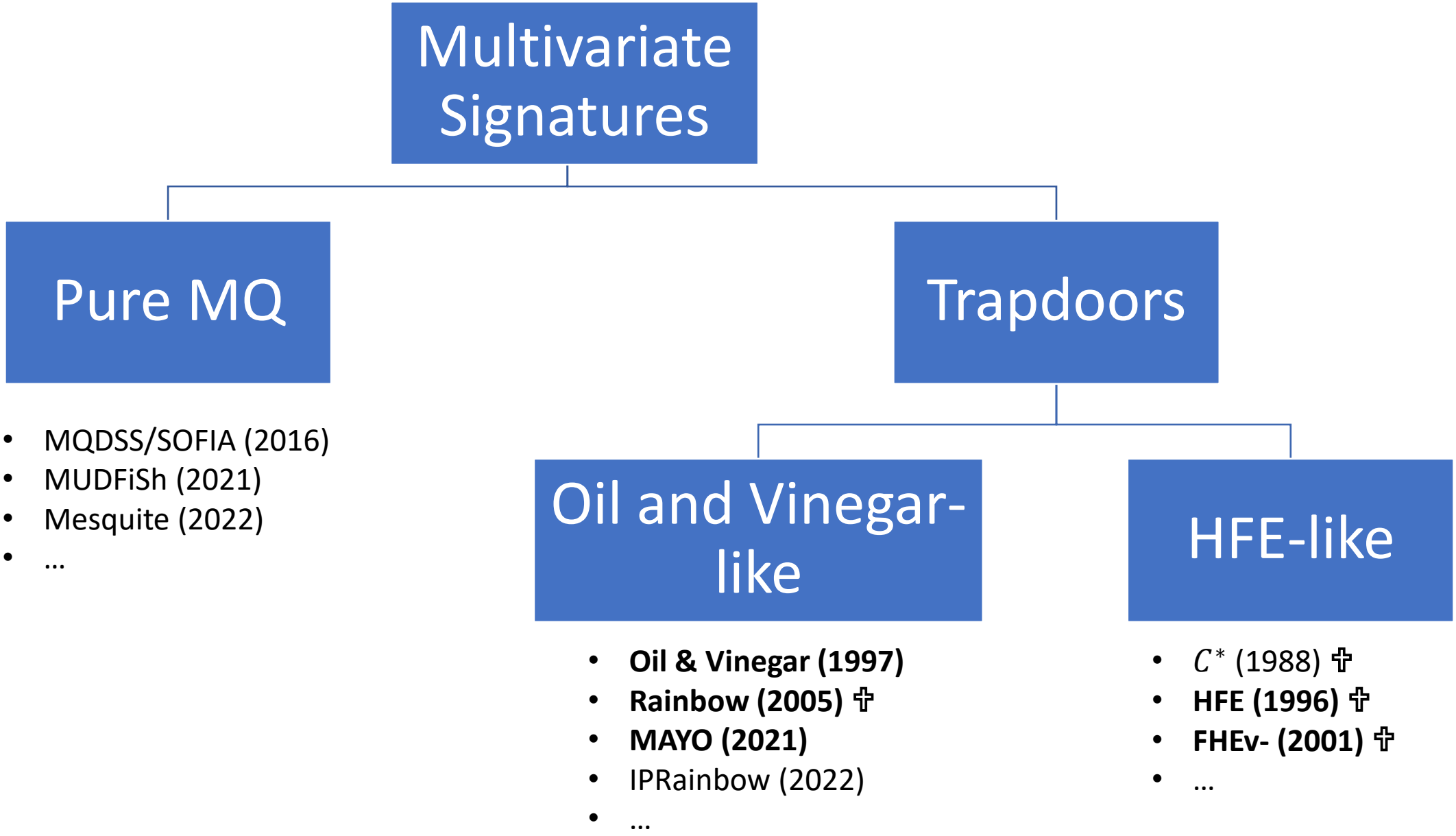
Breaking Rainbow takes a weekend on a Laptop

Ward Beullens
IBM Research Europe
Crypto 2022

~~Breaking Rainbow takes a weekend on a Laptop~~

A (biased) overview of MQ Signatures

Ward Beullens
IBM Research Europe
Crypto 2022


Multivariate Signatures
Pure MQ
Trapdoors
Oil and Vinegar-like
HFE-like
MQDSS/SOFIA (2016)
MUDFiSh (2021)
Mesquite (2022)
…
Oil & Vinegar (1997)
Rainbow (2005) ✞
MAYO (2021)
IPRainbow (2022)
…
C^* (1988) ✞
HFE (1996) ✞
FHEv- (2001) ✞
…

Overview

Oil & vinegar

Rainbow

MAYO

Multivariate Trapdoors

Public key is multivariate quadratic map $P = (p_1(x), \dots, p_m(x)) \colon \mathbb{F}_q^n \to \mathbb{F}_q^m$

$$\begin{cases} p_1(x) = 2\,x_1^2 + x_1x_2 + 6\,x_1x_3 + x_3^2 \ \ mod\ 7 \\ p_2(x) = 5x_1^2 + 2x_1x_2 + x_2^2 + 6x_2x_3 \ mod\ 7 \\ p_3(x) = 4x_1^2 + x_1x_2 + 3x_2^2 + 4x_2x_3 \ mod\ 7 \end{cases}$$

P is supposed to look random ⟹ Sampling preimages for P is hard.

But, there is hidden structure in P which allows to solve $P(x) = y$ for x.

Trapdoor signatures

Public key: $P = (p_1(x), \ldots, p_m(x)) : \mathbb{F}_q^n \to \mathbb{F}_q^m$

Secret key: trapdoor information

Signature for message m:

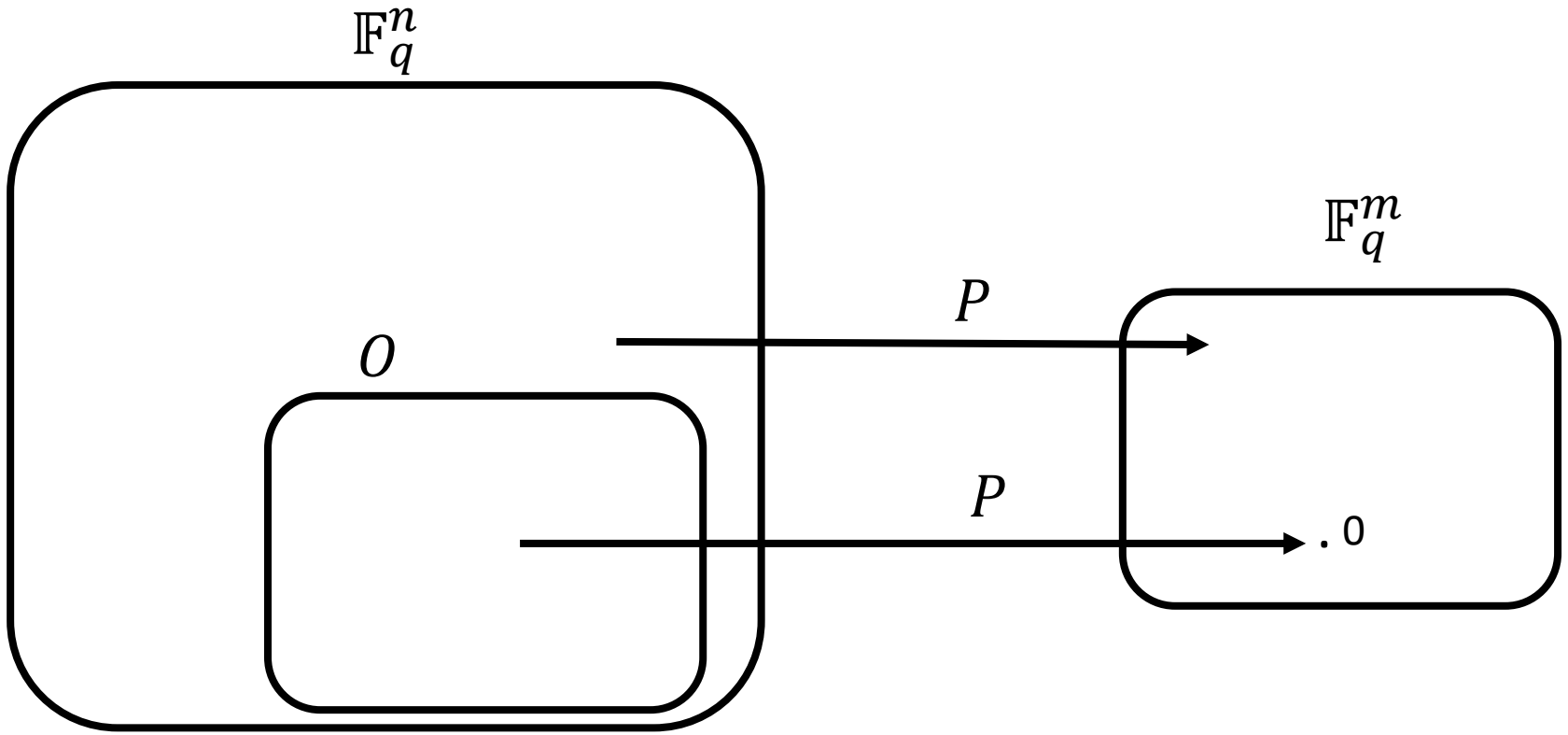
x s.t. $P(x) = H(m)$

How to trapdoor a MQ map?

Oil & Vinegar Trapdoor as presented in [Beu21]

Public key is a quadratic map: $P = (p_1(x), \dots, p_m(x)) : \mathbb{F}_q^n \to \mathbb{F}_q^m$

Trapdoor is a subspaces $O \subset \mathbb{F}_q^n$ of dimension m on which P vanishes.



Definition of differential:

Let $P: \mathbb{F}_q^n \to \mathbb{F}_q^m$, then we define it's differential at x as:

$$D_x: \mathbb{F}_q^n \to \mathbb{F}_q^m : y \mapsto P(x+y) - P(x) - P(y)$$

This is bi-linear in x and y:

$$D_{x+x'}(y) = D_x(y) + D_{x'}(y)$$

$$D_x(y+y') = D_x(y) + D_x(y')$$

Using the trapdoor O

Given $P: \mathbb{F}_q^n \to \mathbb{F}_q^m, O, y \in \mathbb{F}_q^m$. We want to find x s.t. $P(x) = y$.

1. Pick $v \in \mathbb{F}_q^n$ uniformly at random.
2. Solve for $o \in O$ s.t. $P(v + o) = y$.

$$P(v + o) = P(v) + P(o) + D_v(o) = y$$

Is a linear system of m equations in m variables.

If no solution, retry with different v.

Example parameters (NIST SL 1)

2 constraints:

- Finding oil space O should be hard
- It should be hard to solve $P(x) = H(M)$ without O

Attacks:

$O(q^{n-2m})$ [KS1998]

$O(2^{cn})$

# Variables	160	112
# Equations	64	44
Finite Field	GF(16)	GF(256)
Pk size	66 KB	43 KB
Signature size	96 B	128 B

Overview

Oil & vinegar

Rainbow

MAYO

History of Rainbow

1997 Oil & Vinegar [Patarin]

2005 Rainbow [Ding, Schmidt]

2008 First wave of cryptanalysis dries up [KS98,BC05,BG06, DYCCC08,…]

2017 NIST PQC

’20-’21 Improved MinRank attacks, RBS [BBCGPSTV20,BBBGNRT20,BBCPSV21, PS20,NIWDR20]

2021 Rainbow is one of signature finalists.

2021 New description of Rainbow, new attacks [Beu21]

2022 Practical break [Beu22]

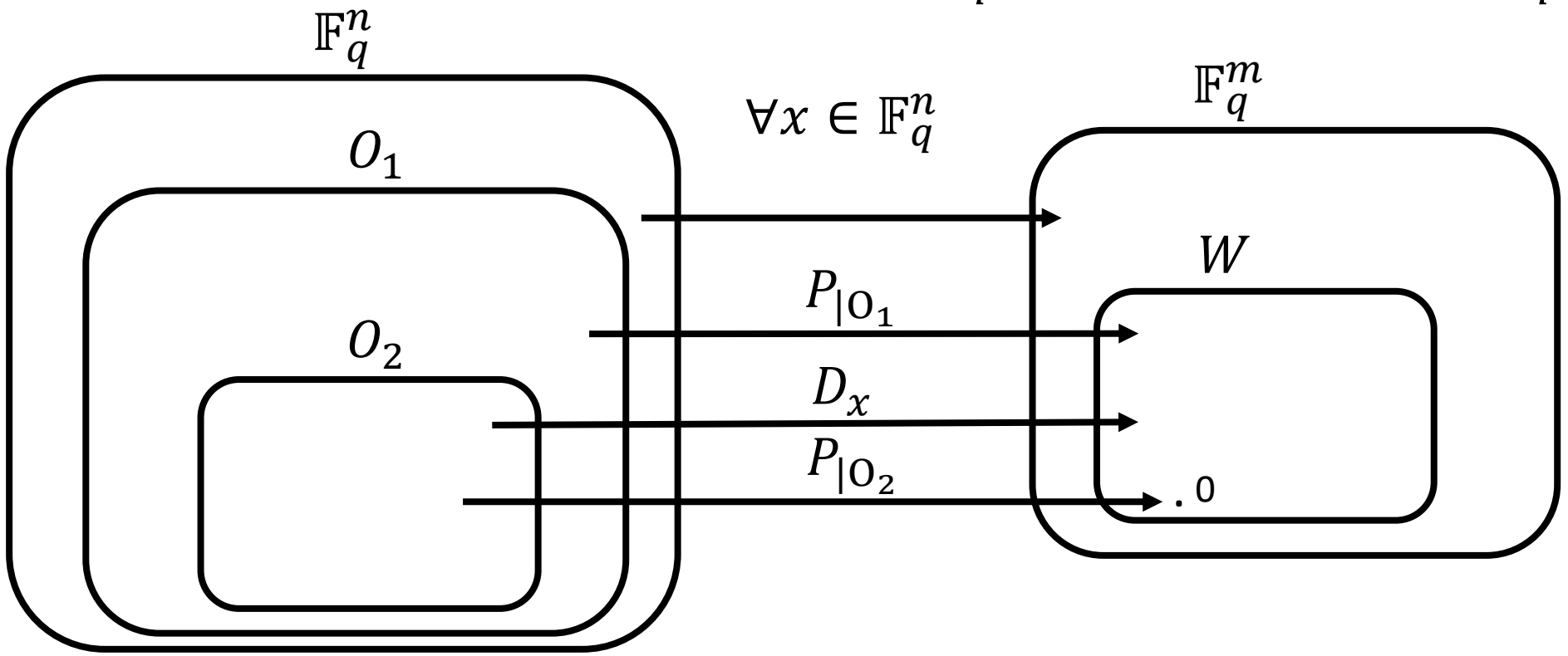
Example parameters (NIST SL 1)

	Oil & Vinegar GF(16)	Oil & Vinegar GF(256)	Rainbow
# Variables	160	112	100
# Equations	64	44	64
Finite Field	GF(16)	GF(256)	GF(16)
Pk size	66 KB	43 KB	58 KB
Signature size	96 B	128 B	66 B

Rainbow Trapdoor as presented in [Beu21]

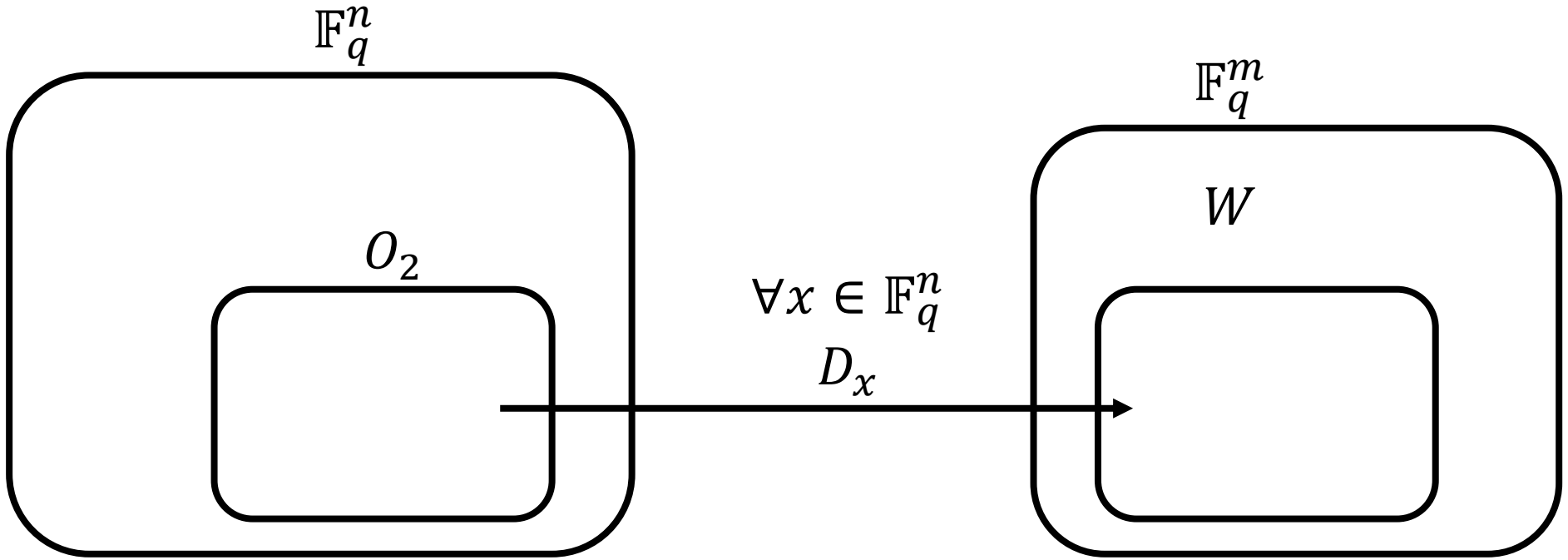
Public key is a quadratic map: $P(x)\colon \mathbb{F}_q^n \to \mathbb{F}_q^m$

Trapdoor consists of subspaces $O_2 \subset O_1 \subset \mathbb{F}_q^n$ and subspaces $W \subset \mathbb{F}_q^m$ s.t.



The structure of a Rainbow public key

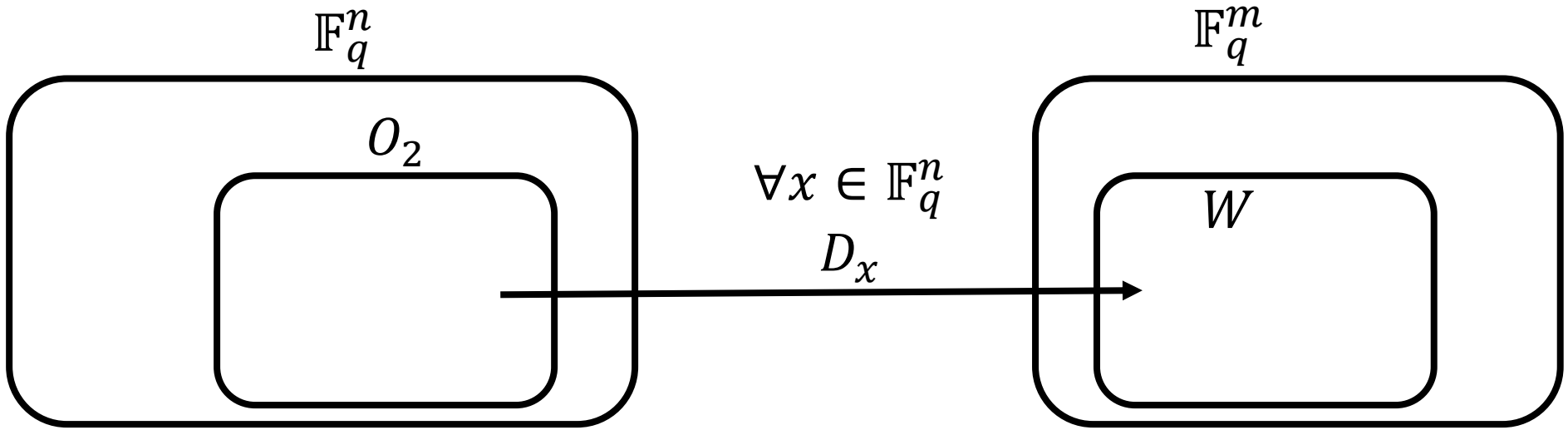
Main idea



For every x we get a linear map $D_x: \mathbb{F}_q^n \to \mathbb{F}_q^m$ that sends O_2 to W.
We want to find O_2. (This reduces to a MinRank problem [Beu21])

Main observation: D_x is more likely to have a kernel vector in O_2.

D_x is likely to have kernel vectors in O_2



Average number of non-zero kernel vectors in O_2 is $\frac{|O_2|-1}{|W|} \approx 1$

The probability of a non-zero kernel vector in O_2 is $\approx 1/(q-1)$

New Attack:

1. Guess $x \in \mathbb{F}_q^n$, hope that $\ker(D_x) \cap O_2$ is non-trivial
2. Solve $\begin{cases} D_x o = 0 \\ P(o) = 0 \end{cases}$
3. If no solutions, return to 1.

R2SL1: Attempting to solving the system takes 3 hours 32 minutes using standard techniques. (Wiedemann-XL)

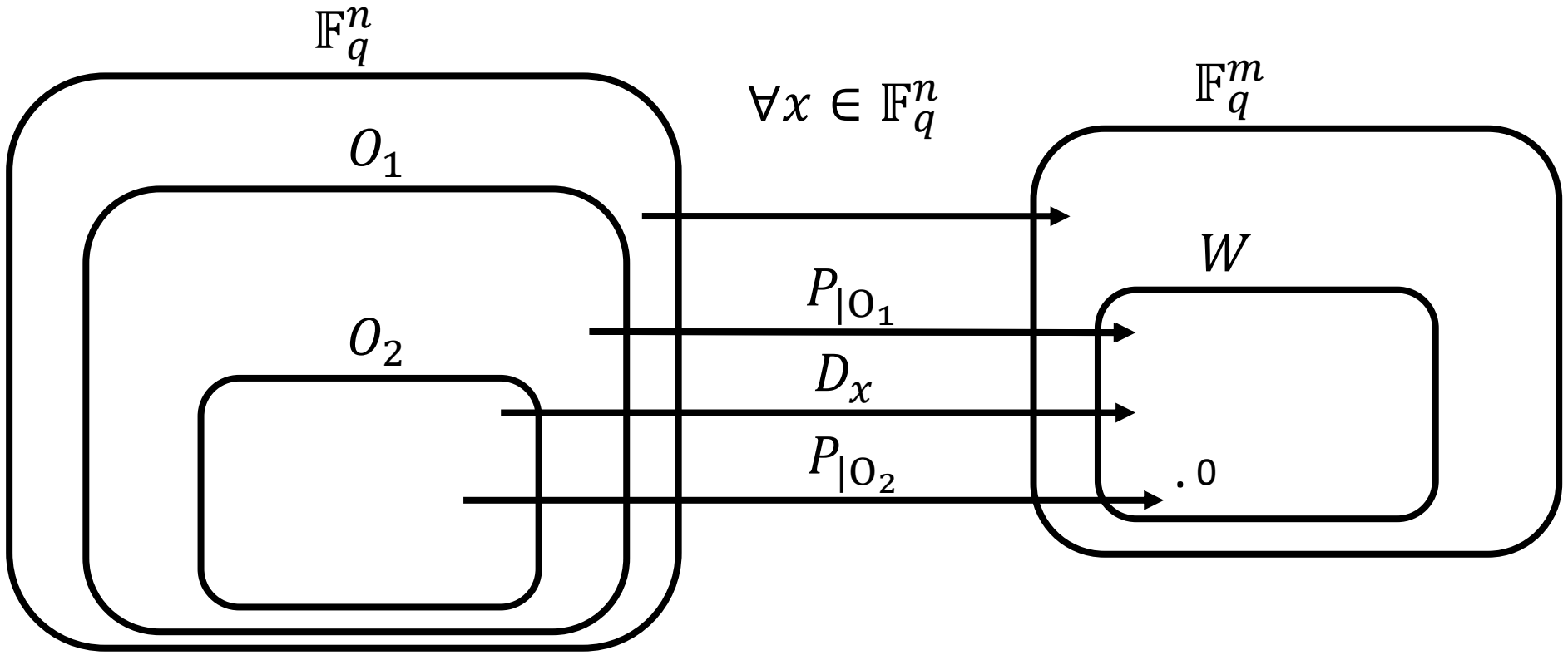
Repeat $q - 1 = 15$ times ⟹ 53 hours (one weekend)

Finishing the attack

We have a single vector o in O_2. How to find the full sk key (O_1, O_2, W)?

1) $\forall x: D_x(o) \in W$, so we learn all of W

2) Solve for all o' s.t. $D_x(o') \in W$ for all x, reveals all of O_2



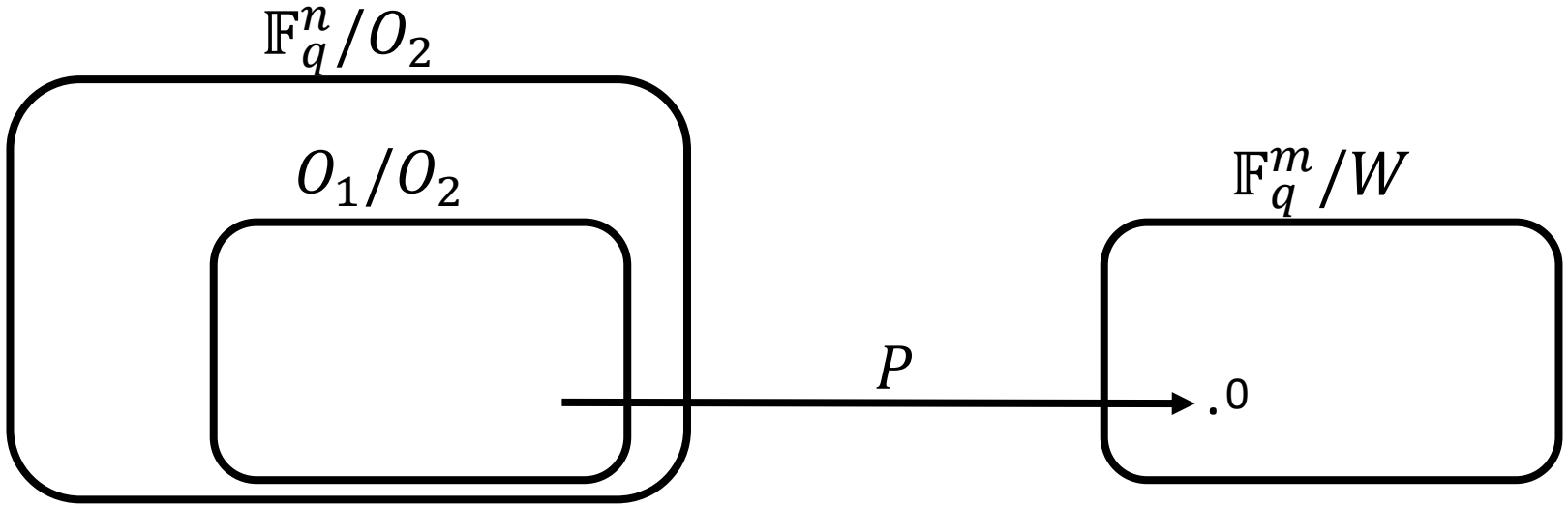
Finishing the attack

We have a single vector o in O_2. How to find the full sk key (O_1, O_2, W)?

1) $\forall x:\ D_x(o) \in W$, so we learn all of W

2) Solve for all o' s.t. $D_x(o') \in W$ for all x, reveals all of O_2

3) Take quotient by O_2 and W. Break the remaining Oil & Vinegar key with existing attacks (e.g. Kipnis-Shamir)



New Rainbow parameters (Old SL 3 is now SL 1)

	Oil & Vinegar GF(16)	Oil & Vinegar GF(256)	Rainbow (updated params)
# Variables	160	112	148
# Equations	64	44	80
Finite Field	GF(16)	GF(256)	GF(256)
Pk size	66 KB	43 KB	258 KB
Signature size	96 B	128 B	164 B

Rainbow is no longer better than Oil & Vinegar!

Use Oil & Vinegar instead. (NIST)

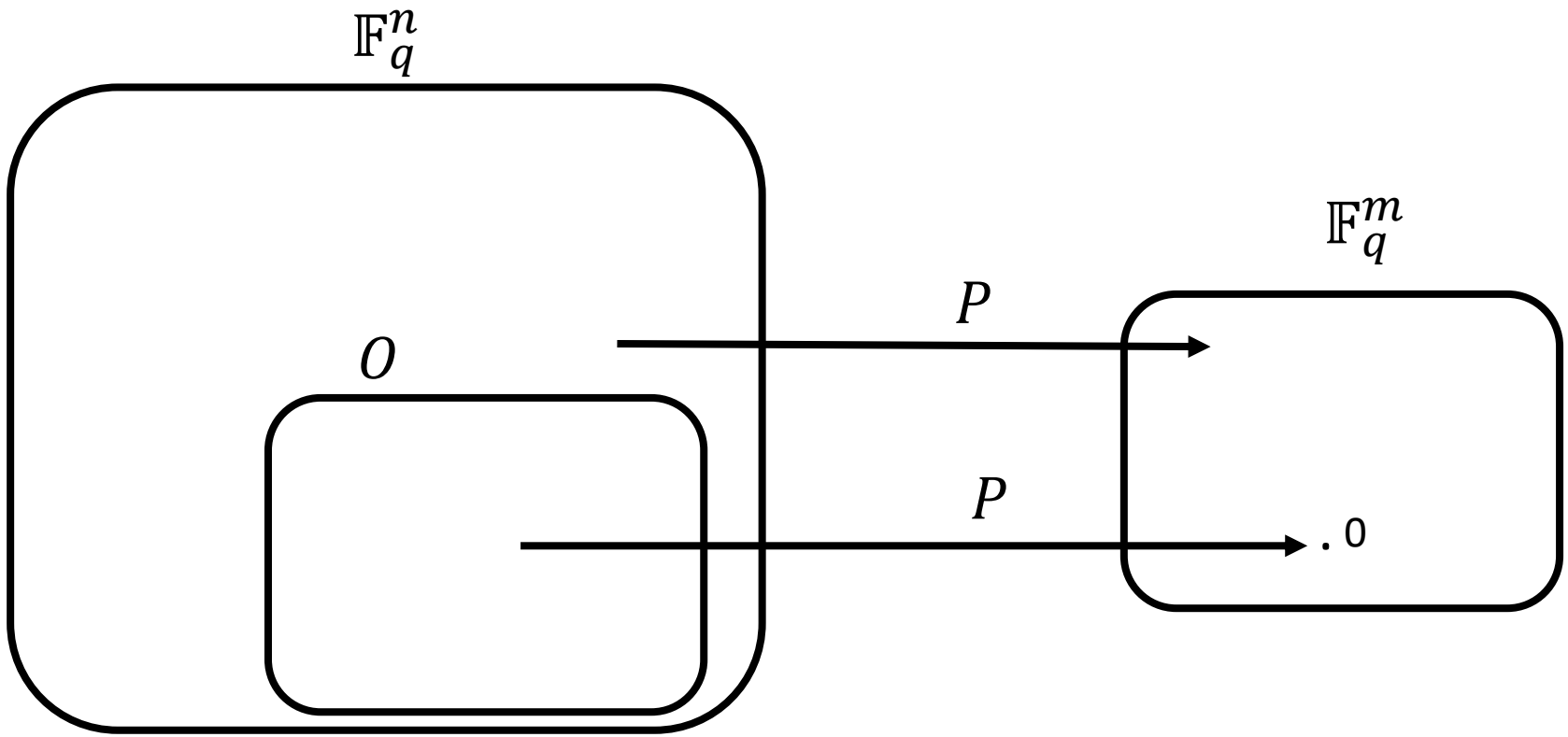
Overview

Oil & vinegar

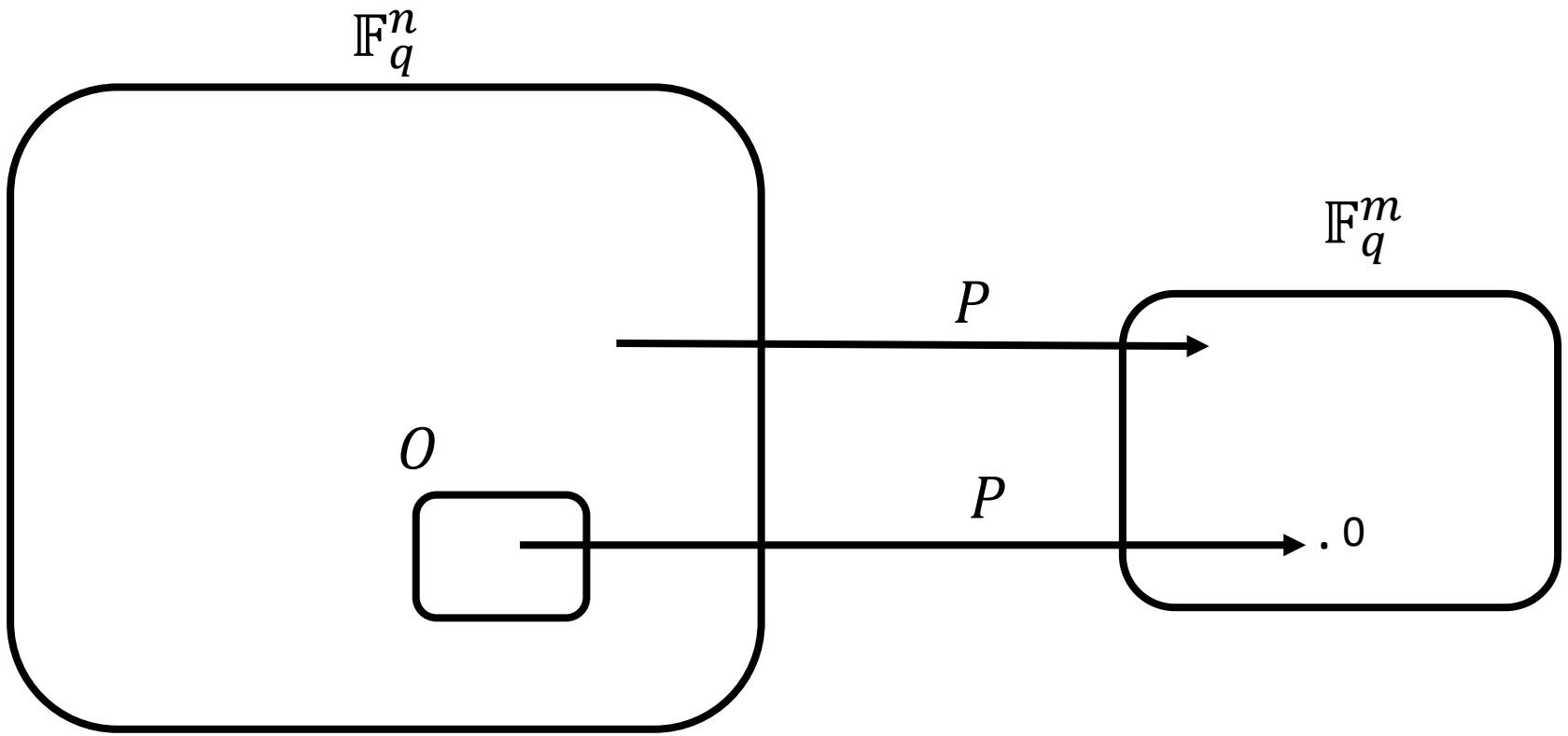
Rainbow

MAYO

MAYO Trapdoor



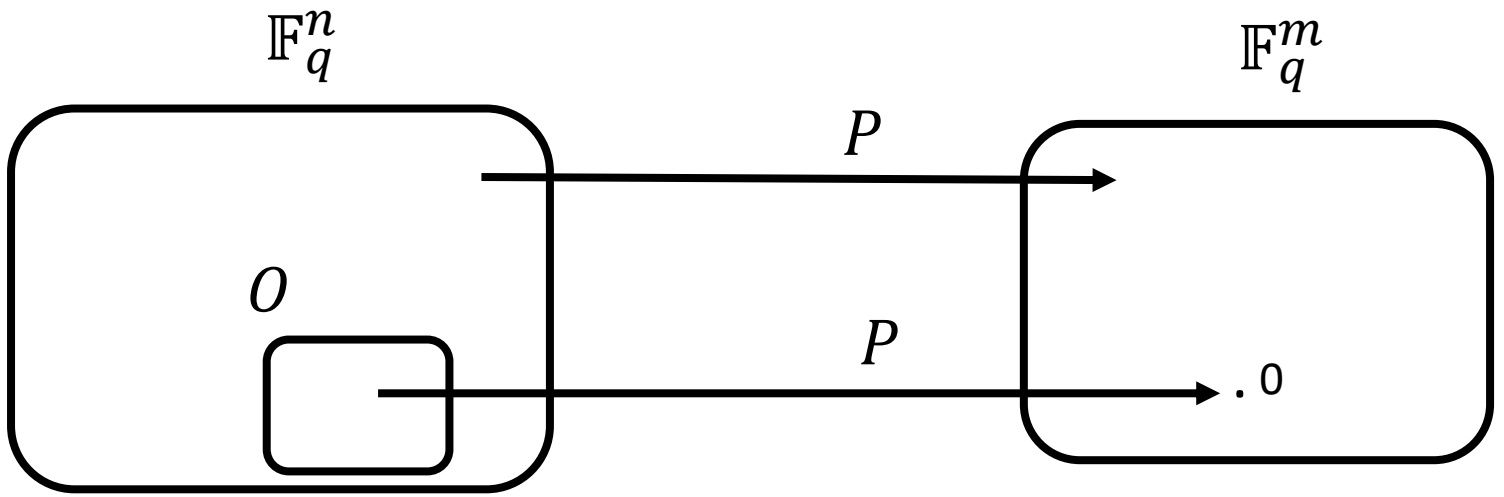
MAYO Trapdoor



Making O smaller has 2 benefits:

- We can use smaller n (key recovery attack: $O(q^{n-2o})$)

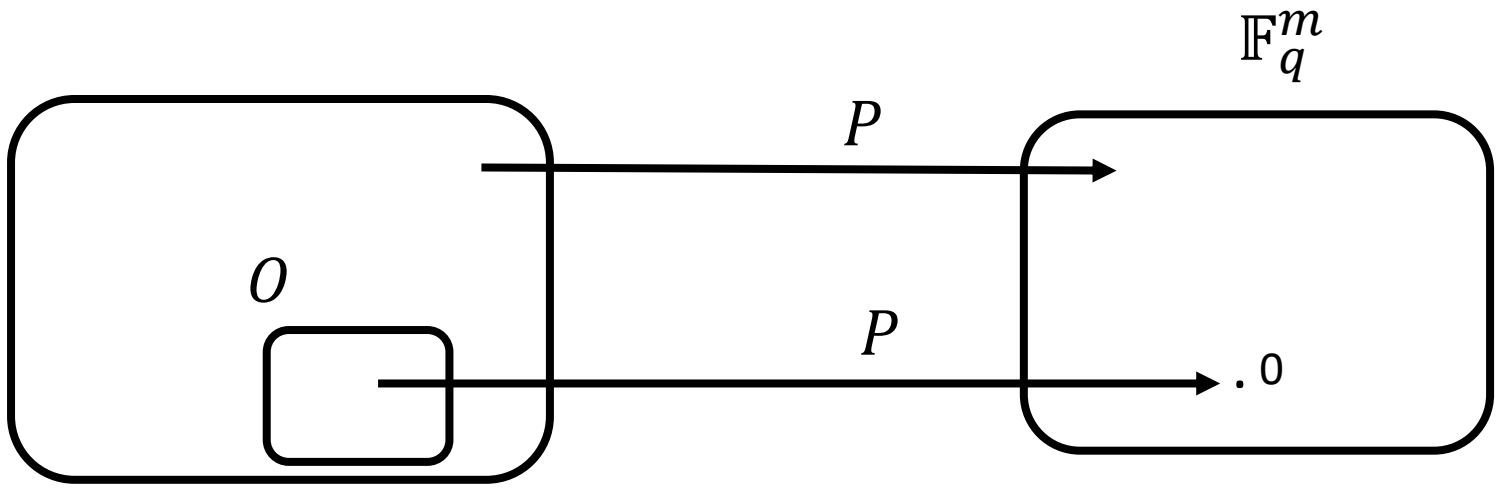
MAYO Trapdoor



Making O smaller has 2 benefits:

- We can use smaller n (key recovery attack: $O(q^{n-2o})$)
- Public key becomes smaller: $O(o^2 m)$ instead of $O(m^3)$

MAYO Trapdoor



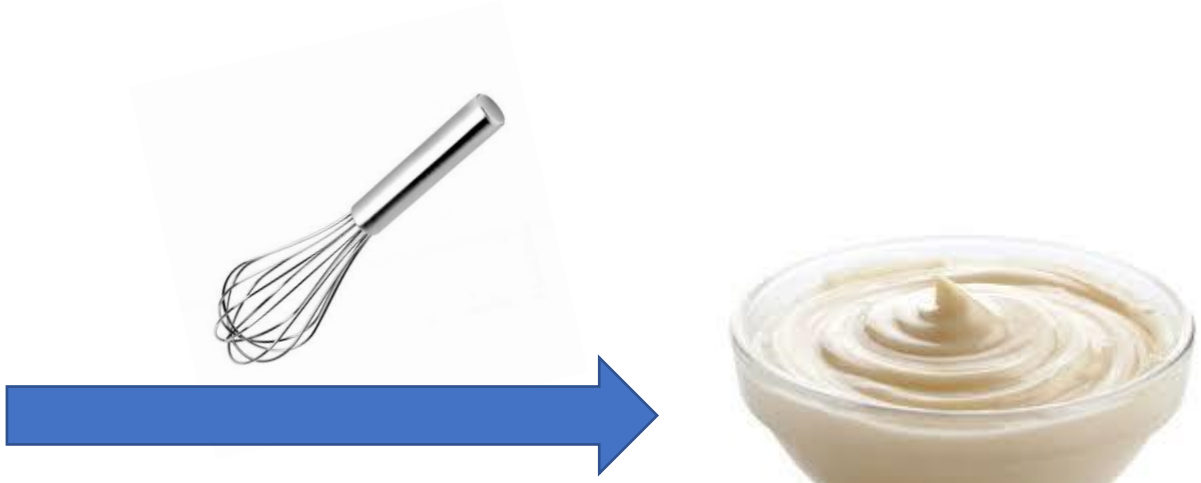
But, if $\dim(O) < m$ the signing algorithm fails:

$P(v + o) = P(v) + D_v(o) = t \in \mathbb{F}_q^m$: m equations, $\dim(O)$ variables.

A little oil can go a long way

Given an oil and vinegar map $P: \mathbb{F}_q^n \to \mathbb{F}_q^m$ that vanishes on an oil space that is too small, we try to "whip up" a larger map $P^\star: \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$, that vanishes on a sufficiently large oil space.

$P: \mathbb{F}_q^n \to \mathbb{F}_q^m$



$P^\star: \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$

Whipping Oil-and-Vinegar: Attempt 1

Let $P^\star(x_1, \ldots, x_k) = P(x_1) + P(x_2) + \cdots + P(x_k)$.

Then $P^\star$: $\mathbb{F}_q^{kn} \to \mathbb{F}_q^m$ vanishes on a large oil space

$$O^k = \{ (o_1, \ldots, o_k) \mid o_1, \ldots, o_k \in O \}$$

So, if $\dim(O^k) = ko \geq m$, then we can sample preimages for $P^\star$.

However, $P^\star$ has extra oil spaces e.g. $\{ (x, ix, 0, \ldots, 0) \mid x \in \mathbb{F}_q^n \}$

$$P(x) + P(ix) = P(x) - P(x) = 0$$

Whipping Oil-and-Vinegar: Attempt 2

Choose m-by-m matrices E_i and set:

$$P^\star(x_1, \ldots, x_k) = E_1 P(x_1) + E_2 P(x_2) + \cdots + E_k P(x_k)$$

Then there is a negligible chance of there being any extra oil spaces.

But, $P^\star$ is the sum of k functions with independent inputs, so finding a preimage = solving a k-sum problem.

Wagner's K-tree alg has complexity $q^{m/(1+\lceil \log_2 k \rceil)}$

Whipping Oil-and-Vinegar: Attempt 3

Choose matrices $E_{i,j}$ for all $0 \leq i \leq j \leq k$ and set

$$P^{\star}(x_1, \ldots, x_k) = \sum_i E_{ii} P(x_i) + \sum_{i<j} E_{ij} D_{x_i}(x_j)$$

Any two variables x_i, x_j interact in the $E_{ij} D_{x_i}(x_j)$ term, so the K-Tree attack does not apply.

Security Analysis

Assume that:

1) Oil-and-Vinegar maps P are indistinguishable from random MQ maps. ☺
2) Whipping up a random map P, results in a (multi-target) preimage resistant MQ map $P^{\star}$. ?

Then the MAYO signature scheme is EUF-CMA secure.
(for appropriately chosen parameters)

In particular, we proved that signatures do not leak information about the secret key.

MAYO parameters

	Oil & Vinegar GF(16)	Oil & Vinegar GF(256)	MAYO $o = 19$	MAYO $o = 5$
# Variables	160	112	79 x 4	66 x 16
# Equations	64	44	66	69
Finite Field	GF(16)	GF(256)	GF(16)	GF(16)
Pk size	66 KB	43 KB	6.3 KB	533 B
Signature size	96 B	128 B	174 B	544 B

Size of O gives a trade-off between signature size and pk size.

Logo credit:
Sofía Celi

Ask not what MAYO can do for you, but what you can do for MAYO!

Please reach out to contact@pqmayo.org if you want to help with:

- Design
- Cryptanalysis
- Implementations
- Security Proofs
- Side-channel security
- Saucy puns
- …

"90's" version: **MAYO'nAES**

Questions?