Latest Developments in Rainbow Cryptanalysis

Giovanni Tognolini

University of Trento

May, 2022

Index

Main objects of multivariate cryptography

$$p(x_1, ..., x_n) = \sum_{i=1}^{n} \sum_{j=1}^{n} p_{ij} \cdot x_i x_j + \sum_{i=1}^{n} p_i \cdot x_i + p_0$$

Why are these polynomials so important?

Given m multivariate quadratic polynomials

$$\mathcal{P}(x) := \begin{pmatrix} p^{(1)}(x) \\ \vdots \\ p^{(m)}(x) \end{pmatrix}$$

it is difficult to solve the system $\mathcal{P}(x) = y$.

$$\downarrow$$

It is a good starting point to construct cryptosystems!

How do we construct cryptosystems?

We take an easily invertible quadratic map $\mathcal{F} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$
To hide its structure, we hide it with two invertible affine maps
$\mathcal{S} : \mathbb{F}_q^m \longrightarrow \mathbb{F}_q^m$ and $\mathcal{T} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n$.

$$\text{PK} : (\mathcal{P} := \mathcal{S} \circ \mathcal{F} \circ \mathcal{T})$$
$$\text{SK} : (\mathcal{S}, \mathcal{F}, \mathcal{T})$$

$$h(m) \in \mathbb{F}_q^m \xrightarrow{\mathcal{S}^{-1}} x \in \mathbb{F}_q^m \xrightarrow{\mathcal{F}^{-1}} y \in \mathbb{F}_q^n \xrightarrow{\mathcal{T}^{-1}} z \in \mathbb{F}_q^n$$
$$z \in \mathbb{F}_q^n \xrightarrow{\mathcal{P}} h(m) \in \mathbb{F}_q^m$$

Two famous multivariate cryptosystems: (U)OV and Rainbow

(U)OV traditional description

Idea

We contruct an easily invertible $\mathcal{F}$ and hide its structure.

- Consider a finite field $\mathbb{F}_q$.
- Let $v, o \in \mathbb{Z}$ and define $n := v + o$.
- Let $V := \{1, ..., v\}$ and $O := \{v + 1, ..., n\}$.
  We will call $x_1, ..., x_v$ the vinegar variables, and $x_{v+1}, ..., x_n$ the oil variable.
- The central map $\mathcal{F} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^o$ consists of o quadratic polynomials of the form

$$f^{(k)} = \sum_{i,j \in V} \alpha_{i,j}^{(k)} x_i x_j + \sum_{i \in V, j \in O} \beta_{i,j}^{(k)} x_i x_j$$

Observation

$f^{(k)}$ contains no quadratic terms $x_i x_j$ with both $i, j \in O$.

How to invert $\mathcal{F}$

Example

- $\mathbb{F} = \mathbb{F}_7$.
- $o = v = 2 \quad (\longrightarrow OV)$
- Let $\mathcal{F}$ be given by

$$f^{(1)}(x_1, ..., x_4) = 2x_1^2 + 3x_1x_2 + 6x_1x_3 + x_1x_4 + 4x_2^2 + 5x_2x_4$$
$$f^{(2)}(x_1, ..., x_4) = 3x_1^2 + 6x_1x_2 + 5x_1x_4 + 3x_2^2 + 5x_2x_3 + x_2x_4$$

$$\downarrow$$

Suppose we want to find a preimage of $(3, 4)$.

$$\downarrow$$

We proceed as follows

1. Choose random value for the vinegar variables, e.g. $(x_1, x_2) = (1, 4)$.
2. Substitute them into $f^{(1)}$ and $f^{(2)}$:

$$f^{(1)}\Big|_{(1,4)} = 6x_3 + 1$$
$$f^{(2)}\Big|_{(1,4)} = 5 + 2x_4 - x_3$$

3. Solve the *linear* system. We obtain $(x_3, x_4) = (5, 2)$

$$\downarrow$$

The required preimage is $x = (1, 4, 5, 2)$.

(U)OV alternative description

- The public key is a multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$ which vanishes on a secret linear subspace O of dimension m.
- The private key is a description of O.

$$
\begin{array}{ccc}
\mathbb{F}_q^n & \hookleftarrow & O \\
\downarrow \mathcal{P} & & \downarrow \mathcal{P} \\
\mathbb{F}_q^m & \hookleftarrow & \{0\}
\end{array}
$$

How to generate a public key?

- Pick the subspace O uniformly at random.
- Pick $\mathcal{P}$ uniformly at random.

Before finding preimages...

Observation (Polar form of $\mathcal{F}$)

Given a multivariate quadratic polynomial $p(x)$ we can define its *polar form*

$$p'(x, y) := p(x + y) - p(x) - p(y) + p(0)$$

Similarly, given m multivariate quadratic polynomials, we define

$$\mathcal{P}'(x, y) := \begin{pmatrix} p'_1(x, y) \\ \vdots \\ p'_m(x, y) \end{pmatrix}$$

$\mathcal{P}'(x, y)$ is a simmetric and bilinear map.

Finding preimages

Suppose we want to find a preimage for $t \in \mathbb{F}_q^m$.

- Pick $v \in \mathbb{F}_q^n$ randomly.
- Solve $\mathcal{P}(v+o) = t$ for $o \in O$.

Observation (This is an easy task!)

Memo: $\mathcal{P}'(x,y) := \mathcal{P}(x+y) - \mathcal{P}(x) - \mathcal{P}(y)$

$$\mathcal{P}(v+o) = \mathcal{P}(v) + \mathcal{P}(o) + \mathcal{P}'(v,o) = t$$

- $\mathcal{P}(v)$ is fixed.
- $\mathcal{P}(o) = 0$.
- $\mathcal{P}'(v,o)$ is linear and it has
  - m variables.
  - m equations.

Rainbow

Is just a multi-layer version of UOV.

Advantages

- Smaller key size.
- Smaller signature size.
- Better performance.

Approaching Rainbow with an example

Example

- $\mathbb{F} = \mathbb{F}_7$.
- Let $\mathcal{F}$ be given by

$$
\begin{aligned}
f^{(1)} &= x_1^2 + 3x_1x_2 + 5x_1x_3 + 6x_1x_4 + 2x_2^2 + 6x_2x_3 + 4x_2x_4 \\
f^{(2)} &= 2x_1^2 + x_1x_2 + x_1x_3 + 3x_1x_4 + x_2^2 + x_2x_3 + 4x_2x_4 \\
f^{(3)} &= 2x_1^2 + 3x_1x_2 + 3x_1x_3 + 3x_1x_4 + x_1x_5 + 3x_1x_6 + 4x_2^2 + x_2x_3 \\
&\quad + 4x_2x_4 + x_2x_5 + 3x_2x_6 + 3x_3x_4 + x_3x_5 + 2x_3x_6 + 3x_4x_5 \\
f^{(4)} &= 2x_1^2 + 5x_1x_2 + x_1x_3 + 5x_1x_4 + 5x_1x_6 + 5x_2^2 + 3x_2x_3 + 5x_2x_5 \\
&\quad + 4x_2x_6 + 3x_3^2 + 5x_3x_4 + 4x_3x_5 + 2x_3x_6 + x_4^2 + 6x_4x_5 + 3x_4x_6
\end{aligned}
$$

$$\downarrow$$

Suppose we want to find a preimage of $(6, 2, 0, 5)$.

We proceed as follows

1. Choose random values for x_1 and x_2, e.g. $(x_1, x_2) = (0, 1)$.
2. Substitute them into $f^{(1)}, ..., f^{(4)}$:

$$f^{(1)}\Big|_{(0,1)} = 6x_3 + 5x_4 + 2$$
$$f^{(2)}\Big|_{(0,1)} = x_3 + 4x_4 + 1$$
$$f^{(3)}\Big|_{(0,1)} = 3x_4x_5 + 2x_3x_6 + x_3x_5 + 3x_3x_4 + 3x_6 + x_5 + 4x_4 + x_3 + 4$$
$$f^{(4)}\Big|_{(0,1)} = 3x_4x_6 + 6x_4x_5 + x_4^2 + 2x_3x_6 + 4x_3x_5 + 5x_3x_4 + 3x_3^2 + 4x_6 + 5x_5 + 3x_3 + 5$$

3. Solve the small *linear* system and obtain $(x_3, x_4) = (5, 6)$.

4. Substitute these values into $f^{(3)}, f^{(4)}$:

$$f^{(3)}\Big|_{(0,1,5,6)} = -4x_5 - 7x_6 - 2$$
$$f^{(4)}\Big|_{(0,1,5,6)} = -9x_5 - 3x_6 + 1$$

5. Solve the *linear* system and obtain $(x_5, x_6) = (3, 6)$

$$\downarrow$$

The required preimage is $x = (0, 1, 5, 6, 3, 6)$.

Rainbow traditional description

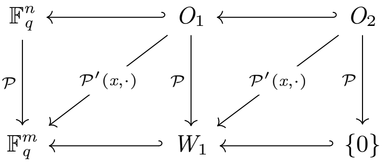
We don't really care about it here...

Rainbow alternative description

- The public key is a multivariate quadratic map $\mathcal{P} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^m$.
- The private key consists of
  - Two sequences of nested subspaces:

$$\mathbb{F}_q^n = O_0 \supseteq O_1 \supseteq O_2$$
$$\mathbb{F}_q^m = W_0 \supseteq W_1 \supseteq W_2 = \{0\}$$

  - Some constrains:
    - ★ $\dim(O_i) = \dim(W_{i-1})$.
    - ★ $\mathcal{P}(x) \in W_i$ for all $x \in O_i$.
    - ★ $\mathcal{P}'(x, y) \in W_{i-1}$ for all $x \in \mathbb{F}_q^n, y \in O_i$.



How to sign?

- Suppose we have a target $t \in \mathbb{F}_q^m$.
- Consider the UOV instance

$$
\begin{array}{ccc}
\mathbb{F}_q^n / O_2 & \hookleftarrow & O_1 / O_2 \\
\Big\downarrow \tilde{\mathcal{P}} & & \Big\downarrow \tilde{\mathcal{P}} \\
\mathbb{F}_q^m / W_1 & \hookleftarrow & \{0\}
\end{array}
$$

Observation

This is indeed an UOV instance as $\dim(O_1/O_2) = \dim(\mathbb{F}_q^m / W_1)$

Pick $[v] \in \mathbb{F}_q^n / O_2$ randomly and solve for $[o_1] \in O_1/O_2$ the system

$$\tilde{\mathcal{P}}([v] + [o_1]) = [t]$$

- Solve for $o_2 \in O_2$ the system

$$\mathcal{P}(v + o_1 + o_2) = t$$

Observation (This is an easy task!)

Memo: $\mathcal{P}'(x, y) := \mathcal{P}(x + y) - \mathcal{P}(x) - \mathcal{P}(y)$

$$\mathcal{P}((v + o_1) + o_2) = \mathcal{P}(v + o_1) + \mathcal{P}(o_2) + \mathcal{P}'(v + o_1, o_2) = t$$

- $\mathcal{P}(v + o_1)$ is fixed.
- $\mathcal{P}(o_2) = 0$.
- $\mathcal{P}'(v + o_1, o_2)$ is linear and it has
  - $\dim(O_2) = \dim(W_1)$ variables.
  - $\dim(W_1)$ equations.

Attacking Rainbow

Simple attack

Idea

0. Consider the map

$$\begin{aligned} D_x\colon \mathbb{F}_q^n &\longrightarrow \mathbb{F}_q^m \\ y &\longmapsto \mathcal{P}'(x,y) \end{aligned}.$$

1. Observe that with high probability it has an element in $O_2 \cap \ker(D_x)$.
2. Find this element.
3. Reconstruct O_2.
4. Reconstruct W.
5. Reconstruct O_1 (key recovery) or forge a signature.

1. D_x has an element in $O_2 \cap \ker(D_x)$ with high probability.

Observation

- D_x is a linear map, indeed

$$\begin{aligned} D_x(y_1 + y_2) &= \mathcal{P}'(x, y_1 + y_2) \\ &= \mathcal{P}'(x, y_1) + \mathcal{P}'(x, y_2) \\ &= D_x(y_1) + D_x(y_2). \end{aligned}$$

- $D_{x|_{O_2}} : O_2 \longrightarrow W$, indeed

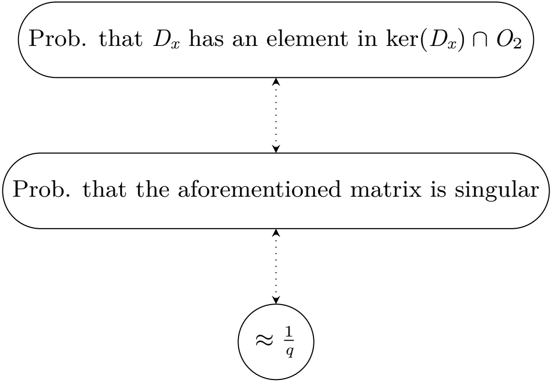
$$D_x(o) = \mathcal{P}'(x, o) \in W.$$

- $\dim(O_2) = o_2 = \dim(W)$.

Result

We can represent $D_{x|_{O_2}}$ as a square o_2-by-o_2 random matrix over $\mathbb{F}_q$.

1. D_x has an element in $O_2 \cap \ker(D_x)$ with high probability.



2. Find this element $o \in \ker(D_x) \cap O_2$.

A good idea would be to solve the system

$$\begin{cases} D_x(o) = 0 \\ \mathcal{P}(o) = 0 \end{cases}$$

Observation

- $D_x(o) = 0$ consists of m linear equations in the n variables of o.
- $\mathcal{P}(o) = 0$ consists of m homogeneous quadratic equations in the n variables of o.

We can reduce to a system of

- m homogeneous equations.
- $n - m$ variables.

2. Find this element $o \in \ker(D_x) \cap O_2$.

Concretely:

Let $B \in \mathbb{F}_q^{n\times(n-m)}$ a basis for $\ker(D_x)$.

$$\begin{cases} D_x(o) = 0 \\ \mathcal{P}(o) = 0 \end{cases} \iff \begin{cases} o \in \ker(D_x) \\ \mathcal{P}(o) = 0 \end{cases} \iff \begin{cases} o = By \\ \mathcal{P}(o) = 0 \end{cases} \iff \tilde{\mathcal{P}}(y) := \mathcal{P}(By) = 0$$

Observation

Finding $o \in \ker(D_x) \cap O_2$ reduces to find $y \in \mathbb{F}_q^{n-m}$ s.t. $\tilde{\mathcal{P}}(y) = 0$.

2. Find this element $o \in \ker(D_x) \cap O_2$.

We would like to solve $\tilde{\mathcal{P}}(y) = 0$ with the XL algorithm.

Observation

In order to apply the XL algorithm we need to be sure that the system is random.

We distinguish the cases:

- $\mathrm{ch}(\mathbb{F}_q)$ odd.
- $\mathrm{ch}(\mathbb{F}_q)$ even.

Odd characteristic

Observation

In this case $\tilde{\mathcal{P}}$ behaves like a random system.

What does it mean that it behaves like a random system?

The ranks of Macaulay matrices (at various degree D) of $\tilde{\mathcal{P}}(x) = 0$ are identical to the ranks of systems of uniformly random quadratic equations with the same dimensions.

Conclusion

If a solution to $\tilde{\mathcal{P}}(x) = 0$ exists, we can find it with XL.

Even characteristic

Observation

In this case $\tilde{\mathcal{P}}$ *does not* behave like a random system.

$$\downarrow$$

Applying the XL sometimes fails.

Why?

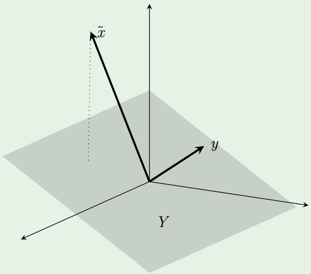
In characteristic 2 it is possible to show that there is an $\tilde{x}$ (known to the attacker) such that:

$$\tilde{\mathcal{P}}(\tilde{x} + y) = \tilde{\mathcal{P}}(\tilde{x}) + \tilde{\mathcal{P}}(y)$$

which is not something that usually happens for random $\tilde{\mathcal{P}}$.

How to solve this problem?

- Restrict $\tilde{\mathcal{P}}$ to $Y \subseteq \mathbb{F}_q^{n-m}$
  (Y is a subspace of dimension $n-m-1$ that does not contain $\tilde{x}$).
- Find $y \in Y$ s.t. $\tilde{\mathcal{P}}(y) = \alpha\tilde{\mathcal{P}}(\tilde{x})$.



Why are we looking for such an y?

In this case $\tilde{x} + \alpha^{-\frac{1}{2}} y$ is a solution to $\tilde{\mathcal{P}}(x) = 0$, indeed:

$$\begin{aligned}\tilde{\mathcal{P}}(\tilde{x} + \alpha^{-\frac{1}{2}} y) &= \tilde{\mathcal{P}}(\tilde{x}) + \tilde{\mathcal{P}}(\alpha^{-\frac{1}{2}} y) \\ &= \tilde{\mathcal{P}}(\tilde{x}) + \alpha^{-1}\tilde{\mathcal{P}}(y) \\ &= 0\end{aligned}$$

How do we find y?

$$\tilde{\mathcal{P}}(y) = \alpha\tilde{\mathcal{P}}(\tilde{x}) \iff \left\{\tilde{p}_i(y) = \alpha\tilde{p}_i(\tilde{x})\right\}_{i=1}^{m}$$
$$\iff (\star)$$

Observation

If we assume (with loss of generality) that $\tilde{p}_1(\tilde{x}) \neq 0$ then we can write

$$\alpha = \frac{\tilde{p}_1(y)}{\tilde{p}_1(\tilde{x})}$$

and we obtain

$$(\star) \iff \left\{\tilde{p}_i(y) = \frac{\tilde{p}_1(y)}{\tilde{p}_1(\tilde{x})} \cdot \tilde{p}_i(\tilde{x})\right\}_{i=2}^{m}$$
$$\iff \left\{\tilde{p}_i(y)\tilde{p}_1(\tilde{x}) - \tilde{p}_1(y)\tilde{p}_i(\tilde{x}) = 0\right\}_{i=2}^{m}$$

So...

In order to find y we restrict $\tilde{\mathcal{P}}$ to Y and solve the previous system.

Result

The new system

$$\left\{\tilde{p}_i(y)\tilde{p}_1(\tilde{x}) - \tilde{p}_1(y)\tilde{p}_i(\tilde{x}) = 0\right\}_{i=2}^{m}$$

is a system of

- $m - 1$ homogeneous quadratic equations.
- $n - m - 1$ variables.

and it behaves like a random system.

Conclusion

If a solution exists, we can find it with XL.

At this point we managed to find an element $o \in O_2$.

$\downarrow$

It is now easy to recover O_2 and W.

Recovering W

Observation

Given a single vector $o \in O_2$, we can compute

$$\langle \mathcal{P}'(o, e_1), ..., \mathcal{P}'(o, e_n) \rangle \subseteq W$$

which will be (with overwhelming probability) an equality.

Recovering O_2

- Let V a change of variables which sends W to the last o_2 coordinates of $\mathbb{F}_q^m$.

$$\begin{aligned} V\colon \quad \mathbb{F}_q^m &\longrightarrow \mathbb{F}_q^m \\ w \in W &\longmapsto (0,0,\dots,0,\star,\dots,\star)^T \end{aligned}$$

- We can split up $V \circ \mathcal{P}$ as

$$V \circ \mathcal{P}(x) = \begin{cases} \mathcal{P}_1(x) & \longleftarrow \text{ first } m - o_2 \text{ coordinates} \\ \mathcal{P}_2(x) & \longleftarrow \text{ last } o_2 \text{ coordinates} \end{cases}$$

Observation

With very high probability

$$O_2 = \ker\left(x \mapsto \begin{pmatrix} \mathcal{P}_1'(e_1, x) \\ \vdots \\ \mathcal{P}_1'(e_n, x) \end{pmatrix} \right)$$

- "$\subseteq$" is clear: $o \in O_2 \implies \mathcal{P}_1'(e_i, o) = V \circ \mathcal{P}'(e_i, o)\big|_{m-o_2} = 0.$
- "$=$" is very likely.

We can reduce Rainbow to
a UOV instance with parameters
$n' = n - o_2$
$m' = m - o_2$.

An old slide: How to sign?

- We had a target $t \in \mathbb{F}_q^m$.
- We considered the UOV instance

$$\begin{array}{ccc} \mathbb{F}_q^n/O_2 & \hookleftarrow & O_1/O_2 \\ \downarrow \tilde{\mathcal{P}} & & \downarrow \tilde{\mathcal{P}} \\ \mathbb{F}_q^m/W_1 & \hookleftarrow & \{0\} \end{array}$$

  We picked $[v] \in \mathbb{F}_q^n/O_2$ randomly and solved for $[o_1] \in O_1/O_2$ the system

$$\tilde{\mathcal{P}}([v] + [o_1]) = [t]$$

- We solved for $o_2 \in O_2$ the system

$$\mathcal{P}(v + o_1 + o_2) = t$$

These are easy tasks!

Concluding the Simple attack

Two ways to force the first step:

1. Recover O_1 (full key recovery).
2. Forge the signature.

Observation

- SL1 parameter sets of 2° and 3° round NIST submission:
  - $(n', m') = (64, 32)$
  - $(n', m') = (68, 32)$

  $\rightarrow$ Key recovery with Kipnis-Shamir attack $(q^{n'-2m'} \cdot \text{poly}(n))$
- SL3 and 5
  - (n', m') is too big for a full key recovery

  $\rightarrow$ We can find a preimage for a UOV instance with XL.

Performance on NIST parameters sets

Parameter set		(q, n, m, o_2)	Simple attack	Known attacks
(2°)	SL1	(16,96,64,32)	61^*	123
	SL3	(256, 140, 72, 36)	186	151
	SL5	(256, 188, 96, 48)	246	191
(3°)	SL1	(16, 100, 64, 32)	69^*	127
	SL3	(256, 148, 80, 48)	160	177
	SL5	(256, 196, 100, 64)	257	226

We can try to combine the simple attack with some known attack

Rectangular MinRank Attack

Rectangular MinRank Problem

An instance of this problem is:

- a list of matrices $L_1, ..., L_k$.
- a target rank r.

The task is to find a non-zero linear combination of the matrices whose rank is at most r.

Consider the n matrices

$$L_i := \begin{pmatrix} \mathcal{P}'(e_1, e_i) \\ \vdots \\ \mathcal{P}'(e_n, e_i) \end{pmatrix}$$

Observation

- Since $\mathcal{P}$ is bilinear

$$\forall\ x \in \mathbb{F}_q^n \qquad \sum_{i=1}^{n} x_i L_i = \begin{pmatrix} \mathcal{P}'(e_1, x) \\ \vdots \\ \mathcal{P}'(e_n, x) \end{pmatrix}$$

- Furthermore

$$o \in O_2 \implies \mathcal{P}'(e_i, o) \in W$$
$$\implies \operatorname{rank}(\sum o_i L_i) \leq \dim W$$

So...

We have n matrices $\{L_i\}_{i=1}^n$

We know there exists an x s.t. $\operatorname{rank}(\sum x_i L_i) \leq \dim W$

$\downarrow$

This is an instance of the MinRank problem!

$\downarrow$

We can use known algorithm to solve this problem

(if o is a solution, then with overwhelming prob. $o \in O_2$)

Observation

As before, once a solution $o \in O_2$ is found, the security of Rainbow is reduced to the security of a UOV instance with

$$\begin{cases} n' = n - o_2 \\ m' = m - o_2 \end{cases}$$

Combination of previous attacks

The idea is to solve (for $o \in \mathbb{F}_q^n$)

$$\text{minRank on } \sum o_i L_i$$

but since we expect to have $o \in O_2$, we add the constrain

$$o \in \ker(D_x)$$

for a random $x \in \mathbb{F}_q^n$.

Why?

$\ker(D_x) \cap O_2 \neq \{0\}$ with prob. $\approx \frac{1}{q}$.

CONS

We have to repeat the attack on average approx. q times.

PROS

Now we have a minRank problem with only $n - m$ matrices (definitely less than the original minRank problem).

Performance on NIST parameters sets

Parameter set		(q, n, m, o_2)	Combined attack	Known attacks
(2°)	SL1	(16,96,64,32)	93^*	123
	SL3	(256, 140, 72, 36)	131	151
	SL5	(256, 188, 96, 48)	164	191
(3°)	SL1	(16, 100, 64, 32)	99^*	127
	SL3	(256, 148, 80, 48)	157	177
	SL5	(256, 196, 100, 64)	206	226

Conclusions

We could move to larger parameters, BUT:

1. The new signature and public keys would be very big.
2. These seems to be room for improvement for attacks.
3. The resulting Rainbow scheme would be less efficient than UOV.

$\downarrow$

There is no reason to prefer Rainbow over UOV, since:

- Rainbow is based on UOV.
- UOV is older.
- UOV is simpler.
- UOV has a smaller attack surface.


Questions?

Bibliography

- Beullens, Ward. “Breaking Rainbow Takes a Weekend on a Laptop.” Cryptology ePrint Archive (2022).
- Beullens, Ward. “Improved cryptanalysis of UOV and rainbow.” Annual International Conference on the Theory and Applications of Cryptographic Techniques. Springer, Cham, 2021.
- Ding, Jintai, and Albrecht Petzoldt. “Current state of multivariate cryptography.” IEEE Security & Privacy 15.4 (2017): 28-36.
- Ding, Jintai, and Dieter Schmidt. “Rainbow, a new multivariable polynomial signature scheme.” International conference on applied cryptography and network security. Springer, Berlin, Heidelberg, 2005.

XL

We would like to solve $\tilde{\mathcal{P}}(y) = 0$ with the XL algorithm.

Memo: XL algorithm

It solves an instance with m random homogeneous equations in n variables at the cost of

$$3\binom{n-1+D}{D}^2\binom{n+1}{2}$$

field multiplication, where D is the operating degree of XL.

Observation

D is the smallest integer such that the coefficient of the t^D term in the power expansion of

$$\frac{(1-t^2)^m}{(1-t)^n}$$

is non positive.

XL

Example

Suppose we want to find a solution to a system of 63 random homogeneous quadratic equations in 31 variables. We have:

$$\frac{(1-t^2)^{63}}{(1-t)^{31}} = 1 + 31t + 433t^2 + 3503t^3 + 17081t^4 + 41447t^5 - 44919t^6 + O(t^7)$$

so we can run XL at degree $D = 6$, with an estimated cost of

$$3\binom{31-1+6}{6}^2\binom{31+1}{2} \approx 2^{52.3}$$

field multiplications.