\ XY^{q^t} &= X^{q^{2t}}Y \end{aligned}$$

  - $\Rightarrow$ bilinear relation between secret input X and known output Y
  - **Attack step 1**: Collect many input-output pairs to form a bilinear system
  - **Attack step 2**: In the bilinear system plug in Y, and solve for X

C* [Matsumoto and Imai '85]

- Central map over extension field extremely simple – permutation monomial of algebraic degree 2:

$$\widetilde{\mathcal{F}}(X) = X^{q^t+1}$$

where $\gcd(q^t+1, q^n-1) = 1$ (condition for bijectivity). Secret key is t.
- The inverse can be computed as

$$\widetilde{\mathcal{F}}^{-1}(Y) = Y^h$$

where h is the multiplicative inverse of q^t+1 modulo q^n-1.

- **Very easy to break!** [Message recovery attack Patarin '95]
  - input X and the output Y of the map connected as

$$\begin{aligned} Y^{q^t-1}XY &= (X^{q^t+1})^{q^t-1}XY \\ XY^{q^t} &= X^{q^{2t}}Y \end{aligned}$$

  - $\Rightarrow$ bilinear relation between secret input X and known output Y
  - **Attack step 1**: Collect many input-output pairs to form a bilinear system
  - **Attack step 2**: In the bilinear system plug in Y, and solve for X

C^* [Matsumoto and Imai '85]

- Central map over extension field extremely simple – permutation monomial of algebraic degree 2:

$$\widetilde{\mathcal{F}}(X) = X^{q^t+1}$$

where $\gcd(q^t+1, q^n-1) = 1$ (condition for bijectivity). Secret key is t.
- The inverse can be computed as

$$\widetilde{\mathcal{F}}^{-1}(Y) = Y^h$$

where h is the multiplicative inverse of q^t+1 modulo q^n-1.

- **Very easy to break!** [Message recovery attack Patarin '95]
  - input X and the output Y of the map connected as

$$\begin{aligned} Y^{q^t-1}XY &= (X^{q^t+1})^{q^t-1}XY \\ XY^{q^t} &= X^{q^{2t}}Y \end{aligned}$$

  - $\Rightarrow$ bilinear relation between secret input X and known output Y
  - **Attack step 1**: Collect many input-output pairs to form a bilinear system
  - **Attack step 2**: In the bilinear system plug in Y, and solve for X

C* modifications

- C^{*-} scheme using the "minus" modifier
- used in SFLASH - a signature scheme proposed by Patarin, Goubin and Courtois in 2001
- SFLASH was selected in 2003 by the NESSIE European Consortium **as one of the three recommended public key signature schemes, and as the best known solution for low cost smart cards**
- It was broken in 2007 by Dubois using a differential attack
- pFLASH - proposed in 2015
  - projection modifier (project the input to smaller hyperplane)
  - broken in 2021 - øygarden, Smith-Tone, Verbel
  - uses attack by Tao, Petzoldt, Ding '20 that applies to virtually all HFE variants with modifiers

C^* modifications

- C^{*-} scheme using the "minus" modifier
- used in SFLASH - a signature scheme proposed by Patarin, Goubin and Courtois in 2001
- SFLASH was selected in 2003 by the NESSIE European Consortium **as one of the three recommended public key signature schemes, and as the best known solution for low cost smart cards**
- It was broken in 2007 by Dubois using a differential attack
- pFLASH - proposed in 2015
  - projection modifier (project the input to smaller hyperplane)
  - broken in 2021 - øygarden, Smith-Tone, Verbel
  - uses attack by Tao, Petzoldt, Ding '20 that applies to virtually all HFE variants with modifiers

C^* modifications

- C^{*-} scheme using the "minus" modifier
- used in SFLASH - a signature scheme proposed by Patarin, Goubin and Courtois in 2001
- SFLASH was selected in 2003 by the NESSIE European Consortium **as one of the three recommended public key signature schemes, and as the best known solution for low cost smart cards**
- It was broken in 2007 by Dubois using a differential attack
- pFLASH - proposed in 2015
  - projection modifier (project the input to smaller hyperplane)
  - broken in 2021 - øygarden, Smith-Tone, Verbel
  - uses attack by Tao, Petzoldt, Ding '20 that applies to virtually all HFE variants with modifiers

HFE (Hidden field equation) [Patarin '96]

- Original HFE proposed by Patarin in '96 as a direct generalization of C^*
- Uses general quadratic polynomial (Dembowski-Ostrom polynomial) over $\mathbb{F}_{q^n}$

$$\widetilde{\mathcal{F}}(X) = \sum_{\substack{0 \le i,j \le D \\ q^i + q^j \le D}} a_{ij} X^{q^i + q^j} + \sum_{\substack{0 \le k \le D \\ q^k \le D}} b_k X^{q^k} + c$$

- Degree D must be bounded for efficient inversion (signing)
- Inversion of polynomial done using Berlekamp's algorithm
- The DO polynomial is not a bijection in general, so no guarantees for
  - Existence of signatures (can be fixed by a diversifier)
  - Unique decryption if used as an encryption scheme (can be fixed by adding some disambiguation in the plaintext)

HFE (Hidden field equation) [Patarin '96]

- Original HFE proposed by Patarin in '96 as a direct generalization of C^*
- Uses general quadratic polynomial (Dembowski-Ostrom polynomial) over $\mathbb{F}_{q^n}$

$$\widetilde{\mathcal{F}}(X) = \sum_{\substack{0 \le i,j \le D \\ q^i + q^j \le D}} a_{ij} X^{q^i + q^j} + \sum_{\substack{0 \le k \le D \\ q^k \le D}} b_k X^{q^k} + c$$

- Degree D must be bounded for efficient inversion (signing)
- Inversion of polynomial done using Berlekamp's algorithm

- The DO polynomial is not a bijection in general, so no guarantees for
  - Existence of signatures (can be fixed by a diversifier)
  - Unique decryption if used as an encryption scheme (can be fixed by adding some disambiguation in the plaintext)

HFE security

- **Key recovery attacks**
  - MinRank over extension field [Kipnis and Shamir '99]
  - MinRank over ground field [Bettale, Faugère, Perret '11]
- **Message recovery attacks**
  - Faugère solved HFE Challenge 1 (HFE over GF2, d = 96) in 2002
  - System can be solved much faster than a random system
  - Ding and Hodges prove that degree of regularity is connected to the degree D of the DO polynomials
  - Efficiency and security contradict each other
    - Signing using Berlekamp is $O(nD)$
    - Attacks $O(n^{q \log_q D})$
    - For $q = 2$, $D = 512$, attack is quite low
- **Conclussion:** HFE is not secure!

- Several fixes proposed
  - HFEv- survived the longest (Quartz, GUI, GeMSS)

HFE security

- **Key recovery attacks**
  - MinRank over extension field [Kipnis and Shamir '99]
  - MinRank over ground field [Bettale, Faugère, Perret '11]
- **Message recovery attacks**
  - Faugère solved HFE Challenge 1 (HFE over GF2, d = 96) in 2002
  - System can be solved much faster than a random system
  - Ding and Hodges prove that degree of regularity is connected to the degree D of the DO polynomials
  - Efficiency and security contradict each other
    - Signing using Berlekamp is $O(nD)$
    - Attacks $O(n^{q \log_q D})$
    - For $q = 2$, $D = 512$, attack is quite low
- **Conclusion:** HFE is not secure!
- Several fixes proposed
  - HFEv- survived the longest (Quartz, GUI, GeMSS)

HFE security

- **Key recovery attacks**
  - MinRank over extension field [Kipnis and Shamir '99]
  - MinRank over ground field [Bettale, Faugère, Perret '11]
- **Message recovery attacks**
  - Faugère solved HFE Challenge 1 (HFE over GF2, d = 96) in 2002
  - System can be solved much faster than a random system
  - Ding and Hodges prove that degree of regularity is connected to the degree D of the DO polynomials
  - Efficiency and security contradict each other
    - Signing using Berlekamp is $O(nD)$
    - Attacks $O(n^{q \log_q D})$
    - For $q = 2$, $D = 512$, attack is quite low
- **Conclussion:** HFE is not secure!

- Several fixes proposed
  - HFEv- survived the longest (Quartz, GUI, GeMSS)

HFE security

- **Key recovery attacks**
  - MinRank over extension field [Kipnis and Shamir '99]
  - MinRank over ground field [Bettale, Faugère, Perret '11]
- **Message recovery attacks**
  - Faugère solved HFE Challenge 1 (HFE over GF2, d = 96) in 2002
  - System can be solved much faster than a random system
  - Ding and Hodges prove that degree of regularity is connected to the degree D of the DO polynomials
  - Efficiency and security contradict each other
    - Signing using Berlekamp is $O(nD)$
    - Attacks $O(n^{q \log_q D})$
    - For $q = 2$, $D = 512$, attack is quite low
- **Conclussion:** HFE is not secure!

- Several fixes proposed
  - HFEv- survived the longest (Quartz, GUI, GeMSS)

HFEv- and GeMSS (finalist in NIST standardization process)

- **HFEv- = HFE + vinegar modification + minus modification**
  - vinegar mod. adds v extra vinegar variables
  - minus mod. removes a polynomials from the public key
- **Central map is:** $\widetilde{\mathcal{F}}(X) : \mathbb{F}_q^v \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$

$$\widetilde{\mathcal{F}}(X) = \sum_{\substack{0 \le i,j \le D \\ q^i + q^j \le D}} a_{ij} X^{q^i+q^j} + \sum_{\substack{0 \le k \le D \\ q^k \le D}} b_k(v_1, v_2, \ldots, v_v) X^{q^k} + c(v_1, v_2, \ldots, v_v)$$

- **Signing:**
  - Compute $\mathbf{w} = H(\mathbf{m}) \in \mathbb{F}_q^{n-a}$
  - Compute $\mathbf{u} = \mathcal{T}^{-1}(\mathbf{w}) \in \mathbb{F}_q^n$ and $U = \phi^{-1}(\mathbf{u}) \in \mathbb{F}_{q^n}$
  - Choose random values for the vinegar variables $v_1, \ldots, v_v$
  - Solve $\widetilde{\mathcal{F}}_v(Y) = U$ over $\mathbb{F}_{q^n}$ via Berlekamp's algorithm
  - Compute $\mathbf{y} = \phi(Y) \in \mathbb{F}_q^n$
  - Signature is $\sigma = \mathcal{S}^{-1}(\mathbf{y}||v_1||\ldots||v_v)$
- **Verification** works as usual

HFEv- and GeMSS (finalist in NIST standardization process)

- **HFEv- = HFE + vinegar modification + minus modification**
  - vinegar mod. adds v extra vinegar variables
  - minus mod. removes a polynomials from the public key
- **Central map is:** $\widetilde{\mathcal{F}}(X) : \mathbb{F}_q^v \times \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$

$$\widetilde{\mathcal{F}}(X) = \sum_{\substack{0 \le i,j \le D \\ q^i + q^j \le D}} a_{ij} X^{q^i + q^j} + \sum_{\substack{0 \le k \le D \\ q^k \le D}} b_k(v_1, v_2, \ldots, v_v) X^{q^k} + c(v_1, v_2, \ldots, v_v)$$

- **Signing:**
  - Compute $\mathbf{w} = H(\mathbf{m}) \in \mathbb{F}_q^{n-a}$
  - Compute $\mathbf{u} = \mathcal{T}^{-1}(\mathbf{w}) \in \mathbb{F}_q^n$ and $U = \phi^{-1}(\mathbf{u}) \in \mathbb{F}_{q^n}$
  - Choose random values for the vinegar variables $v_1, \ldots, v_v$
  - Solve $\widetilde{\mathcal{F}}_v(Y) = U$ over $\mathbb{F}_{q^n}$ via Berlekamp's algorithm
  - Compute $\mathbf{y} = \phi(Y) \in \mathbb{F}_q^n$
  - Signature is $\sigma = \mathcal{S}^{-1}(\mathbf{y}||v_1||...||v_v)$
- **Verification** works as usual

Security of GeMSS (finalist in NIST standardization process)

- Just an **HFEv-** scheme
- **Several iteration of MinRank:**
  - Min-Q-rank attack

$$O(\binom{n + \log_q D + a + v + 1}{\log_q D + a + v + 1}^{\omega})$$

  - MinRank style attack [Tao, Petzoldt, Ding '21]

$$O(\binom{n + \log_q D + v + 1}{\log_q D + v + 1}^{\omega})$$

    - Completely independent of a
- Not feasible anymore to create an efficient scheme
- GeMSS completely broken!
- NIST security level III should be: $D \geq 2^{19}$!

Security of GeMSS (finalist in NIST standardization process)

- Just an **HFEv-** scheme
- **Several iteration of MinRank:**
  - Min-Q-rank attack

$$O\left(\binom{n+\log_q D+a+v+1}{\log_q D+a+v+1}^{\omega}\right)$$

  - MinRank style attack [Tao, Petzoldt, Ding '21]

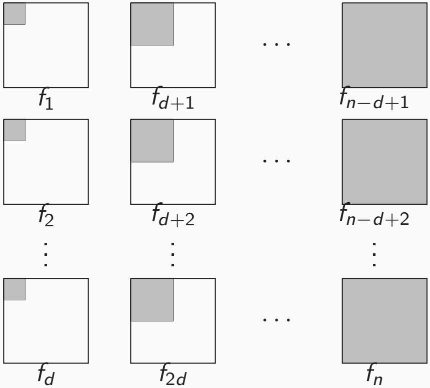
$$O\left(\binom{n+\log_q D+v+1}{\log_q D+v+1}^{\omega}\right)$$

    - Completely independent of a
- Not feasible anymore to create an efficient scheme
- GeMSS completely broken!
- NIST security level III should be: $D \geq 2^{19}$!

Single field schemes

Layered schemes

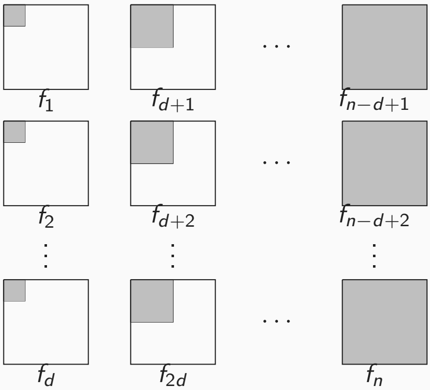
- The central map defined by several layers, in each layer several new variables introduced
- In matrix form, the central (symmetric) matrices are:



- The structure can be disguised (TTS, EnTTS, MQQ-sig)
- **Very susceptible to rank defect attacks!**
- And these attacks only get better :)

Layered schemes

- The central map defined by several layers, in each layer several new variables introduced
- In matrix form, the central (symmetric) matrices are:



- The structure can be disguised (TTS, EnTTS, MQQ-sig)
- **Very susceptible to rank defect attacks!**
- And these attacks only get better :)

Unbalanced Oil and Vinegar (UOV)

- Proposed by Kipnis and Patarin '99 as amendment of the Oil and Vinegar scheme by Patarin (broken by Kipnis and Shamir '98)
- The central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^o$ is $\mathcal{F}(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_o(x_1, \ldots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V \\ i \le j}} \alpha_{ij}{}^{(s)} x_i x_j + \sum_{\substack{i \in V \\ j \in O}} \beta_{ij}{}^{(s)} x_i x_j$$

  where $\alpha_{ij}^{(s)}$ - coefficients of the vinegar-vinegar, the $\beta_{ij}^{(s)}$ of the oil-vinegar monomials
  - $V = \{1, 2, \ldots, v\}$ - index set of vinegar vars, $O = \{v+1, v+2, \ldots, n\}$ - index set of oil vars
- In matrix form, the central matrices are
- No $\mathcal{T}$ map - not necessary and does not add to the security! **Why?**

Unbalanced Oil and Vinegar (UOV)

- Proposed by Kipnis and Patarin '99 as amendment of the Oil and Vinegar scheme by Patarin (broken by Kipnis and Shamir '98)
- The central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^o$ is $\mathcal{F}(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_o(x_1, \ldots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V \\ i \leq j}} \alpha_{ij}{}^{(s)} x_i x_j + \sum_{\substack{i \in V \\ j \in O}} \beta_{ij}{}^{(s)} x_i x_j$$

  where $\alpha_{ij}^{(s)}$ - coefficients of the vinegar-vinegar, the $\beta_{ij}^{(s)}$ of the oil-vinegar monomials
  - $V = \{1, 2, \ldots, v\}$ - index set of vinegar vars, $O = \{v+1, v+2, \ldots, n\}$ - index set of oil vars
- In matrix form, the central matrices are

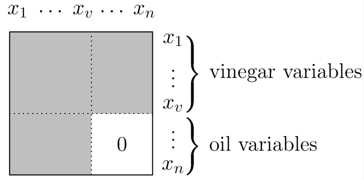
- No $\mathcal{T}$ map - not necessary and does not add to the security! **Why?**

Unbalanced Oil and Vinegar (UOV)

- Proposed by Kipnis and Patarin '99 as amendment of the Oil and Vinegar scheme by Patarin (broken by Kipnis and Shamir '98)
- The central map $\mathcal{F} : \mathbb{F}^n \rightarrow \mathbb{F}^o$ is $\mathcal{F}(x_1, \ldots, x_n) = (f_1(x_1, \ldots, x_n), \ldots, f_o(x_1, \ldots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V \\ i \leq j}} \alpha_{ij}{}^{(s)} x_i x_j + \sum_{\substack{i \in V \\ j \in O}} \beta_{ij}{}^{(s)} x_i x_j$$

  where $\alpha_{ij}^{(s)}$ - coefficients of the vinegar-vinegar, the $\beta_{ij}^{(s)}$ of the oil-vinegar monomials
  - $V = \{1, 2, \ldots, v\}$ - index set of vinegar vars, $O = \{v+1, v+2, \ldots, n\}$ - index set of oil vars
- In matrix form, the central matrices are



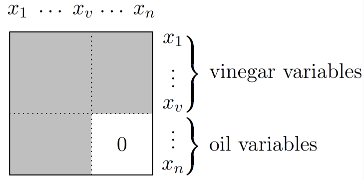
- No $\mathcal{T}$ map - not necessary and does not add to the security! **Why?**

Unbalanced Oil and Vinegar (UOV)

- Proposed by Kipnis and Patarin '99 as amendment of the Oil and Vinegar scheme by Patarin (broken by Kipnis and Shamir '98)
- The central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^o$ is $\mathcal{F}(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_o(x_1, \dots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V \\ i \le j}} \alpha_{ij}{}^{(s)} x_i x_j + \sum_{\substack{i \in V \\ j \in O}} \beta_{ij}{}^{(s)} x_i x_j$$

  where $\alpha_{ij}^{(s)}$ - coefficients of the vinegar-vinegar, the $\beta_{ij}^{(s)}$ of the oil-vinegar monomials
  - $V = \{1, 2, \dots, v\}$ - index set of vinegar vars, $O = \{v+1, v+2, \dots, n\}$ - index set of oil vars
- In matrix form, the central matrices are



- No $\mathcal{T}$ map - not necessary and does not add to the security! **Why?**

UOV baby example

Central map $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

Vinegar variables x_1, x_2 & Oil variables x_3, x_4

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4 + x_3$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3$$

UOV baby example

Central map $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

Vinegar variables x_1, x_2 & Oil variables x_3, x_4

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4 + x_3$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3$$

Linear $\mathcal{S} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

Public map $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

$$\begin{aligned} p_1(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_4 \\ p_2(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_4 + x_3x_4 + x_1 + x_4 \end{aligned}$$

All monomials appear! Looks "random"

To sign a message $\mathbf{m}$,

- hash the message $(h_1, h_2) = H(\mathbf{m})$
- fix randomly the vinegar variables

$$f_1(c_1, c_2, x_3, x_4) = c_1c_2 + c_1x_3 + c_2x_4 + x_3$$

$$f_2(c_1, c_2, x_3, x_4) = c_1x_4 + c_2x_3 + c_2x_4 + x_3$$

- Solve the linear system

$$c_1c_2 + c_1x_3 + c_2x_4 + x_3 = h_1$$

$$c_1x_4 + c_2x_3 + c_2x_4 + x_3 = h_2$$

- The solution is (c_3, c_4) (*-repeat if no solution)
- The signature is $\sigma = (s_1, s_2, s_3, s_4) = \mathcal{S}^{-1}(c_1, c_2, c_3, c_4)$

UOV baby example

Central map $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

Vinegar variables x_1, x_2 & Oil variables x_3, x_4

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4 + x_3$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3$$

$$\text{Linear } \mathcal{S} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$$

Public map $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

$$\begin{aligned} p_1(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_4 \\ p_2(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_4 + x_3x_4 + x_1 + x_4 \end{aligned}$$

All monomials appear! Looks "random"

To sign a message $\mathbf{m}$,

- hash the message $(h_1, h_2) = H(\mathbf{m})$
- fix randomly the vinegar variables

$$f_1(c_1, c_2, x_3, x_4) = c_1c_2 + c_1x_3 + c_2x_4 + x_3$$

$$f_2(c_1, c_2, x_3, x_4) = c_1x_4 + c_2x_3 + c_2x_4 + x_3$$

- Solve the linear system

$$c_1c_2 + c_1x_3 + c_2x_4 + x_3 = h_1$$

$$c_1x_4 + c_2x_3 + c_2x_4 + x_3 = h_2$$

- The solution is (c_3, c_4) (*-repeat if no solution)
- The signature is $\sigma = (s_1, s_2, s_3, s_4) = \mathcal{S}^{-1}(c_1, c_2, c_3, c_4)$

UOV baby example

Central map $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

Vinegar variables x_1, x_2 & Oil variables x_3, x_4

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4 + x_3$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3$$

Linear $\mathcal{S} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

Public map $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

$$\begin{aligned} p_1(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_4 \\ p_2(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_4 + x_3x_4 + x_1 + x_4 \end{aligned}$$

All monomials appear! Looks "random"

To sign a message $\mathbf{m}$,

- hash the message $(h_1, h_2) = H(\mathbf{m})$
- fix randomly the vinegar variables

$$f_1(c_1, c_2, x_3, x_4) = c_1c_2 + c_1x_3 + c_2x_4 + x_3$$

$$f_2(c_1, c_2, x_3, x_4) = c_1x_4 + c_2x_3 + c_2x_4 + x_3$$

- Solve the linear system

$$c_1c_2 + c_1x_3 + c_2x_4 + x_3 = h_1$$

$$c_1x_4 + c_2x_3 + c_2x_4 + x_3 = h_2$$

- The solution is (c_3, c_4) (*-repeat if no solution)
- The signature is $\sigma = (s_1, s_2, s_3, s_4) = \mathcal{S}^{-1}(c_1, c_2, c_3, c_4)$

UOV baby example

Central map $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

Vinegar variables x_1, x_2 & Oil variables x_3, x_4

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4 + x_3$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3$$

Linear $\mathcal{S} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

Public map $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

$$p_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_4$$

$$p_2(x_1, x_2, x_3, x_4) = x_1x_3 + x_2x_4 + x_3x_4 + x_1 + x_4$$

All monomials appear! Looks "random"

To sign a message $\mathbf{m}$,

- hash the message $(h_1, h_2) = H(\mathbf{m})$
- fix randomly the vinegar variables

$$f_1(c_1, c_2, x_3, x_4) = c_1c_2 + c_1x_3 + c_2x_4 + x_3$$

$$f_2(c_1, c_2, x_3, x_4) = c_1x_4 + c_2x_3 + c_2x_4 + x_3$$

- Solve the linear system

$$c_1c_2 + c_1x_3 + c_2x_4 + x_3 = h_1$$

$$c_1x_4 + c_2x_3 + c_2x_4 + x_3 = h_2$$

- The solution is (c_3, c_4) (*-repeat if no solution)
- The signature is $\sigma = (s_1, s_2, s_3, s_4) = \mathcal{S}^{-1}(c_1, c_2, c_3, c_4)$

UOV baby example

Central map $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

Vinegar variables x_1, x_2 & Oil variables x_3, x_4

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4 + x_3$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3$$

Linear $\mathcal{S} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

Public map $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

$$\begin{aligned} p_1(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_4 \\ p_2(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_4 + x_3x_4 + x_1 + x_4 \end{aligned}$$

All monomials appear! Looks "random"

To sign a message $\mathbf{m}$,

- hash the message $(h_1, h_2) = H(\mathbf{m})$
- fix randomly the vinegar variables

$$f_1(c_1, c_2, x_3, x_4) = c_1c_2 + c_1x_3 + c_2x_4 + x_3$$

$$f_2(c_1, c_2, x_3, x_4) = c_1x_4 + c_2x_3 + c_2x_4 + x_3$$

- Solve the linear system

$$c_1c_2 + c_1x_3 + c_2x_4 + x_3 = h_1$$

$$c_1x_4 + c_2x_3 + c_2x_4 + x_3 = h_2$$

- The solution is (c_3, c_4) (*-repeat if no solution)
- The signature is $\sigma = (s_1, s_2, s_3, s_4) = \mathcal{S}^{-1}(c_1, c_2, c_3, c_4)$

UOV baby example

Central map $\mathcal{F} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

Vinegar variables x_1, x_2 & Oil variables x_3, x_4

$$f_1(x_1, x_2, x_3, x_4) = x_1x_2 + x_1x_3 + x_2x_4 + x_3$$

$$f_2(x_1, x_2, x_3, x_4) = x_1x_4 + x_2x_3 + x_2x_4 + x_3$$

Linear $\mathcal{S} = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

Public map $\mathcal{P} = \mathcal{F} \circ \mathcal{S} : \mathbb{F}_2^4 \to \mathbb{F}_2^2$

$$\begin{aligned} p_1(x_1, x_2, x_3, x_4) &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_4 \\ p_2(x_1, x_2, x_3, x_4) &= x_1x_3 + x_2x_4 + x_3x_4 + x_1 + x_4 \end{aligned}$$

All monomials appear! Looks “random”

To sign a message $\mathbf{m}$,

- hash the message $(h_1, h_2) = H(\mathbf{m})$
- fix randomly the vinegar variables

$$f_1(c_1, c_2, x_3, x_4) = c_1c_2 + c_1x_3 + c_2x_4 + x_3$$

$$f_2(c_1, c_2, x_3, x_4) = c_1x_4 + c_2x_3 + c_2x_4 + x_3$$

- Solve the linear system

$$c_1c_2 + c_1x_3 + c_2x_4 + x_3 = h_1$$

$$c_1x_4 + c_2x_3 + c_2x_4 + x_3 = h_2$$

- The solution is (c_3, c_4) (*-repeat if no solution)
- The signature is $\sigma = (s_1, s_2, s_3, s_4) = \mathcal{S}^{-1}(c_1, c_2, c_3, c_4)$

Multivariate signatures – Rainbow

- In UOV, it should hold $v \approx 3o$, otherwise not secure
- big overhead in size of keys and signature
- Rainbow - proposed by Ding & Schmidt '04 as a more efficient variant of UOV
- **Rainbow = Layered UOV** (typically, two layers of UOV)
- The central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^{n-v_1}$ is $\mathcal{F}(x_1, \dots, x_n) = (f_{v_1+1}(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V_\ell \\ i \le j}} \alpha_{ij}{}^{(s)} x_i x_j + \sum_{\substack{i \in V_\ell \\ j \in O_\ell}} \beta_{ij}{}^{(s)} x_i x_j, \quad \text{for} \quad s \in O_\ell$$

  - $O_0 = \emptyset,\ V_1 = \{1, 2, \dots, v_1\},\ O_1 = \{v_1 + 1, \dots, v_2\},\ V_2 = \{1, \dots, v_2\},\ O_2 = \{v_2 + 1, \dots, n\}$
- In matrix form, for parameters $v_1 = |V_1| = 18, o_1 = |O_1| = 12, o_2 = |O_2| = 12$

$\bar{\mathbf{F}}^{(1)}, \dots, \bar{\mathbf{F}}^{(12)}$ $\quad\quad$ $\bar{\mathbf{F}}^{(13)}, \dots, \bar{\mathbf{F}}^{(24)}$

Multivariate signatures – Rainbow

- In UOV, it should hold $v \approx 3o$, otherwise not secure
- big overhead in size of keys and signature
- Rainbow - proposed by Ding & Schmidt '04 as a more efficient variant of UOV
- **Rainbow = Layered UOV** (typically, two layers of UOV)
- The central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^{n-v_1}$ is $\mathcal{F}(x_1, \dots, x_n) = (f_{v_1+1}(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V_\ell \\ i \le j}} {\alpha_{ij}}^{(s)} x_i x_j + \sum_{\substack{i \in V_\ell \\ j \in O_\ell}} {\beta_{ij}}^{(s)} x_i x_j, \quad \text{for} \quad s \in O_\ell$$

  - $O_0 = \emptyset,\ V_1 = \{1, 2, \dots, v_1\},\ O_1 = \{v_1 + 1, \dots, v_2\},\ V_2 = \{1, \dots, v_2\},\ O_2 = \{v_2 + 1, \dots, n\}$
- In matrix form, for parameters $v_1 = |V_1| = 18, o_1 = |O_1| = 12, o_2 = |O_2| = 12$

$\bar{\mathbf{F}}^{(1)}, \dots, \bar{\mathbf{F}}^{(12)}$ $\mathbf{F}^{(\bar{1}3)}, \dots, \bar{\mathbf{F}}^{(24)}$

Multivariate signatures – Rainbow

- In UOV, it should hold $v \approx 3o$, otherwise not secure
- big overhead in size of keys and signature
- Rainbow - proposed by Ding & Schmidt '04 as a more efficient variant of UOV
- **Rainbow = Layered UOV** (typically, two layers of UOV)
- The central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^{n-v_1}$ is $\mathcal{F}(x_1, \dots, x_n) = (f_{v_1+1}(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V_\ell \\ i \le j}} \alpha_{ij}{}^{(s)} x_i x_j + \sum_{\substack{i \in V_\ell \\ j \in O_\ell}} \beta_{ij}{}^{(s)} x_i x_j, \quad \text{for} \quad s \in O_\ell$$

  - $O_0 = \emptyset,\ V_1 = \{1, 2, \dots, v_1\},\ O_1 = \{v_1 + 1, \dots, v_2\},\ V_2 = \{1, \dots, v_2\},\ O_2 = \{v_2 + 1, \dots, n\}$
- In matrix form, for parameters $v_1 = |V_1| = 18, o_1 = |O_1| = 12, o_2 = |O_2| = 12$

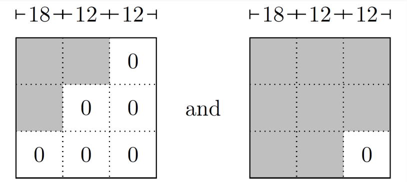
$$\bar{\mathbf{F}}^{(1)}, \dots, \bar{\mathbf{F}}^{(12)} \qquad \bar{\mathbf{F}}^{(13)}, \dots, \bar{\mathbf{F}}^{(24)}$$

Multivariate signatures – Rainbow

- In UOV, it should hold $v \approx 3o$, otherwise not secure
- big overhead in size of keys and signature
- Rainbow - proposed by Ding & Schmidt '04 as a more efficient variant of UOV
- **Rainbow = Layered UOV** (typically, two layers of UOV)
- The central map $\mathcal{F} : \mathbb{F}^n \to \mathbb{F}^{n-v_1}$ is $\mathcal{F}(x_1, \dots, x_n) = (f_{v_1+1}(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$ where

$$f^{(s)}(x) = \sum_{\substack{i,j \in V_\ell \\ i \le j}} \alpha_{ij}{}^{(s)} x_i x_j + \sum_{\substack{i \in V_\ell \\ j \in O_\ell}} \beta_{ij}{}^{(s)} x_i x_j, \quad \text{for} \quad s \in O_\ell$$

  - $O_0 = \emptyset,\ V_1 = \{1, 2, \dots, v_1\},\ O_1 = \{v_1 + 1, \dots, v_2\},\ V_2 = \{1, \dots, v_2\},\ O_2 = \{v_2 + 1, \dots, n\}$
- In matrix form, for parameters $v_1 = |V_1| = 18, o_1 = |O_1| = 12, o_2 = |O_2| = 12$



$\bar{\mathbf{F}}^{(1)}, \dots, \bar{\mathbf{F}}^{(12)}$ $\bar{\mathbf{F}}^{(13)}, \dots, \bar{\mathbf{F}}^{(24)}$

Security of UOV

- In UOV, it should hold $v \approx 3o$, otherwise not secure
  - $v = o$ - (O& V) broken using invariant subspace attack
  - $v >> o$ - easy as a function of n
  - $2o < v < 3o$ - sweet spot
- Cryptanalytical techniques ($\approx$ 15 years old)
  - Invariant subspace attack
  - Direct attack
  - Reconciliation attack
- Parameters for 128 bits security based on these attacks
  - $q = 256, n = 103, m = 44$, private key $194,7KB$, public key $235,6KB$ (plain UOV)
  - $q = 256, n = 103, m = 44$, private key $116,8KB$, public key $43,6KB$ (UOV using eq. keys)
- Beullens in 2020 - reduced the security to 95 bits!
- Current NIST level 1 security parameters (143 bits)
  - $q = 16, n = 160, m = 64$, public key $66,6KB$ (with compression)

Security of UOV

- In UOV, it should hold $v \approx 3o$, otherwise not secure
  - $v = o$ - (O& V) broken using invariant subspace attack
  - $v >> o$ - easy as a function of n
  - $2o < v < 3o$ - sweet spot
- Cryptanalytical techniques ($\approx$ 15 years old)
  - Invariant subspace attack
  - Direct attack
  - Reconciliation attack
- Parameters for 128 bits security based on these attacks
  - $q = 256, n = 103, m = 44$, private key $194,7KB$, public key $235,6KB$ (plain UOV)
  - $q = 256, n = 103, m = 44$, private key $116,8KB$, public key $43,6KB$ (UOV using eq. keys)
- Beullens in 2020 - reduced the security to 95 bits!
- Current NIST level 1 security parameters (143 bits)
  - $q = 16, n = 160, m = 64$, public key $66,6KB$ (with compression)

Security of UOV

- In UOV, it should hold $v \approx 3o$, otherwise not secure
  - $v = o$ - (O& V) broken using invariant subspace attack
  - $v >> o$ - easy as a function of n
  - $2o < v < 3o$ - sweet spot
- Cryptanalytical techniques ($\approx$ 15 years old)
  - Invariant subspace attack
  - Direct attack
  - Reconciliation attack
- Parameters for 128 bits security based on these attacks
  - $q = 256, n = 103, m = 44$, private key $194,7KB$, public key $235,6KB$ (plain UOV)
  - $q = 256, n = 103, m = 44$, private key $116,8KB$, public key $43,6KB$ (UOV using eq. keys)
- Beullens in 2020 - reduced the security to 95 bits!
- Current NIST level 1 security parameters (143 bits)
  - $q = 16, n = 160, m = 64$, public key $66,6KB$ (with compression)

Security of UOV

- In UOV, it should hold $v \approx 3o$, otherwise not secure
  - $v = o$ - (O& V) broken using invariant subspace attack
  - $v >> o$ - easy as a function of n
  - $2o < v < 3o$ - sweet spot
- Cryptanalytical techniques ($\approx$ 15 years old)
  - Invariant subspace attack
  - Direct attack
  - Reconciliation attack
- Parameters for 128 bits security based on these attacks
  - $q = 256, n = 103, m = 44$, private key $194,7KB$, public key $235,6KB$ (plain UOV)
  - $q = 256, n = 103, m = 44$, private key $116,8KB$, public key $43,6KB$ (UOV using eq. keys)
- Beullens in 2020 - reduced the security to 95 bits!
- Current NIST level 1 security parameters (143 bits)
  - $q = 16, n = 160, m = 64$, public key $66,6KB$ (with compression)

Security of UOV

- In UOV, it should hold $v \approx 3o$, otherwise not secure
  - $v = o$ - (O& V) broken using invariant subspace attack
  - $v >> o$ - easy as a function of n
  - $2o < v < 3o$ - sweet spot
- Cryptanalytical techniques ($\approx$ 15 years old)
  - Invariant subspace attack
  - Direct attack
  - Reconciliation attack
- Parameters for 128 bits security based on these attacks
  - $q = 256, n = 103, m = 44$, private key $194,7KB$, public key $235,6KB$ (plain UOV)
  - $q = 256, n = 103, m = 44$, private key $116,8KB$, public key $43,6KB$ (UOV using eq. keys)
- Beullens in 2020 - reduced the security to 95 bits!
- Current NIST level 1 security parameters (143 bits)
  - $q = 16, n = 160, m = 64$, public key $66,6KB$ (with compression)

Security of Rainbow

- **All attacks from UOV plus more!**
- Specific cryptanalytical techniques ($\approx$ 10 years old)
  - MinRank and HighRank
  - Rainbow band separation attack
- **NIST finalist, security believed to be well understood**
- Submitted NIST level 1 security parameters
  - $(GF(16), 32, 32, 32)$, $q = 16, n = 96, m = 64$, private key $97.9KB$, public key $148.5KB$, signature 64 bytes
- Beullens in 2020 - reduced the security to 123 bits!
- Beullens in 2022 - breaks practically this parameters set (61 bits of security)
- Can be fixed, but not competitive to UOV any more!

Security of Rainbow

- **All attacks from UOV plus more!**
- Specific cryptanalytical techniques ($\approx$ 10 years old)
  - MinRank and HighRank
  - Rainbow band separation attack
- **NIST finalist, security believed to be well understood**
- Submitted NIST level 1 security parameters
  - $(GF(16), 32, 32, 32)$, $q = 16, n = 96, m = 64$, private key $97.9KB$, public key $148.5KB$, signature 64 bytes
- Beullens in 2020 - reduced the security to 123 bits!
- Beullens in 2022 - breaks practically this parameters set (61 bits of security)
- Can be fixed, but not competitive to UOV any more!

Security of Rainbow

- **All attacks from UOV plus more!**
- Specific cryptanalytical techniques ($\approx$ 10 years old)
  - MinRank and HighRank
  - Rainbow band separation attack
- **NIST finalist, security believed to be well understood**
- Submitted NIST level 1 security parameters
  - $(GF(16), 32, 32, 32)$, $q = 16, n = 96, m = 64$, private key $97.9KB$, public key $148.5KB$, signature 64 bytes
- Beullens in 2020 - reduced the security to 123 bits!
- Beullens in 2022 - breaks practically this parameters set (61 bits of security)
- Can be fixed, but not competitive to UOV any more!

Security of Rainbow

- **All attacks from UOV plus more!**
- Specific cryptanalytical techniques ($\approx$ 10 years old)
  - MinRank and HighRank
  - Rainbow band separation attack
- **NIST finalist, security believed to be well understood**
- Submitted NIST level 1 security parameters
  - $(GF(16), 32, 32, 32)$, $q = 16, n = 96, m = 64$, private key $97.9KB$, public key $148.5KB$, signature 64 bytes
- Beullens in 2020 - reduced the security to 123 bits!
- Beullens in 2022 - breaks practically this parameters set (61 bits of security)
- Can be fixed, but not competitive to UOV any more!

Security of Rainbow

- **All attacks from UOV plus more!**
- Specific cryptanalytical techniques ($\approx$ 10 years old)
  - MinRank and HighRank
  - Rainbow band separation attack
- **NIST finalist, security believed to be well understood**
- Submitted NIST level 1 security parameters
  - $(GF(16), 32, 32, 32)$, $q = 16, n = 96, m = 64$, private key $97.9KB$, public key $148.5KB$, signature 64 bytes
- Beullens in 2020 - reduced the security to 123 bits!
- Beullens in 2022 - breaks practically this parameters set (61 bits of security)
- Can be fixed, but not competitive to UOV any more!

Security of Rainbow

- **All attacks from UOV plus more!**
- Specific cryptanalytical techniques ($\approx$ 10 years old)
  - MinRank and HighRank
  - Rainbow band separation attack
- **NIST finalist, security believed to be well understood**
- Submitted NIST level 1 security parameters
  - $(GF(16), 32, 32, 32)$, $q = 16, n = 96, m = 64$, private key $97.9KB$, public key $148.5KB$, signature 64 bytes
- Beullens in 2020 - reduced the security to 123 bits!
- Beullens in 2022 - breaks practically this parameters set (61 bits of security)
- Can be fixed, but not competitive to UOV any more!

Security of Rainbow

- **All attacks from UOV plus more!**
- Specific cryptanalytical techniques ($\approx$ 10 years old)
  - MinRank and HighRank
  - Rainbow band separation attack
- **NIST finalist, security believed to be well understood**
- Submitted NIST level 1 security parameters
  - $(GF(16), 32, 32, 32)$, $q = 16, n = 96, m = 64$, private key $97.9KB$, public key $148.5KB$, signature 64 bytes
- Beullens in 2020 - reduced the security to 123 bits!
- Beullens in 2022 - breaks practically this parameters set (61 bits of security)
- Can be fixed, but not competitive to UOV any more!

Summary

Today:

- Multivariate signatures - classic designs

Tomorrow:

- Key size optimization techniques
- Solving the MQ problem

Summary

Today:

- Multivariate signatures - classic designs

Tomorrow:

- Key size optimization techniques
- Solving the MQ problem