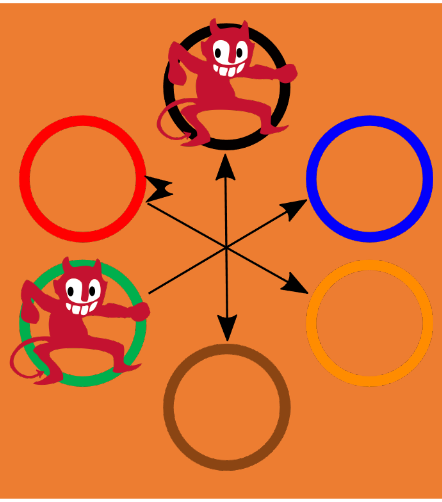
Overview of NIST PQC Standardization (additional call for signatures)

NIST Workshop on Multi-Party Threshold Schemes (MPTS 2023)
NIST, Gaithersburg, USA

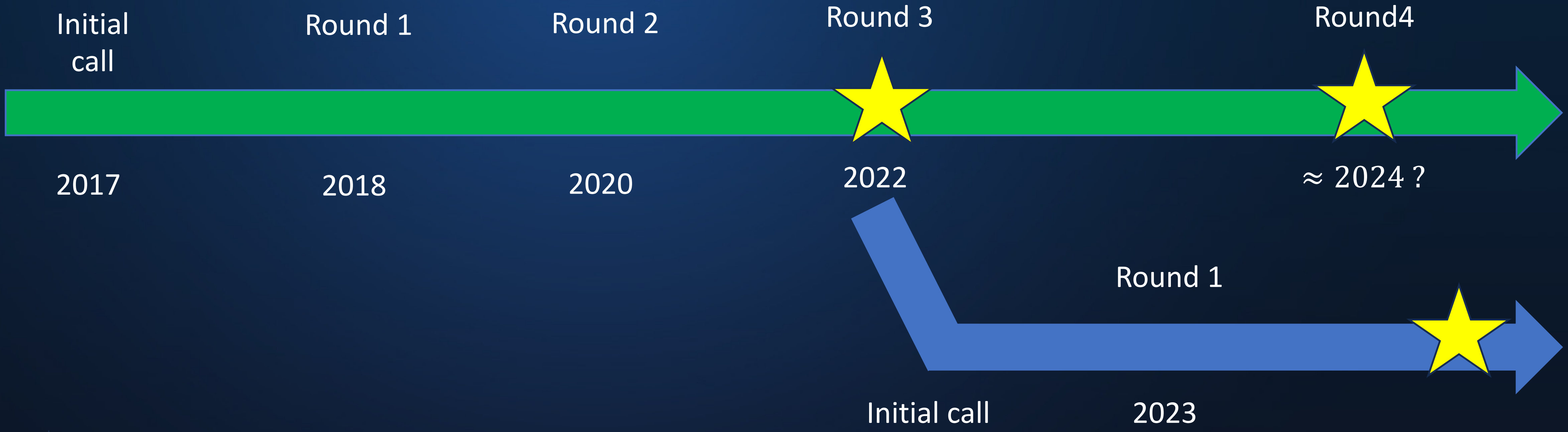


Dr. Maxime Bros
NIST PQC

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Wednesday, September 27th, 2023

Additional call / Onramp call



★ New Standards

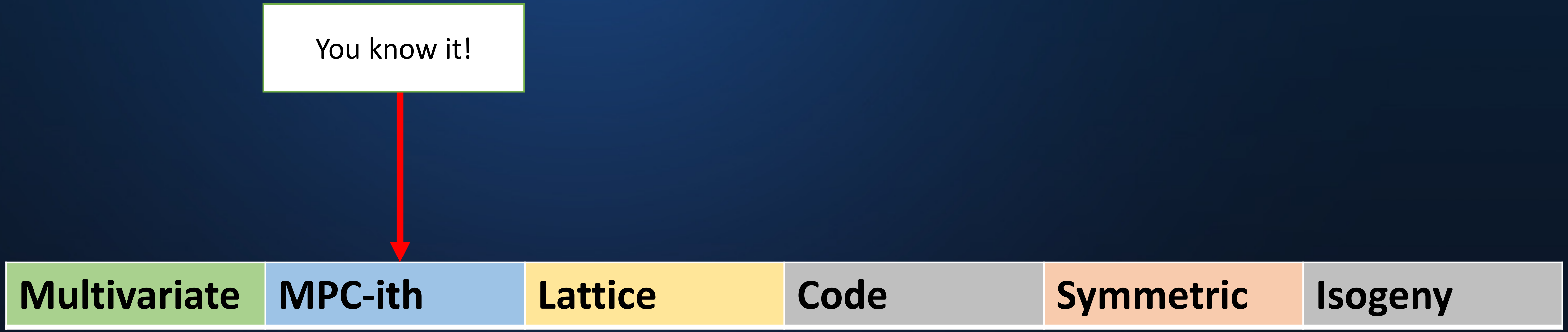
The candidates

- [June 2023] 50 submissions
- [July 2023] 40 accepted

Already 10$^+$ attacks as of today

Multivariate		MPC in-the-head				Lattice	Code	Symmetric	Isogeny	Other
UOV	Other	MinRank	SD/Rank-SD	PKP	MQ					
Mayo	3wise	Mira	RYDE	Perk	MQOM	EagleSign	Enh. Pqsig-rm	Aimer	SQIsign	Alteq
PROV	DMEsign	MiRitH	SDitH		Biscuit	EHT	Fuleeca	Ascon-sign		eMLE-Sig 2.0
QR-UOV	HPPC					HAETAE	LESS	FAEST		KAZ
SNOVA						Hawk	MEDS	SPHINCS-alpha		Preon
TUOV						HuFu	Wave			Xifrat
UOV						Raccoon	Cross			
Vox						Squirrels				
7	3	2	2	1	2	7	6	4	1	5
10		7								
40										

The categories



You know it!

Multivariate | MPC-ith | Lattice | Code | Symmetric | Isogeny

Multivariate based-crypto

$$\mathbb{F}_q[x_1, x_2, \ldots, x_n]$$

$$\begin{cases} f_1(x_1, x_2, \ldots, x_n) \\ f_2(x_1, x_2, \ldots, x_n) \\ \vdots \\ f_m(x_1, x_2, \ldots, x_n) \end{cases}$$

$$\begin{cases} x_1 + 2x_3 \\ 2x_1 + 2x_2 \\ x_1 + x_2 \end{cases}$$

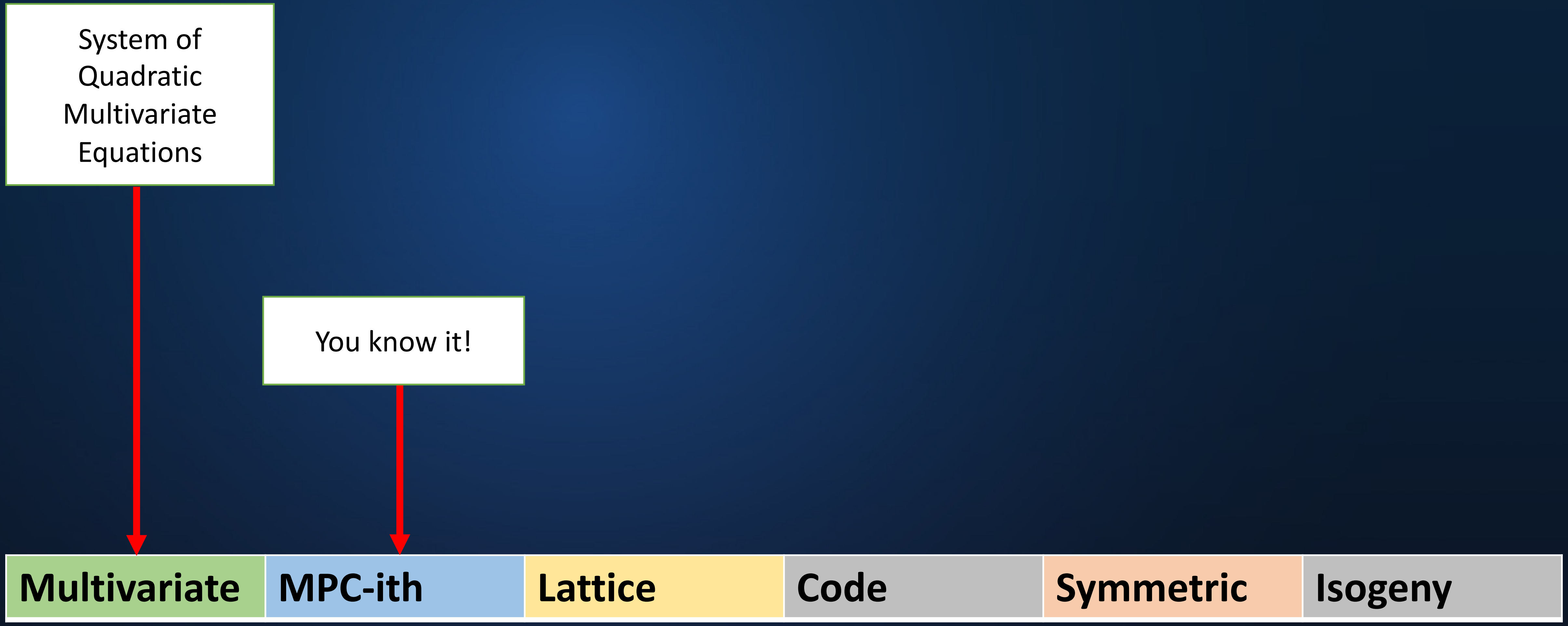
😀

$$\begin{cases} x_1^2 + x_2^2 + x_2x_3 + 2x_3^2 \\ x_1x_2 + x_2^2 + x_2x_3 + x_3^2 \\ x_1^2 + x_1x_2 + x_1x_3 + x_2x_3 \end{cases}$$

😱

Multivariate Quadratic (MQ)

The categories



System of Quadratic Multivariate Equations

You know it!

Multivariate

MPC-ith

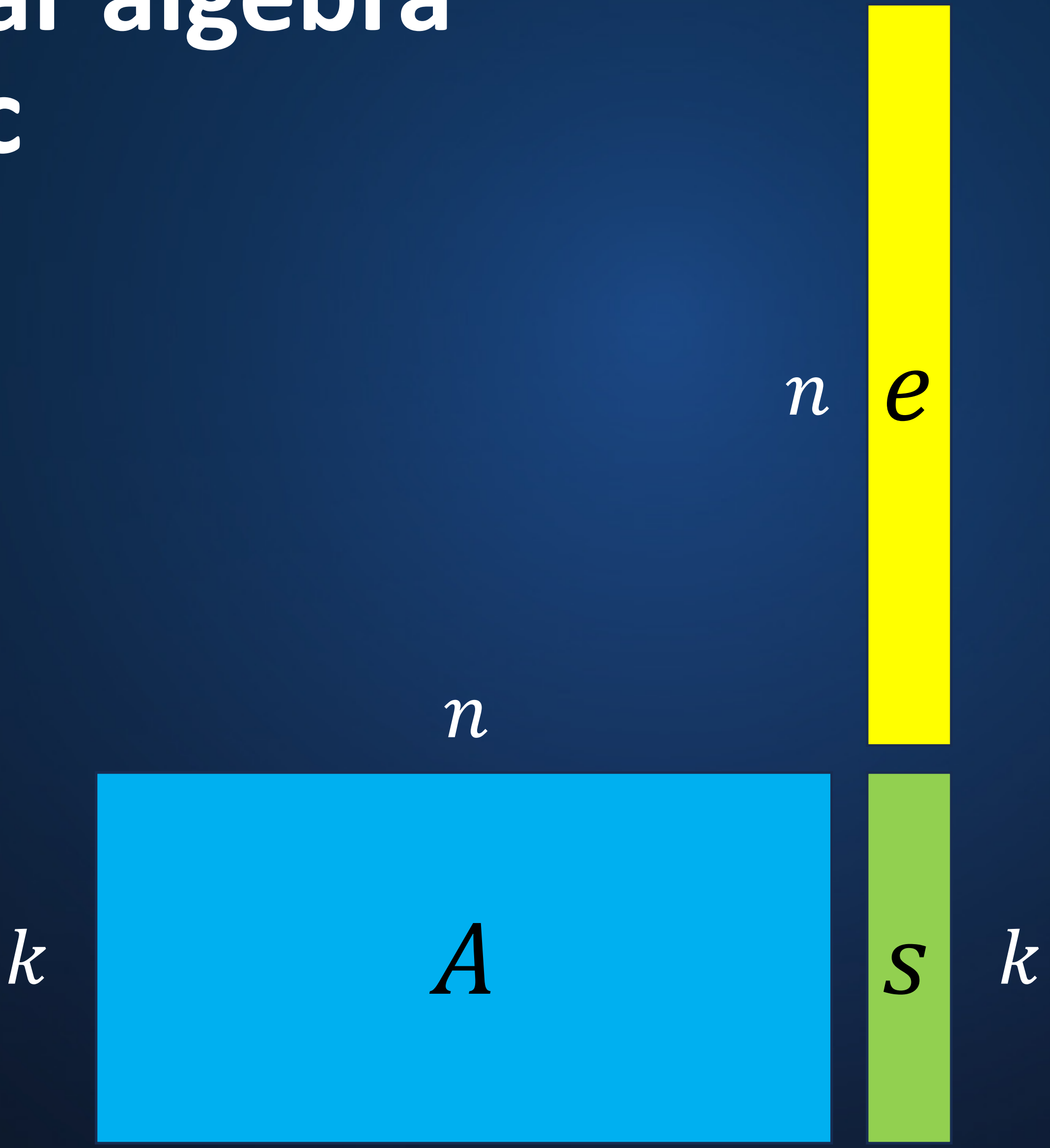
Lattice

Code

Symmetric

Isogeny

Linear algebra
Basic

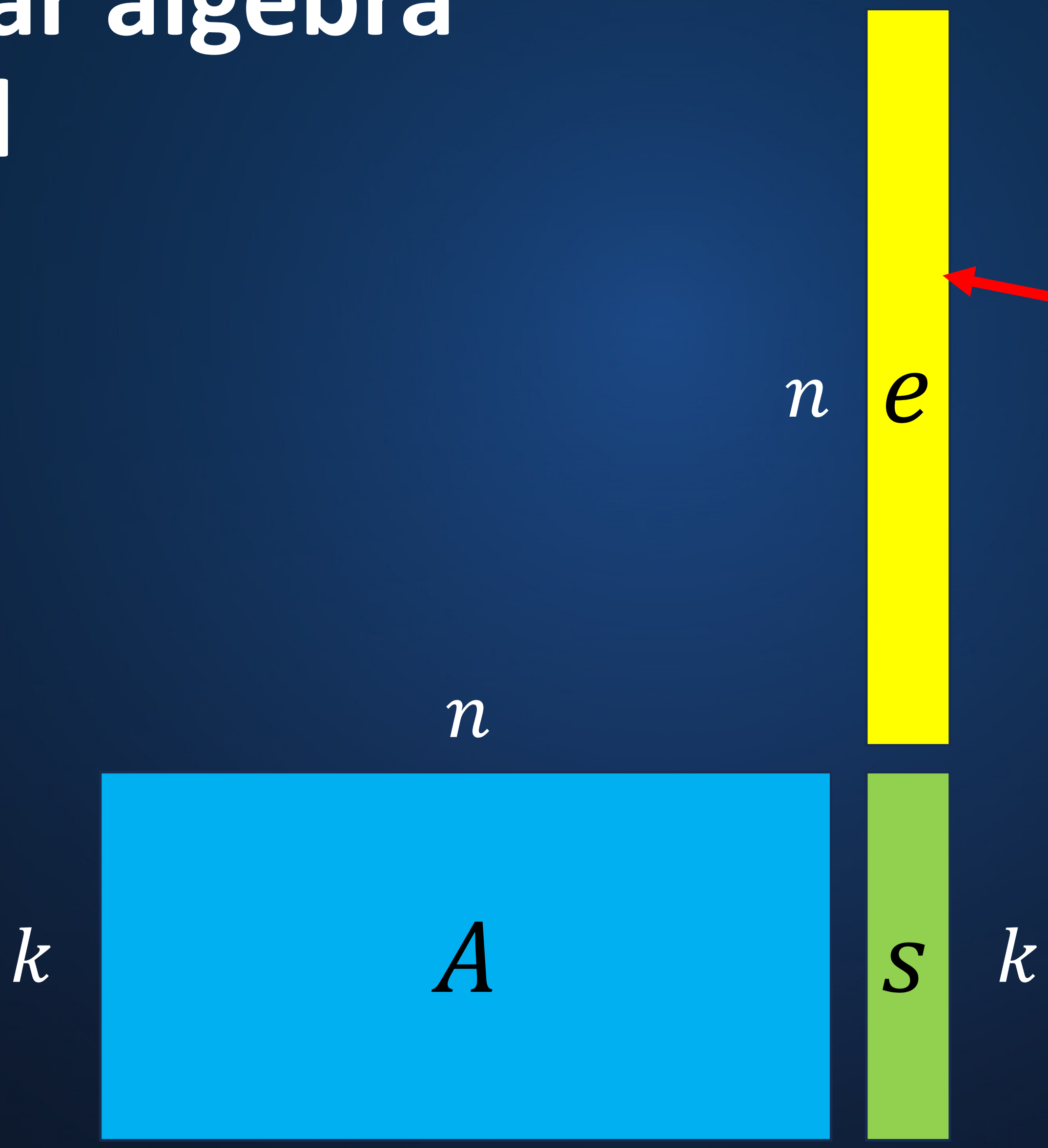


$$Ae^{\intercal} = s^{\intercal}$$

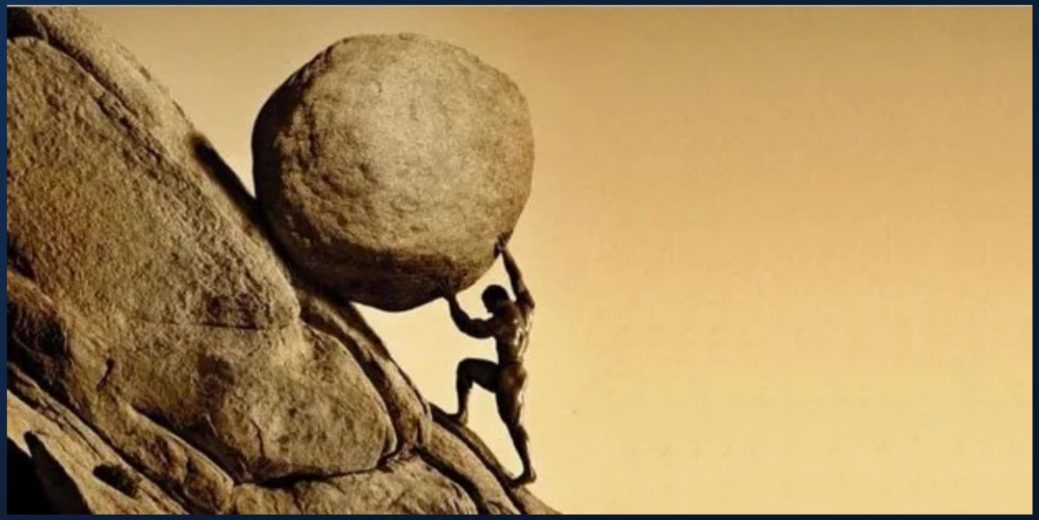
All entries in $\mathbb{F}_q$

Given $(\mathbf{A}, \mathbf{s}) \rightarrow$ **Find** $\boldsymbol{e}$

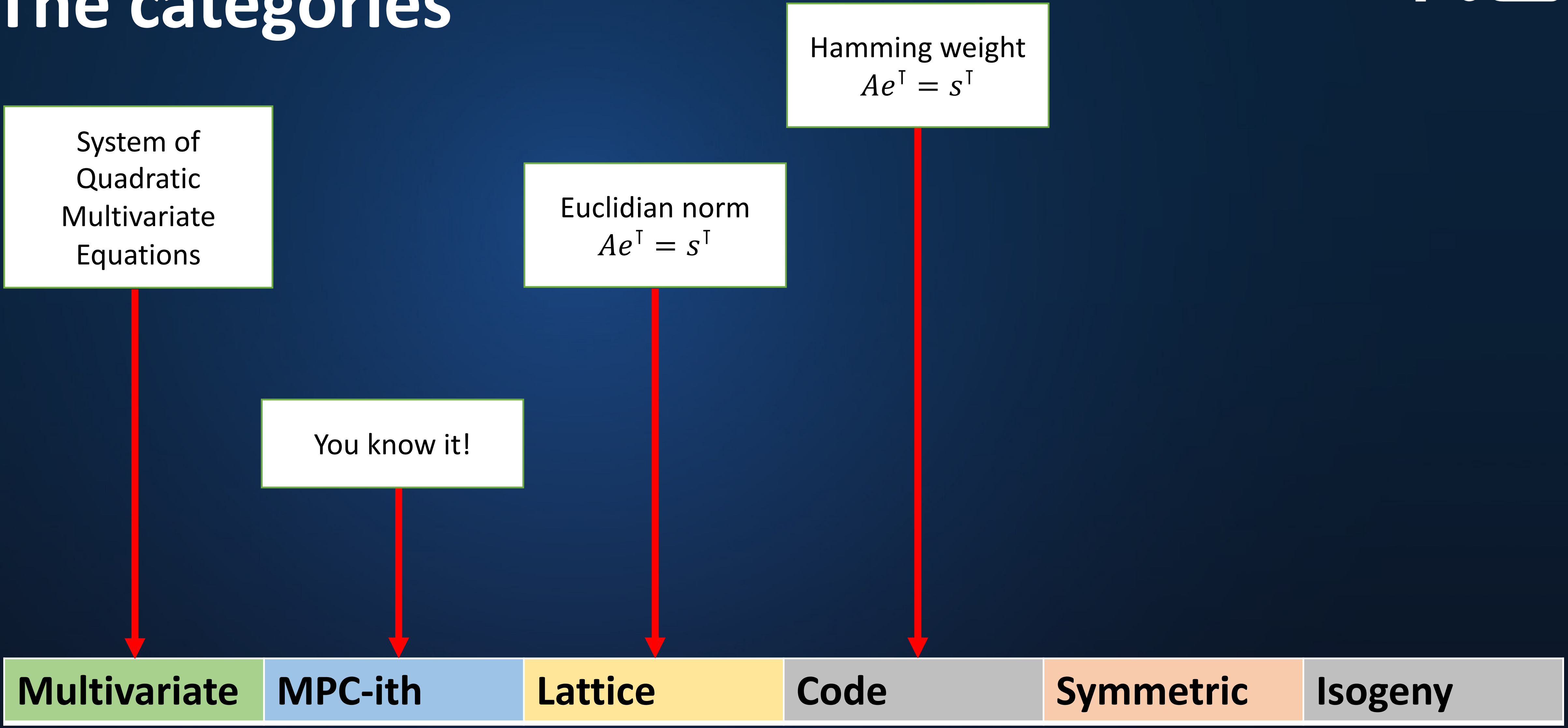
Linear algebra
Hard



Add a constraint
on the ``weight’’



The categories



System of Quadratic Multivariate Equations

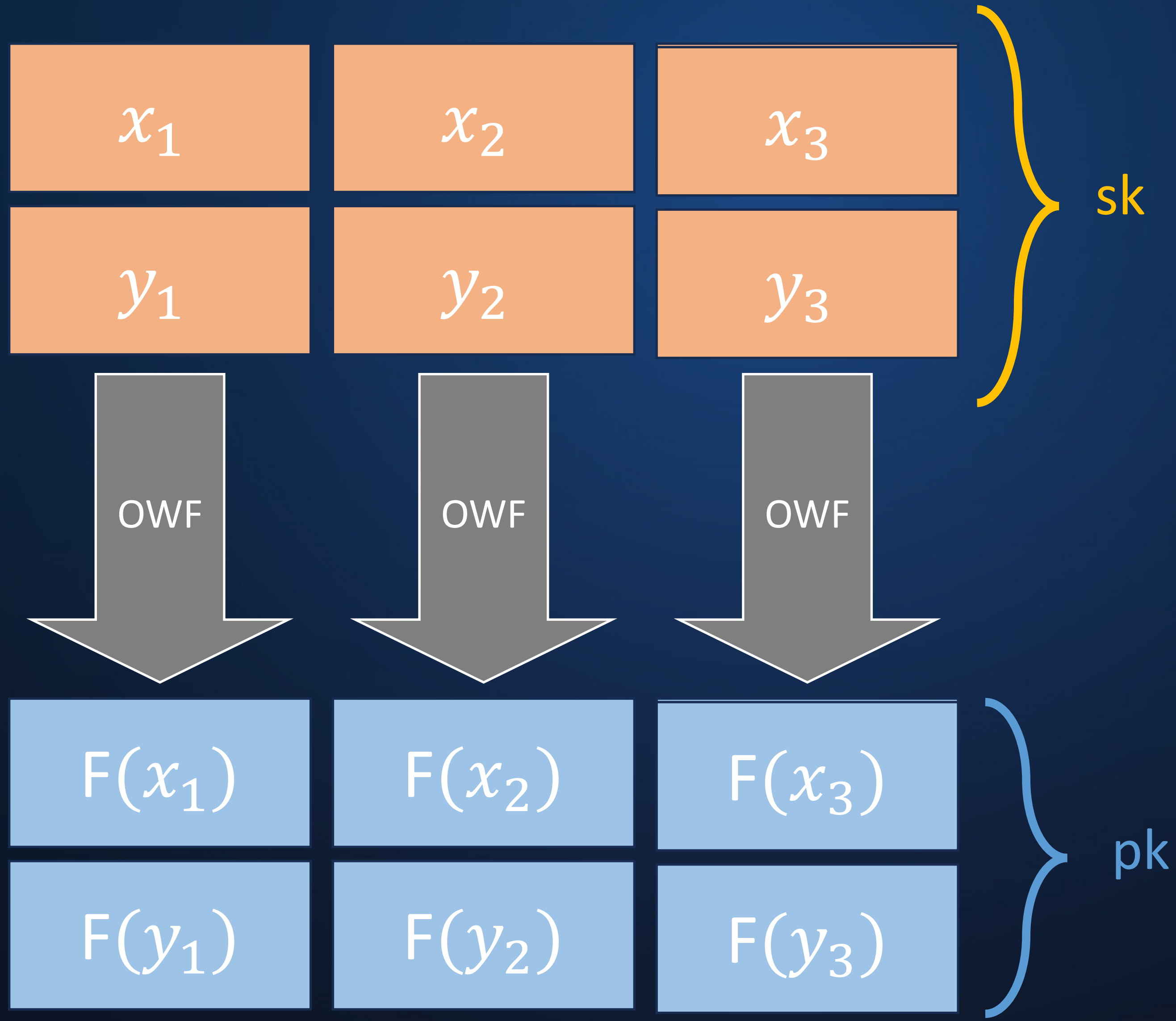
You know it!

Euclidian norm
$Ae^{\top} = s^{\top}$

Hamming weight
$Ae^{\top} = s^{\top}$

Multivariate	MPC-ith	Lattice	Code	Symmetric	Isogeny

Symmetric



x_1 x_2 x_3

y_1 y_2 y_3

sk

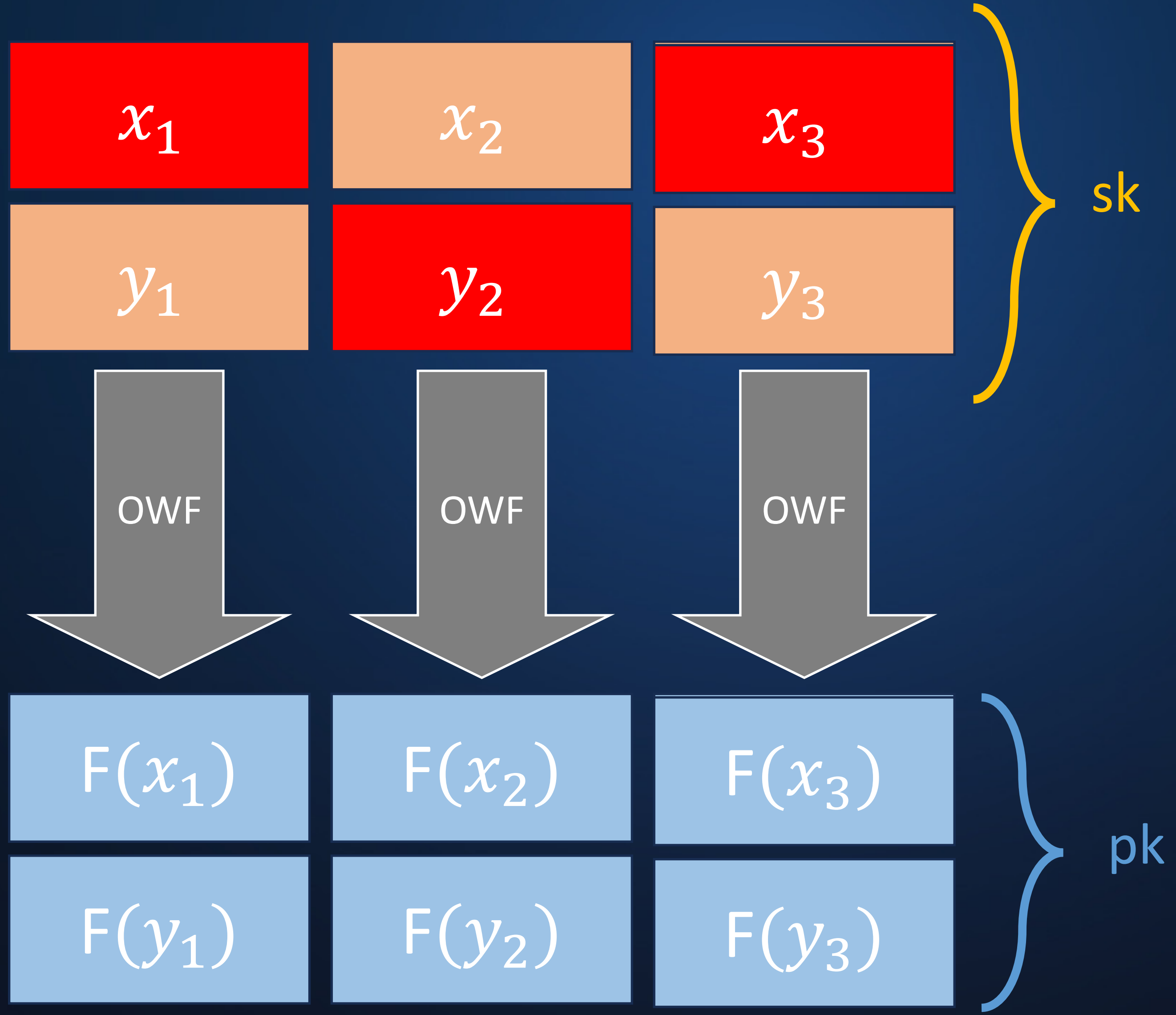
OWF OWF OWF

$F(x_1)$ $F(x_2)$ $F(x_3)$

$F(y_1)$ $F(y_2)$ $F(y_3)$

pk

Symmetric

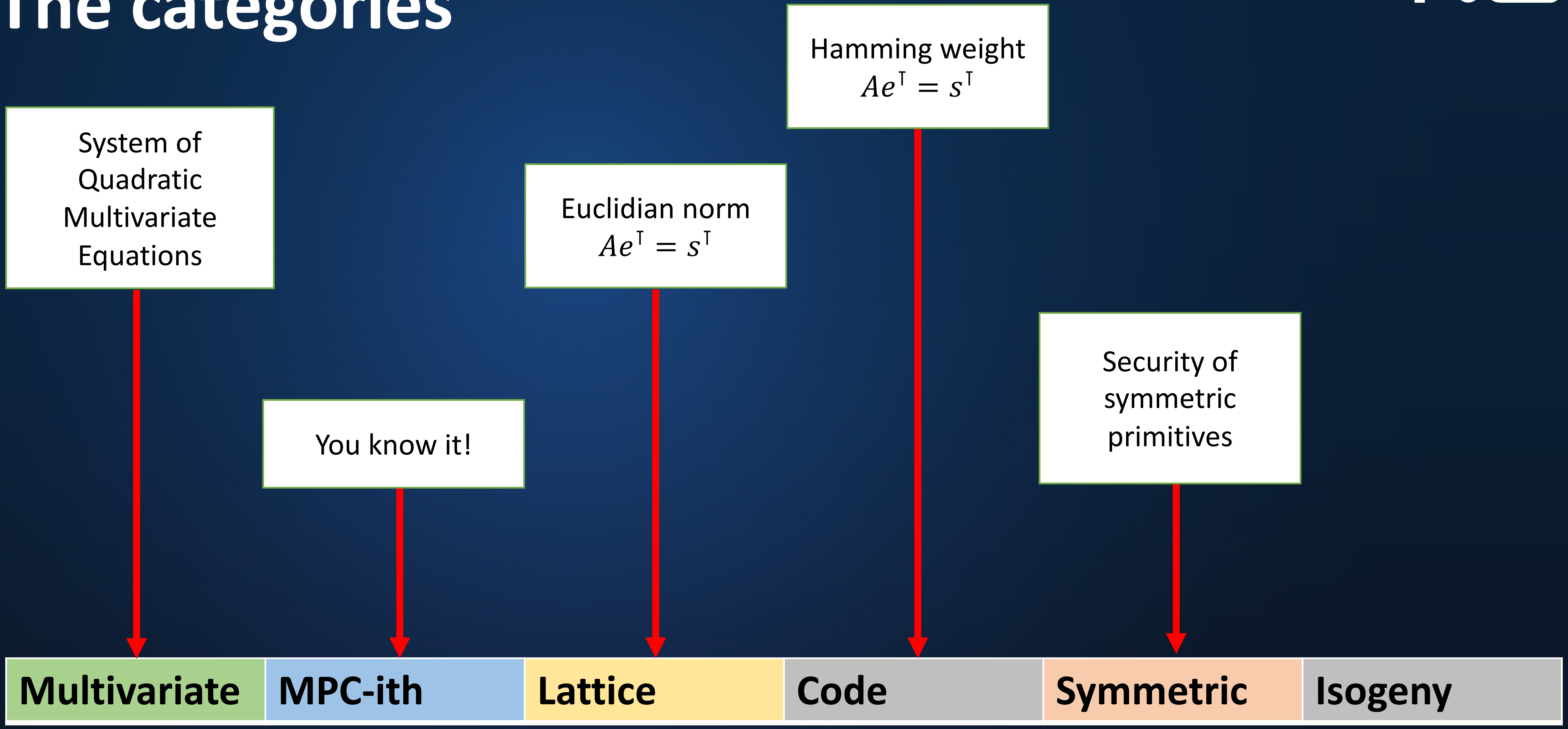


$$\mathrm{Sign}(010) = F(x_1) \mid F(y_2) \mid F(x_3)$$

A LOT of improvements:

- Merkle trees (FTS)
- Winternitz (OTS)
- etc.
- SPHINCS+

The categories



System of Quadratic Multivariate Equations

You know it!

Euclidian norm $Ae^{\top} = s^{\top}$

Hamming weight $Ae^{\top} = s^{\top}$

Security of symmetric primitives

Multivariate

MPC-ith

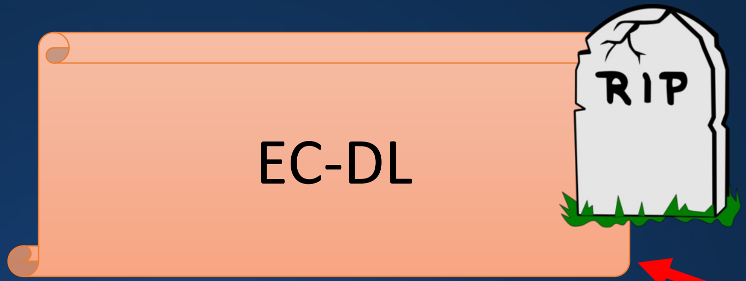
Lattice

Code

Symmetric

Isogeny

Isogeny



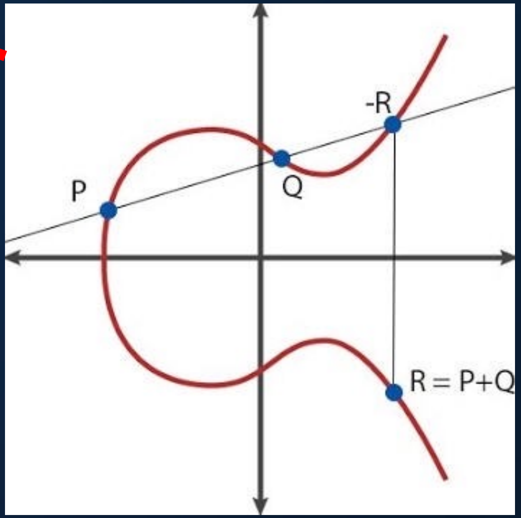
EC-DL

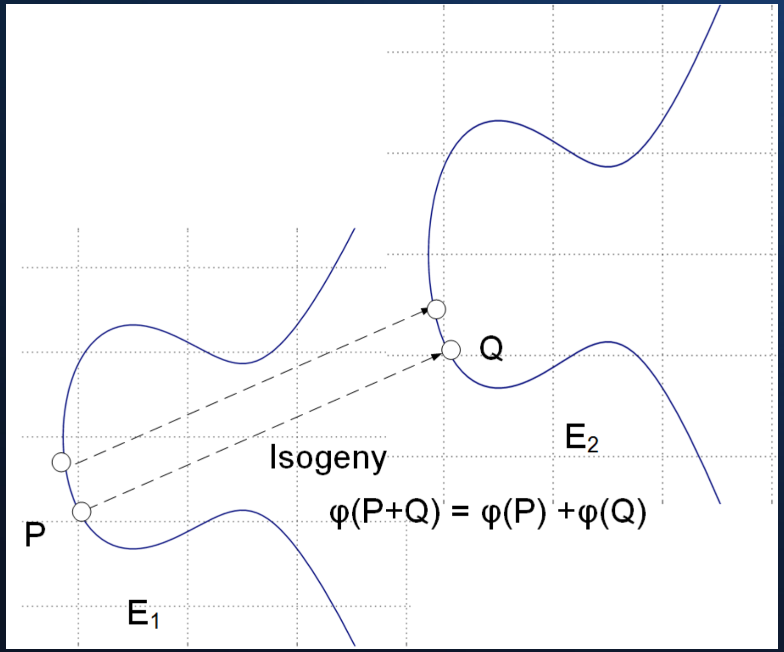
Elliptic curve

$$y = x^3 + ax + b$$

Points in $\mathbb{F}_q$

Abelian group

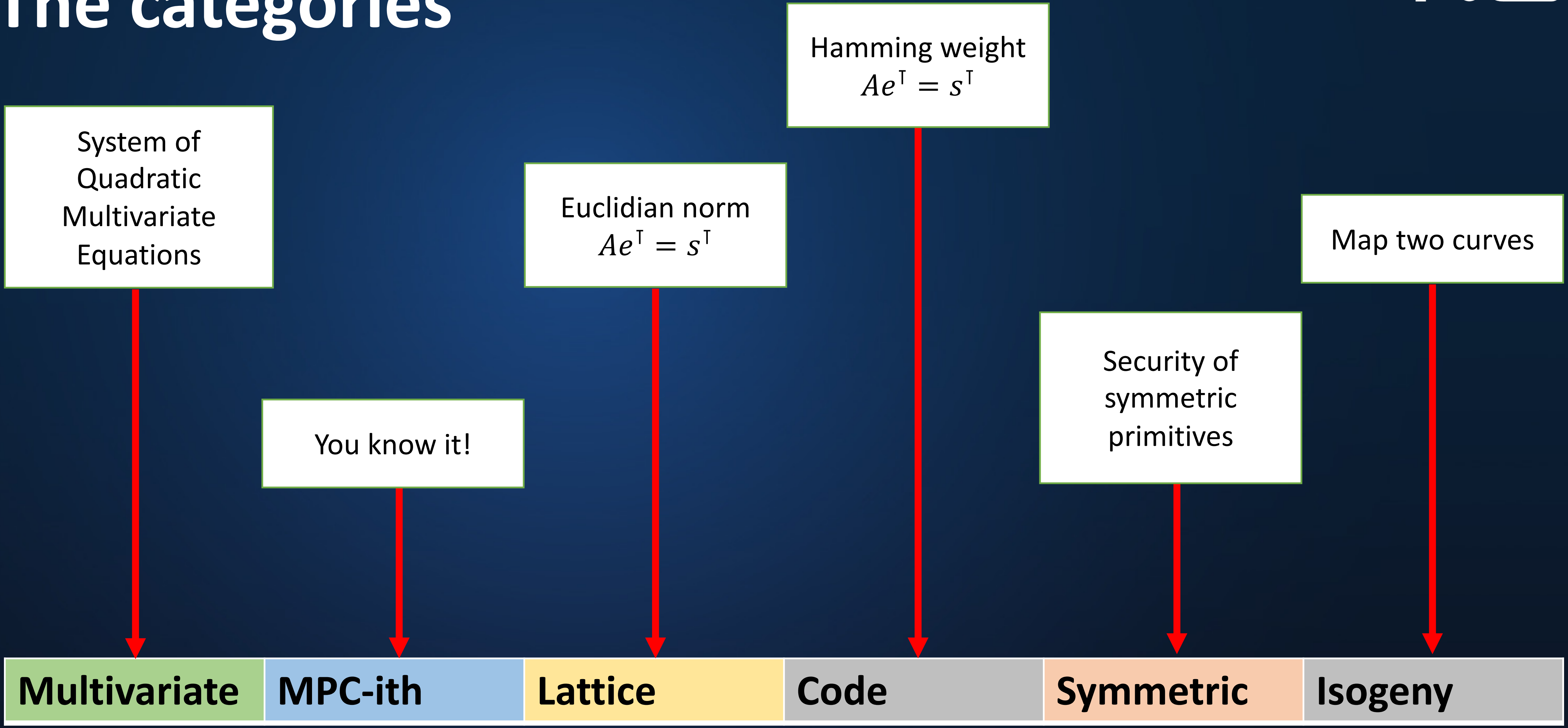




An isogeny ϕ between curves E_1 and E_2 is a group homomorphism $E_1 \longrightarrow E_2$.

(usually defined by its kernel)

The categories



System of Quadratic Multivariate Equations

You know it!

Euclidian norm $Ae^\top = s^\top$

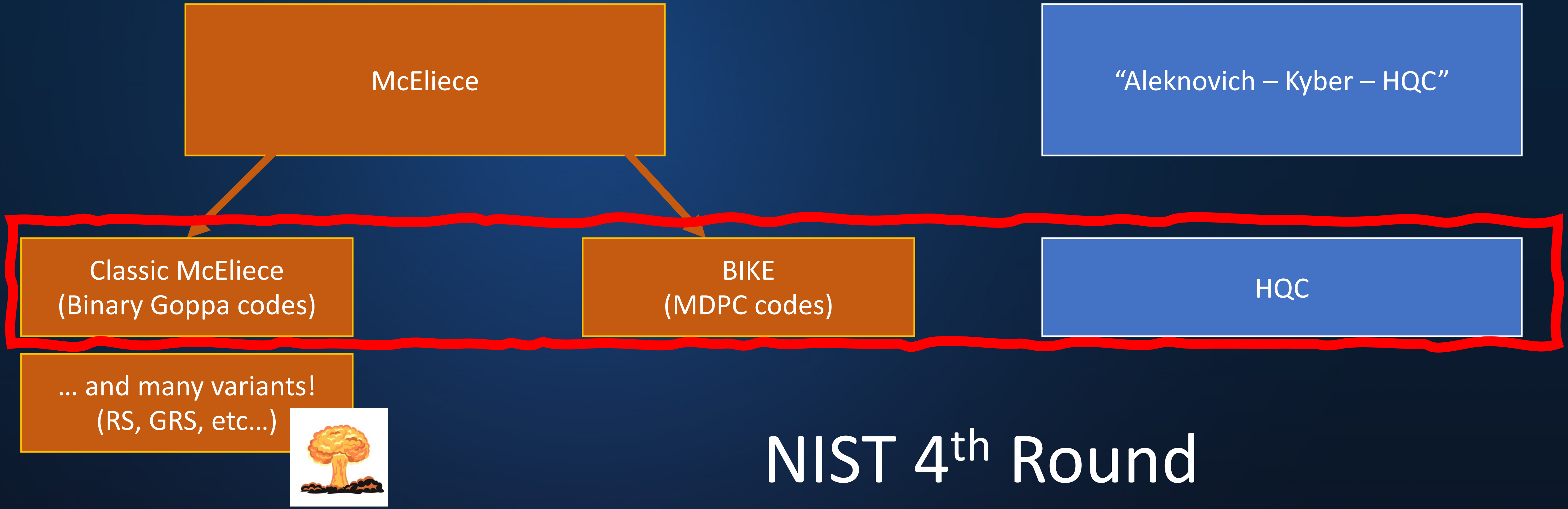
Hamming weight $Ae^\top = s^\top$

Security of symmetric primitives

Map two curves

Multivariate | **MPC-ith** | **Lattice** | **Code** | **Symmetric** | **Isogeny**

Code-based keygens in a few words



McEliece

"Aleknovich – Kyber – HQC"

Classic McEliece
(Binary Goppa codes)

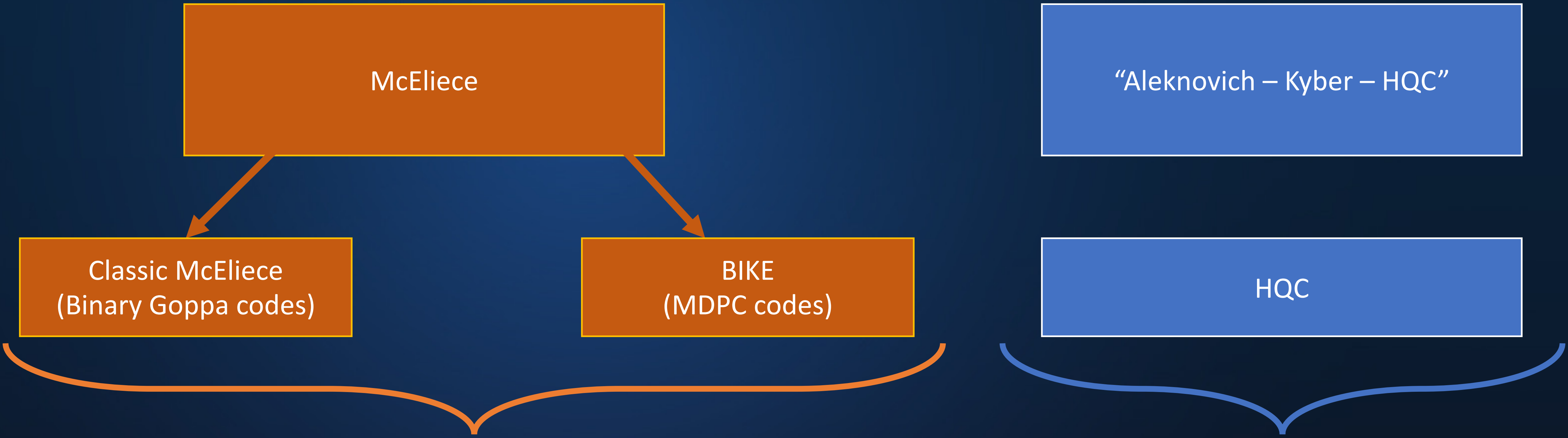
BIKE
(MDPC codes)

HQC

… and many variants!
(RS, GRS, etc…)

NIST 4th Round

Keygens in a few words



McEliece

Classic McEliece
(Binary Goppa codes)

BIKE
(MDPC codes)

“Aleknovich – Kyber – HQC”

HQC

« Hide the structure of a structured code »

Binary Goppa code

Q-Cyclic - Sparse

Q-Cyclic instance of $Ae^\intercal = s^\intercal$

Row echelon form / Gaussian elimination

Matrix-vector product

BIKE (QC-MDPC) : Quasi-Cyclic - Sparse

Row echelon form / Gaussian elimination

$$sk := \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \end{array}\right]$$

$$\mathrm{p}k := \left[\begin{array}{ccccc|ccccc} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \end{array}\right]$$

Polynomials modulo $(X^n - 1)$

$$R := \frac{\mathbb{F}_2[X]}{(X^n - 1)} \cong C \subset \mathbb{F}_2^{n \times n}$$

$$sk := (\mathrm{A}, \mathrm{B}) = (X^4 + X + 1, X^3 + X + 1) \in R^2$$

$$pk := (1, \mathrm{A}^{-1}\mathrm{B}) = (1, X^4 + X^3 + X^2) \in R^2$$

Feel free to contact me for more info on:

- multivariate-based cryptography ♥

- code-based cryptography ♥

maxime.bros@nist.gov