Unbalanced Oil and Vinegar

Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, Bo-Yin Yang

MAYO

Ward Beullens, Fabio Campos, Sofía Celi, Basil Hess, Matthias J. Kannwischer.

Ward Beullens
IBM Research Europe
Oxford 2023

Multivariate Quadratic Cryptography

Cryptography based on the hardness of finding solutions to systems of multivariate quadratic equations.

Example: Solve for x and y mod 7:

$$x + 5x^2 + 3xy = 4 \mod 7$$
$$x^2 + 5xy + 5y^2 = 1 \mod 7$$

Multivariate Quadratic Cryptography

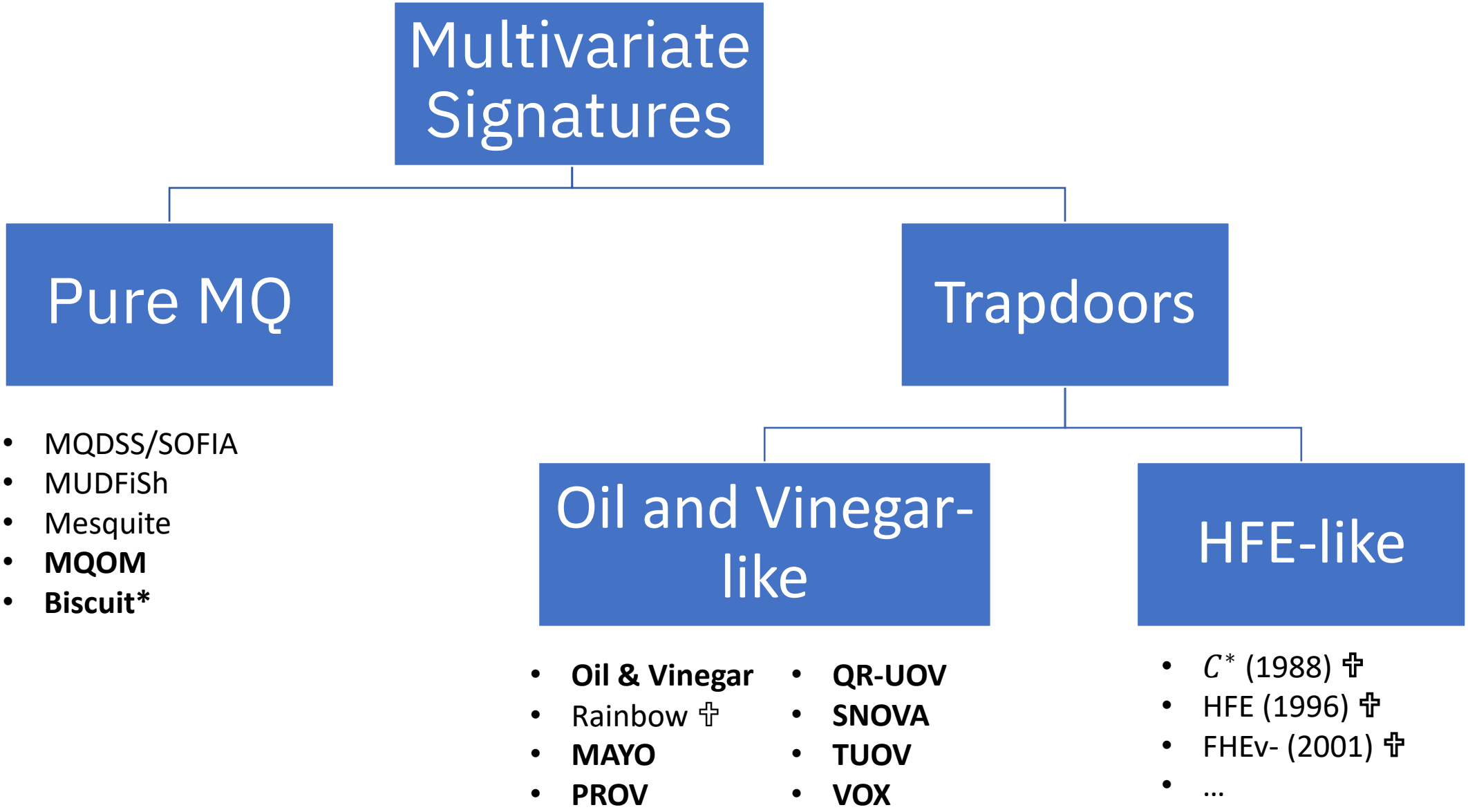
Cryptography based on the hardness of finding solutions to systems of multivariate quadratic equations.

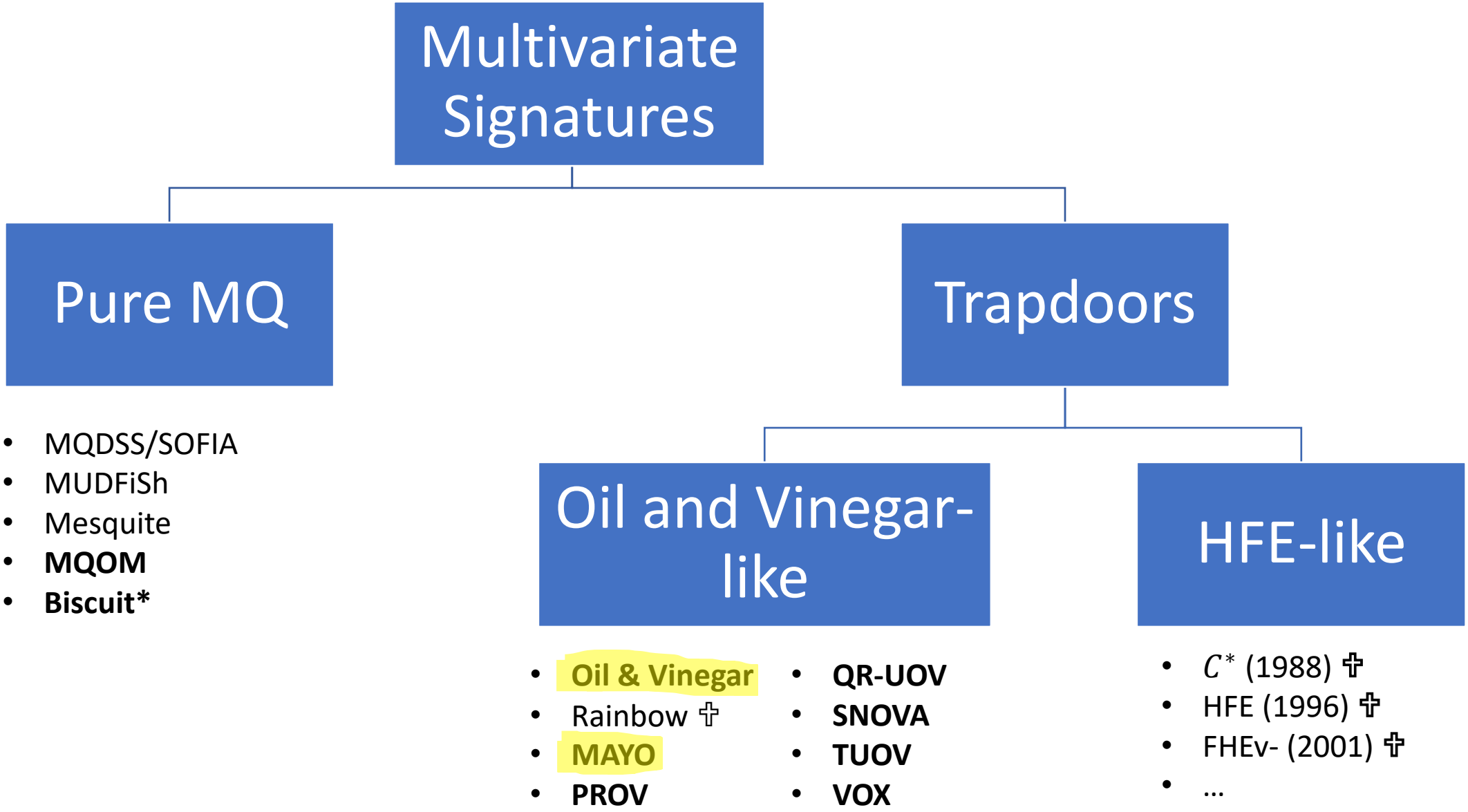
Example: Solve for x and y mod 7:

$$x + 5x^2 + 3xy = 4 \mod 7$$
$$x^2 + 5xy + 5y^2 = 1 \mod 7$$

Solution: $x = 6$ and $y = 0$.

For only 2 variables this is still doable, but for more variables this problem quickly becomes very difficult. E.g. The current record mod 31 is only 20 equations in 20 variables!


Multivariate Signatures
Pure MQ
Trapdoors
Oil and Vinegar-like
HFE-like
MQDSS/SOFIA
MUDFiSh
Mesquite
MQOM
Biscuit*
Oil & Vinegar
Rainbow ✞
MAYO
PROV
QR-UOV
SNOVA
TUOV
VOX
C^* (1988) ✞
HFE (1996) ✞
FHEv- (2001) ✞
…


Multivariate Signatures
Pure MQ
Trapdoors
Oil and Vinegar-like
HFE-like
MQDSS/SOFIA
MUDFiSh
Mesquite
MQOM
Biscuit*
Oil & Vinegar
Rainbow ✞
MAYO
PROV
QR-UOV
SNOVA
TUOV
VOX
C^* (1988) ✞
HFE (1996) ✞
FHEv- (2001) ✞
…

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

Secret key: trapdoor information

Signature for message m:

$(x, salt)$ s.t. $P(x) = H(m||salt)$

How to trapdoor a MQ map?

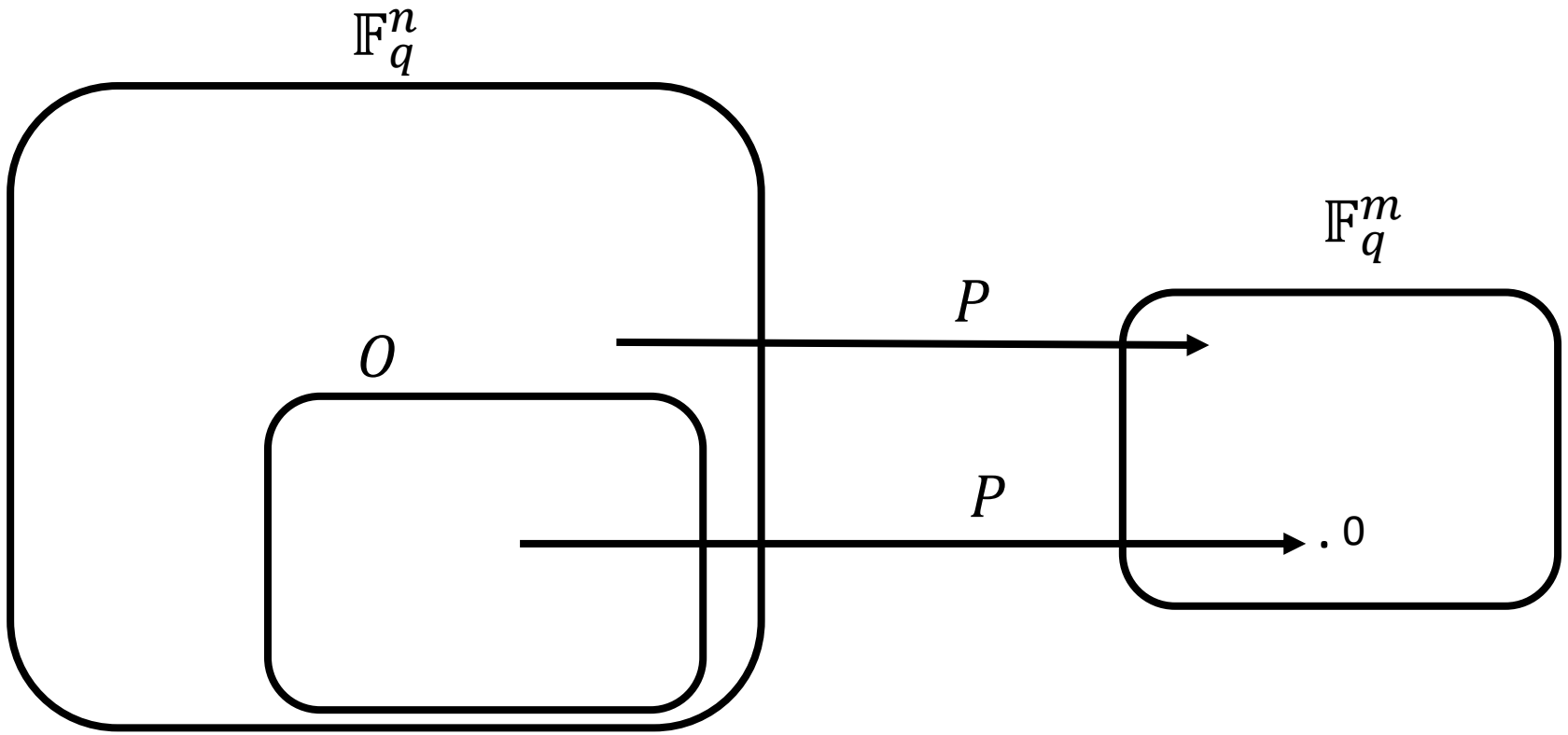
Unbalanced Oil and Vinegar

Ward Beullens, Ming-Shing Chen, Jintai Ding, Boru Gong, Matthias J. Kannwischer, Jacques Patarin, Bo-Yuan Peng, Dieter Schmidt, Cheng-Jhih Shih, Chengdong Tao, Bo-Yin Yang

Oil & Vinegar Trapdoor as presented in [Beu21]

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

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 its 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. $P(v + o) = y$.

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.

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.

Parameters (NIST SL 1)

2 constraints:

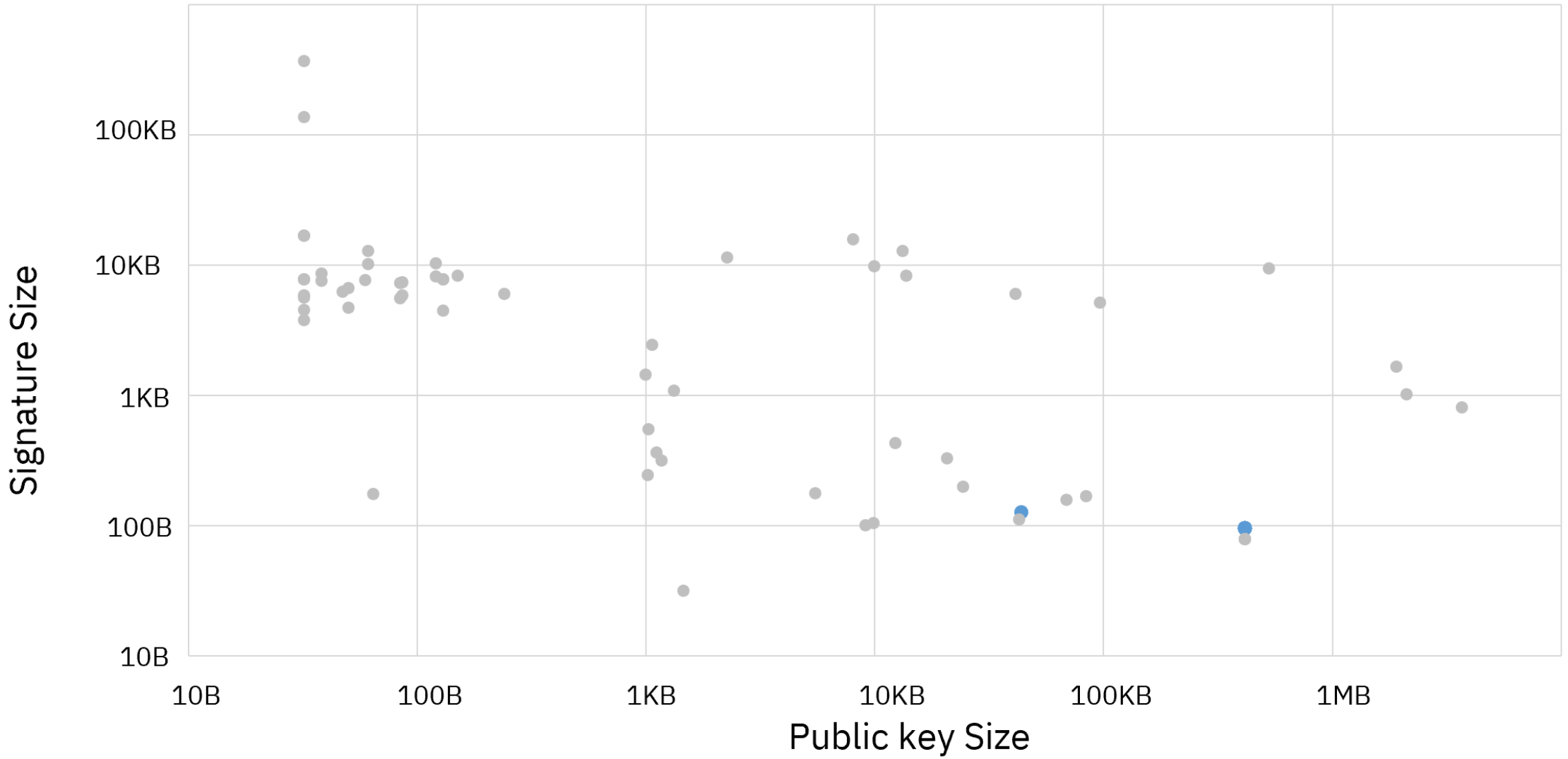
- Finding oil space O should be hard
- It should be hard to solve $P(x) = y$ without O

Attacks:

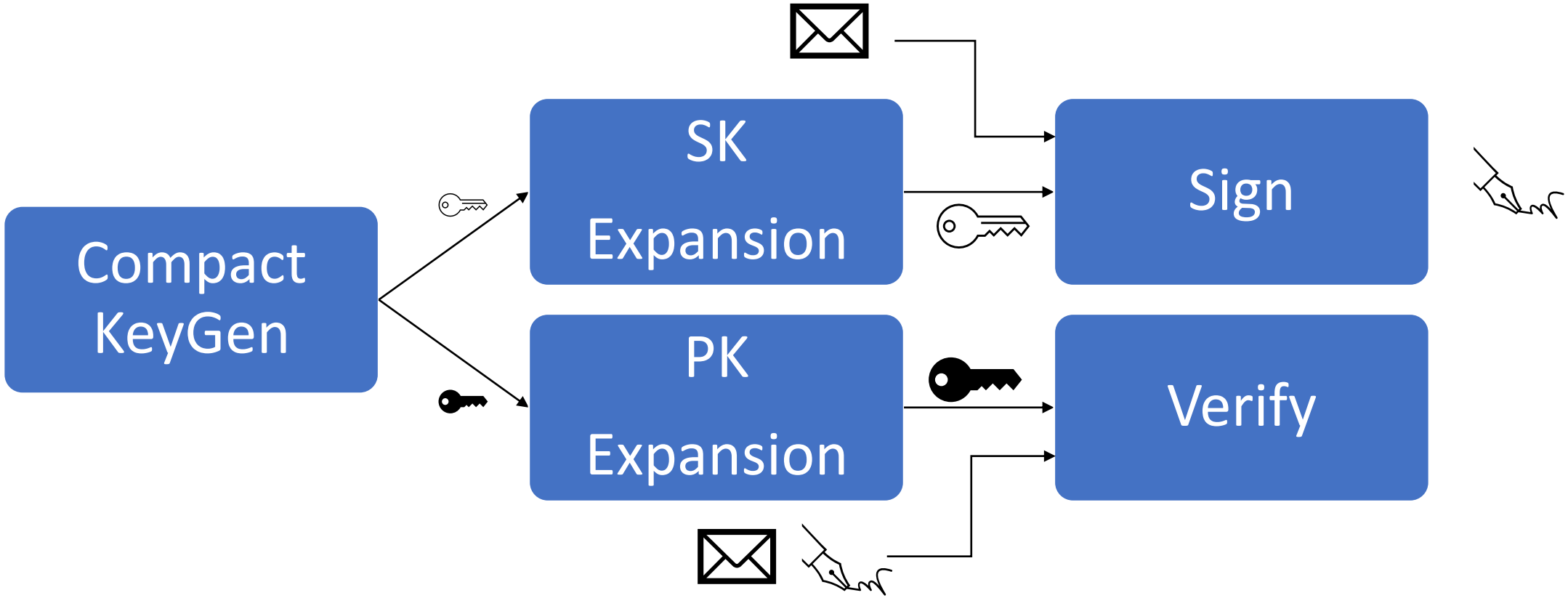
Exponential in $n - 2m$

Exponential in m

	UOV-Ip	UOV-Is
# Variables	112	160
# Equations	44	64
Finite Field	GF(256)	GF(16)
Pk size	44 KB	67 KB
Signature size	128 B	96 B

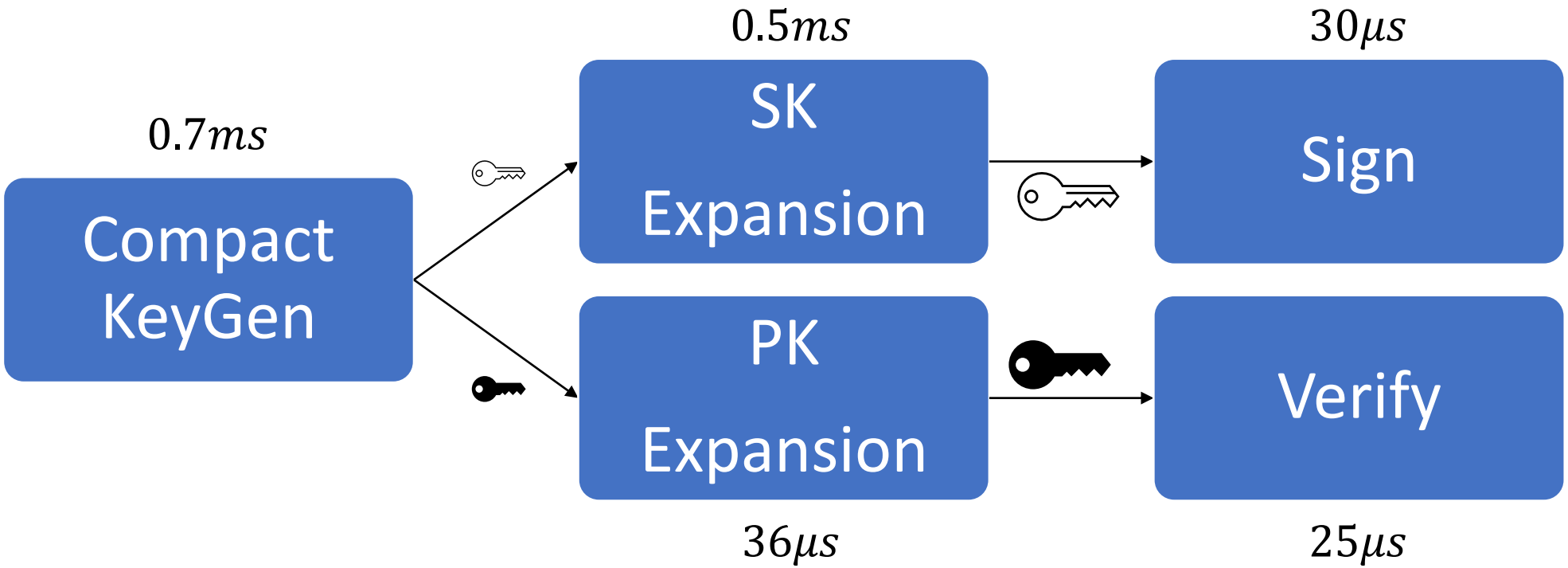

Signature Size
100KB
10KB
1KB
100B
10B
10B
100B
1KB
10KB
100KB
1MB
Public key Size

5-part API

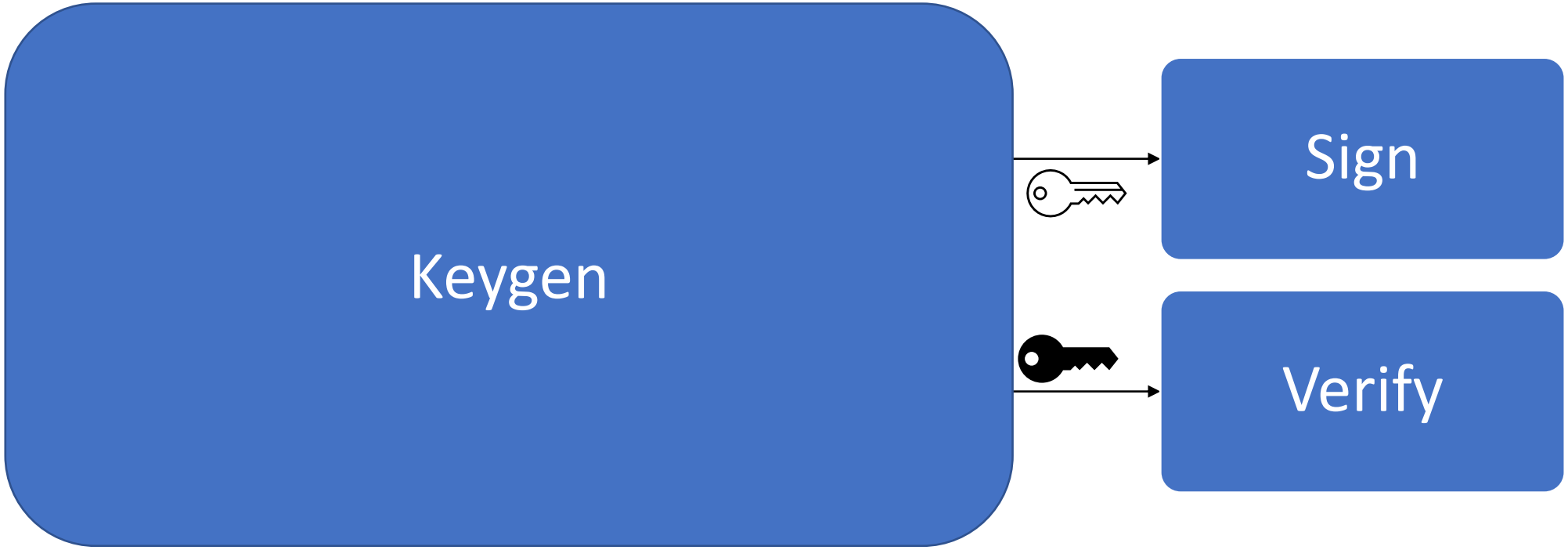


Skylake performance UOV1p

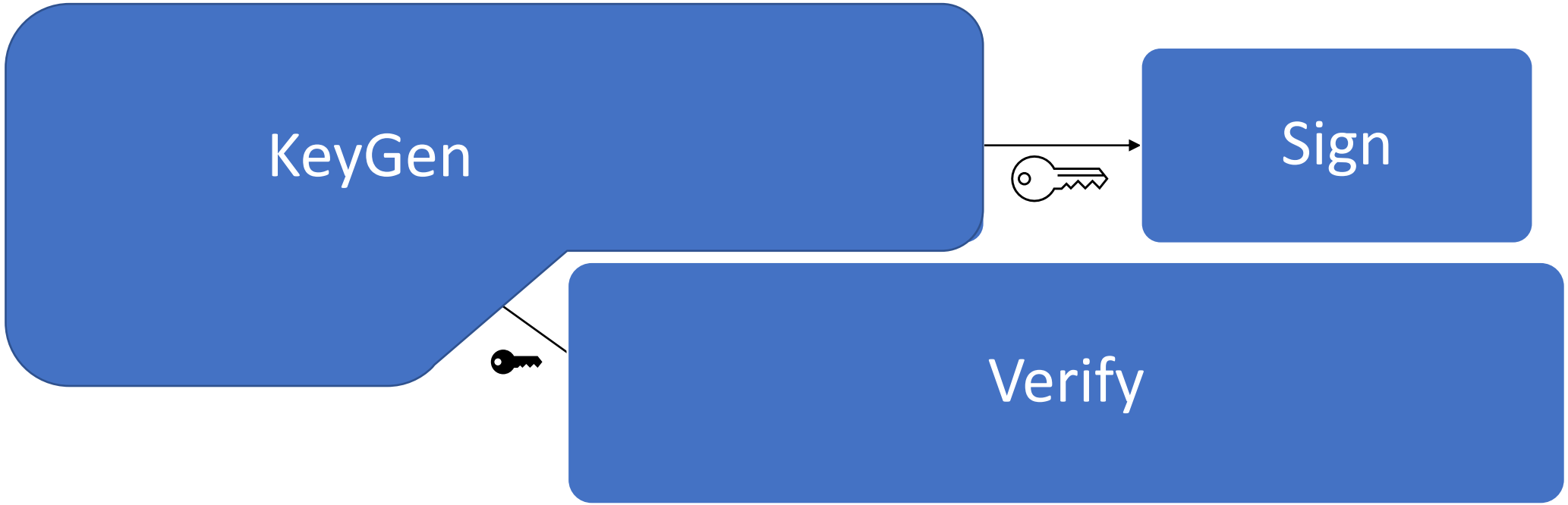
AVX2 + AESNI



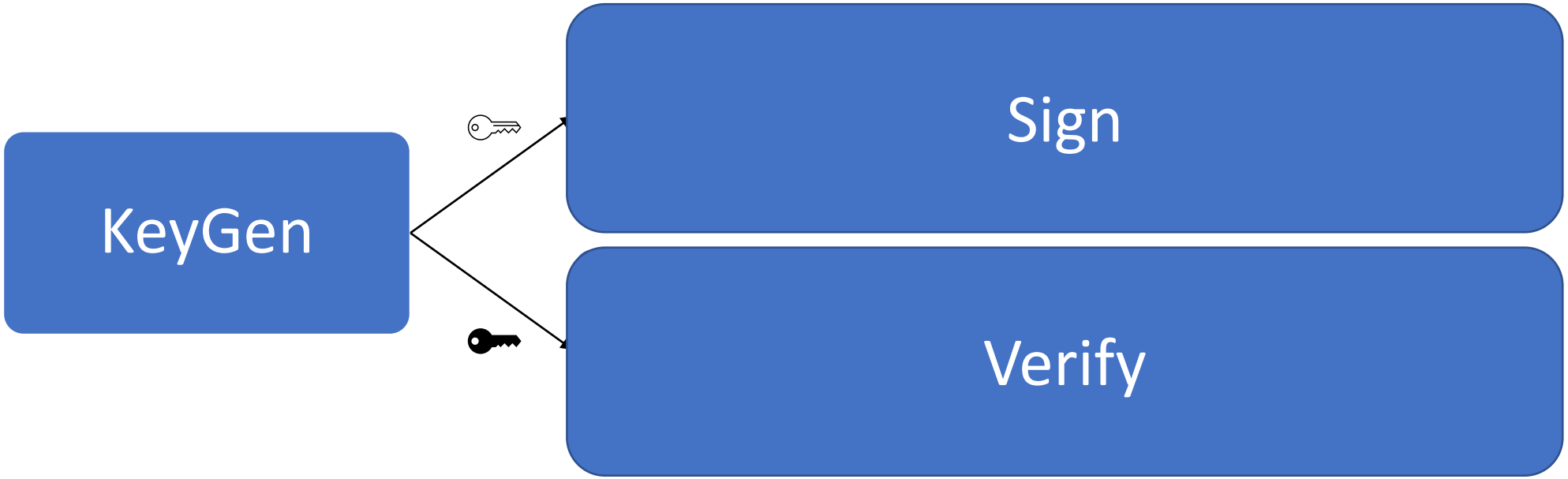
Variant 1: “Classic”



Variant 2: “pkc”



Variant 3: “pkc+skc”



Advantages:

- Old and well studied (1997)
- Small signatures (96B)
- Fast (25μs sign, 30 μs verify)

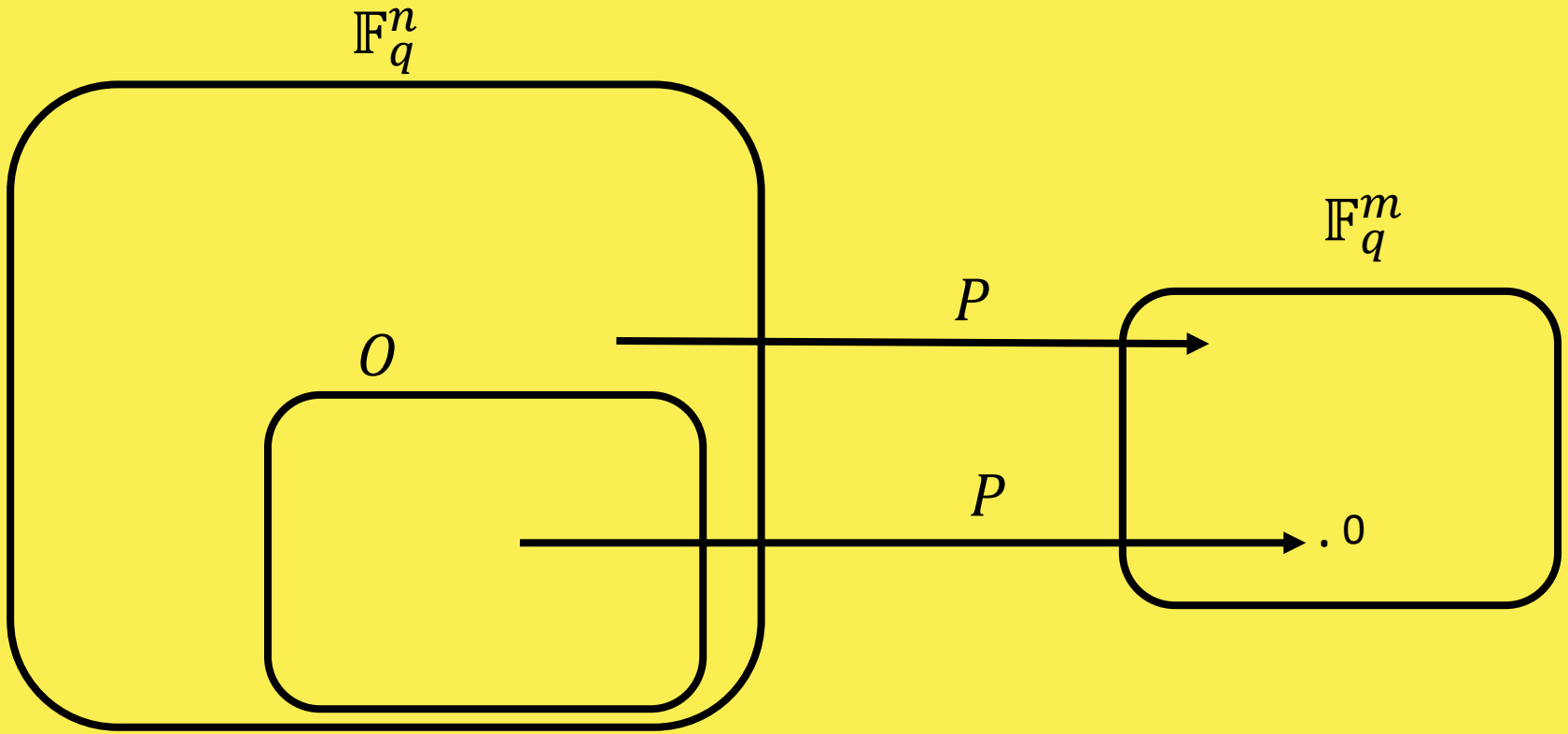
Limitations:

- Somewhat large public keys (44KB)

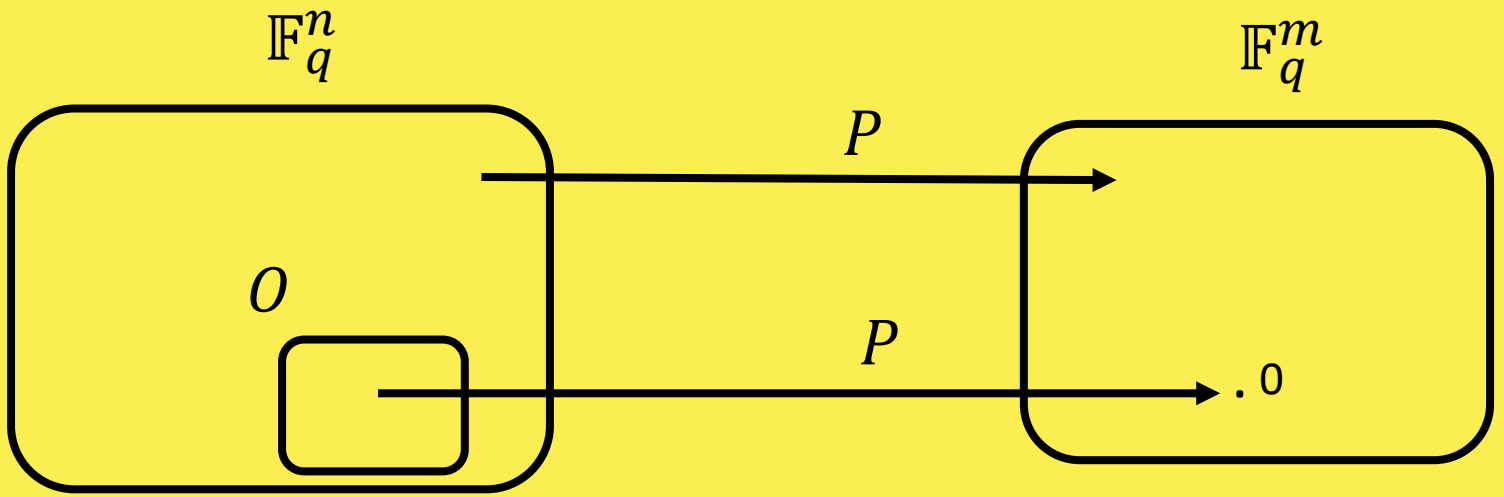
MAYO

Ward Beullens,
Fabio Campos,
Sofía Celi,
Basil Hess, and
Matthias J. Kannwischer.

MAYO Trapdoor



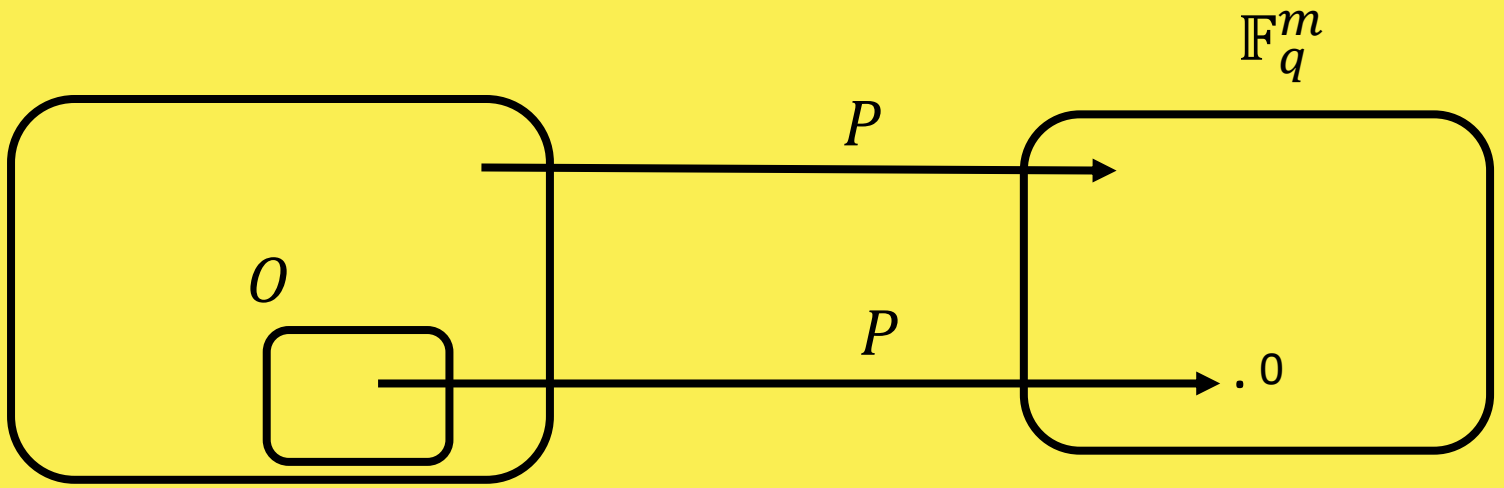
MAYO Trapdoor



Making O smaller has 2 benefits:

- We can use smaller n (key recovery attack exponential in $n - 2o$)
- 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

Whip map $P: \mathbb{F}_q^n \to \mathbb{F}_q^m$ with small space O up to a larger map $P^\star: \mathbb{F}_q^{kn} \to \mathbb{F}_q^m$, that vanishes on a larger oil space O^k.

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

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

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 $P^{\star}$.

Whipping Oil-and-Vinegar: Attempt 2

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

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

New hardness assumption:

Systems P^* of this form are preimage resistant. When P is uniformly random.

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 $P^{\star}$.

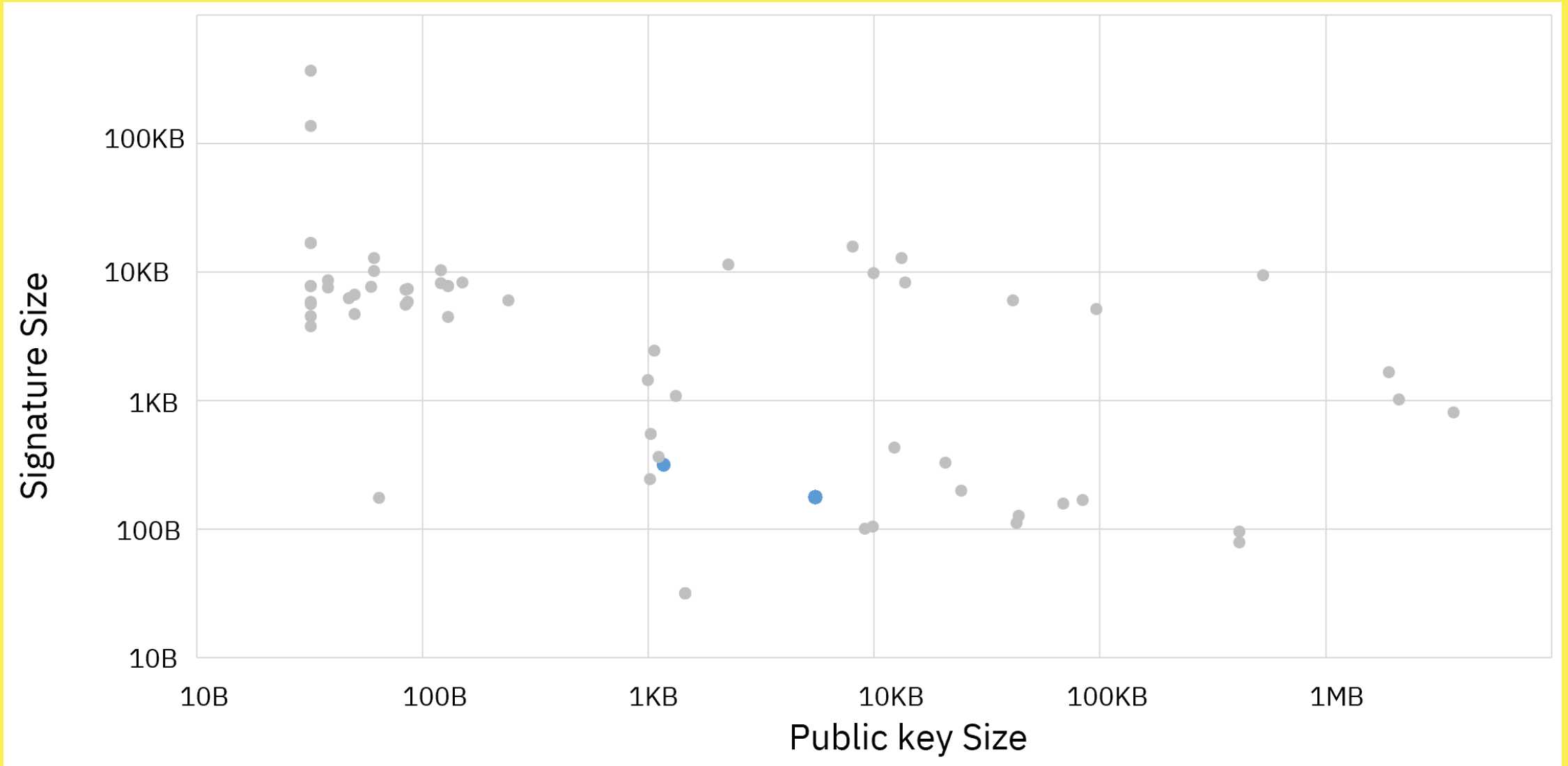
Then the MAYO signature scheme is EUF-CMA secure.
(for appropriately chosen parameters)

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

MAYO parameters

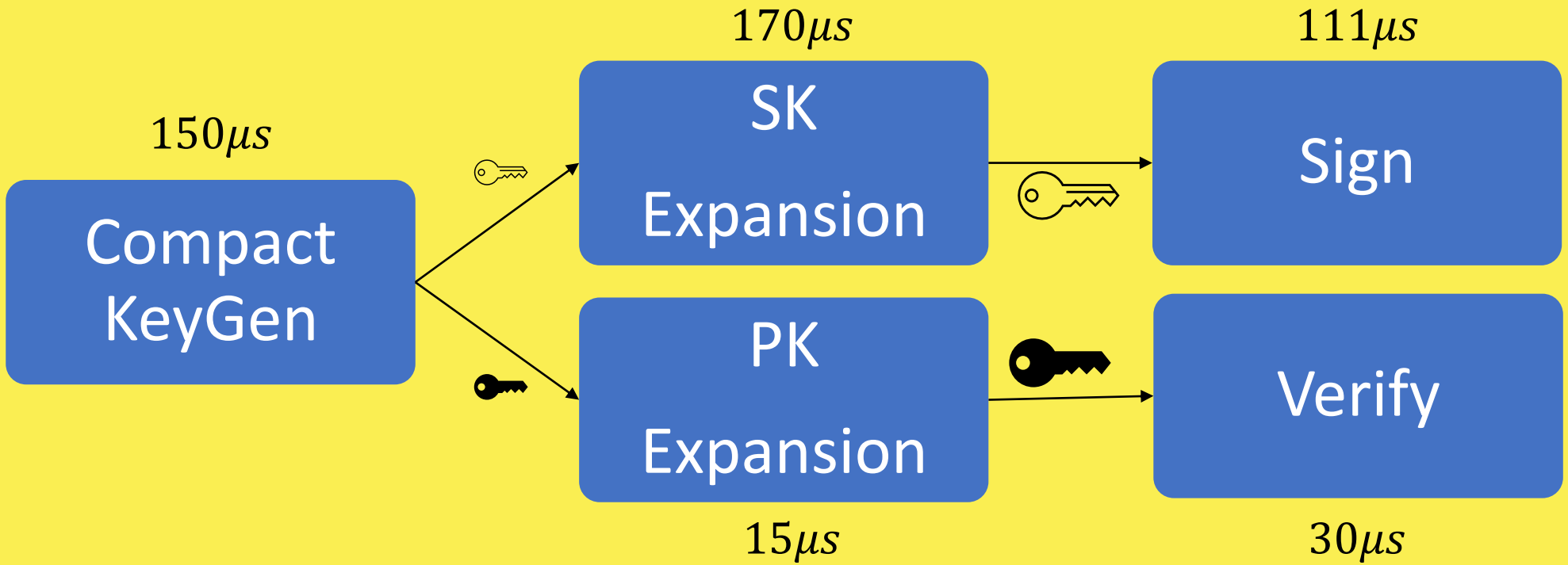
	Oil & Vinegar GF(16)	Oil & Vinegar GF(256)	MAYO 1 $o = 8$	MAYO2 $o = 18$
# Variables	160	112	66 x 9	66 x 16
# Equations	64	44	64	69
Finite Field	GF(16)	GF(256)	GF(16)	GF(16)
Pk size	67 KB	44 KB	1.1 KB	5.4 KB
Signature size	96 B	128 B	321 B	180 B

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


Signature Size
100KB
10KB
1KB
100B
10B
10B
100B
1KB
10KB
100KB
1MB
Public key Size

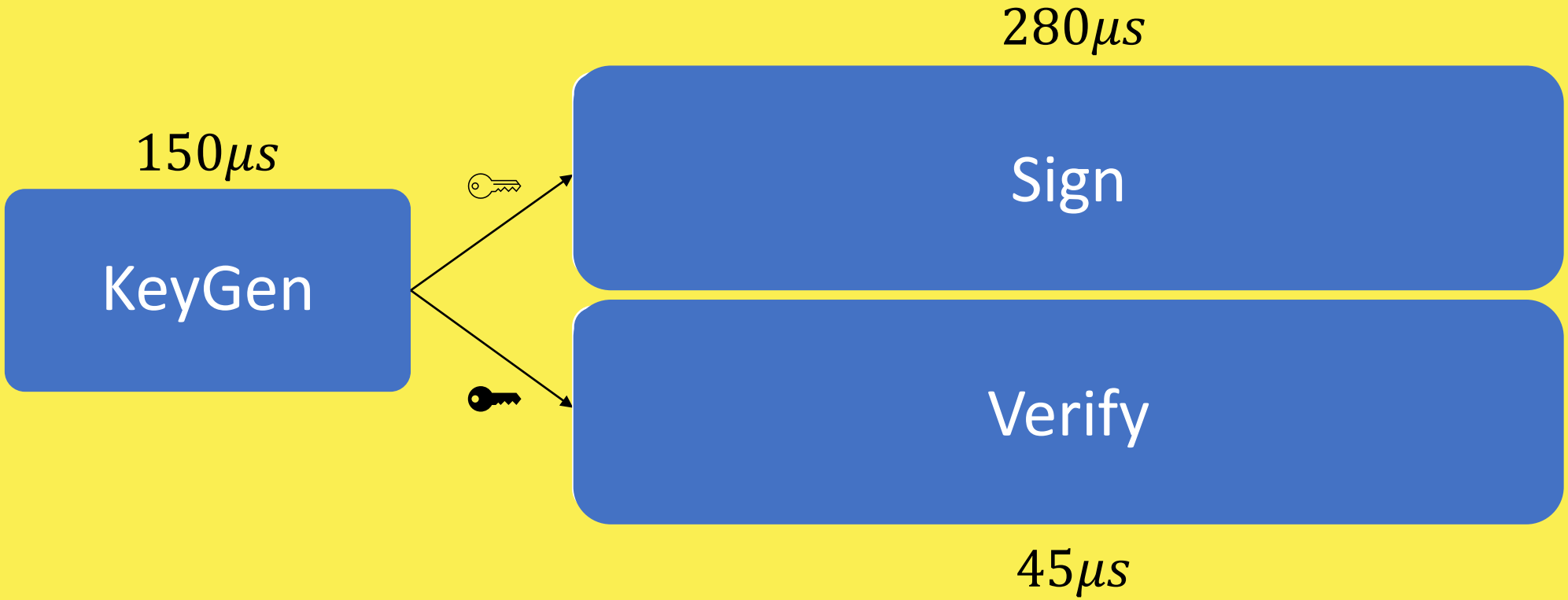
Ice Lake performance MAYO 1

AVX2 + AESNI (work in progress)



Ice Lake performance MAYO 1

AVX2 + AESNI (work in progress)



Advantages:

- Short signatures (180B)
- Short keys (1.1KB)
- Fast ($111\mu s$ signing, $30\mu s$ verify)

Limitations:

- New hardness assumption (2021)