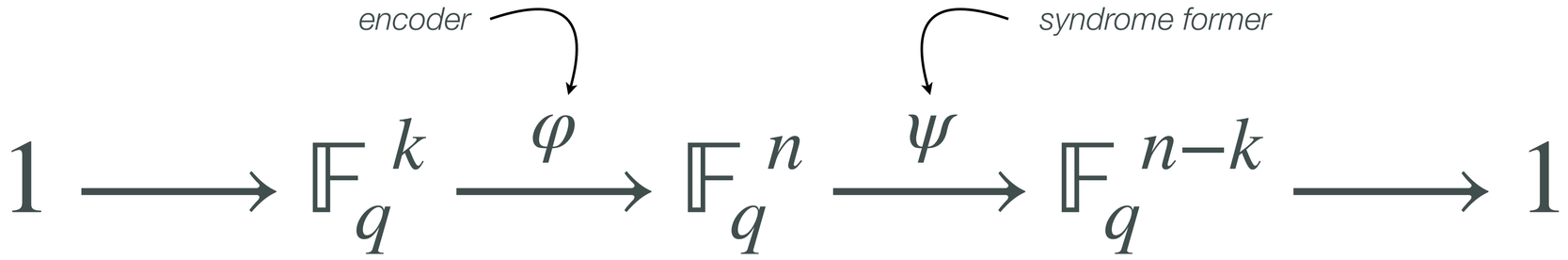
From Curves To Codes

(and back again)

Krijn Reijnders, COSIC, KU Leuven

KU LEUVEN



Linear Code

Code: k-dimensional subspace $C = \operatorname{im}\varphi = \ker\psi$ of $\mathbb{F}_q^{\,n}$

- choose bases, then write φ as a $k \times n$ matrix G
- similarly, write ψ as a $(n-k) \times n$ matrix H
- then also $H \cdot G^t = 0$

with a **metric** $d : \mathbb{F}_q^n \times \mathbb{F}_q^n \to \mathbb{R}$

- which implies a **weight** on $\mathbb{F}_q^n$ by $w(v) = d(v,0)$
- and a **minimum distance** $d_{\min} = \min_{c \in C} w(c)$

1

Hamming metric

Just the number of indices such that $v_i \neq w_i$

2

Rank metric

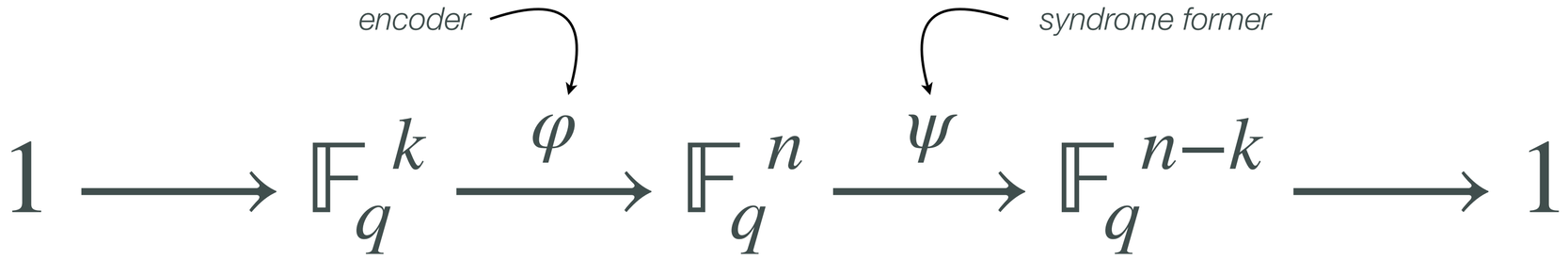
Let $V = \mathbb{F}_q^{n \times m}$ then for matrices A, B, set $d(A,B) = \operatorname{Rank}(A-B)$

3

Lee metric

Let $|\alpha|_L = \min(\alpha, q-\alpha)$, then $d(v,w) := \sum |v_i - w_i|_L$

KU LEUVEN



intermezzo

“Traditional” code-based cryptography relies on **syndrome decoding**.

Rephrased simply, take a code $C \subseteq \mathbb{F}_q^n$ and hide a low-weight code word $\epsilon \in \mathbb{F}_q^n$ in $C' = C + \epsilon$.

Given C', can you find ϵ?

(This is the basis for **McEliece**, **BIKE**, **HQC, CROSS,** etc. etc. etc. but we do not care about these today: we want **group actions!**)

$$C \xrightarrow{\mu} D$$

Q

Given equivalent C and D,
how hard to find μ?

Isometry

Linear map $\mu : C \to D$ that "preserves the weight" of codewords:

- $c \in C$ and $\mu(c) \in D$ have the same weight
- then the codes C and D are **equivalent**

Violetta Weger

Technical University of Munich, Germany

How hard is code equivalence really?

KU LEUVEN

(local) $C \xrightarrow{\mu} D$

$V \xrightarrow{\mu} V$ *(global)*

with $\mu(C) = D$

Isometry

Linear map $\mu : C \to D$ that "preserves the weight" of codewords:

- $c \in C$ and $\mu(c) \in D$ have the same weight
- then the codes C and D are **equivalent**

Local/Global

There is a significant difference in local and global isometries

- any global isometry $\mu : V \to V$ with $\mu(C) = D$ **descends** to a local isometry $\mu_{|C} : C \to D$
- not every local isometry **lifts** per se to a global isometry, depends on the metric!
  - Hamming metric: **MacWilliams Extension Theorem** shows we can *always* lift
  - Rank Metric: Gorla and Salizzoni [1] give ample examples of **obstructions** to lifting

KU LEUVEN

[1] Elisa Gorla and Flavio Salizzoni. "MacWilliams' Extension Theorem for rank-metric codes." *Journal of Symbolic Computation* 122 (2024): 102263.

$$V \xrightarrow{\mu} V$$

with $\mu(C) = D$

(global)

typical codeword

$(1,0,3,5,2,4,0,7,0,2)$

typical codeword

$$\begin{pmatrix} 1 & 0 & 3 \\ 0 & 3 & 7 \\ 4 & 4 & 1 \end{pmatrix}$$

Local/Global

There is a significant difference in local and global isometries

- any global isometry $\mu : V \to V$ with $\mu(C) = D$ **descends** to a local isometry $\mu_{|C} : C \to D$
- not every local isometry **lifts** per se to a global isometry, depends on the metric!
  - Hamming metric: **MacWilliams Extension Theorem** shows we can *always* lift
  - Rank Metric: Gorla and Salizzoni [1] give ample examples of **obstructions** to lifting

1

Hamming Metric

- can permute coordinates
- can rescale coordinates
- that's all!

$$\mathcal{I}(\mathbb{F}_q^n) = \{\ DP, \quad P \in S_n,\ D = \mathrm{diag}(\lambda_i)\ \}$$

$$c \mapsto cDP, \qquad c \in C$$

(or, when choosing a basis)

$$G \mapsto SGDP \qquad S \in \mathrm{GL}_k(q)$$

2

Rank Metric
(global)

- can multiply on the left
- can multiply on the right
- that's all!

$$\mathcal{I}(\mathbb{F}_q^{n\times m}) = \{\ (A,B), \quad A \in \mathrm{GL}_n(q), B \in \mathrm{GL}_m(q)\ \}$$

$$M \mapsto AMB, \qquad M \in C$$

(we may still choose a basis, and change basis by $T \in \mathrm{GL}_k(q)$ but the notation gets confusing)

KU LEUVEN

[1] Elisa Gorla and Flavio Salizzoni. "MacWilliams' Extension Theorem for rank-metric codes." *Journal of Symbolic Computation* 122 (2024): 102263.

NOT
commutative

effective
group action

cryptographic
group action

Code Equivalence

In summary:

- take **vector space** $\mathbb{F}_q^n$ over finite field $\mathbb{F}_q$
- code $C \subseteq \mathbb{F}_q^n$ is k-dim. subspace w/ metric
- group of **global isometries** $\mathscr{I} := \mathscr{I}(\mathbb{F}_q^n)$
- acts on set of dim-k codes $\mathrm{Gr}_k(\mathbb{F}_q^n)$

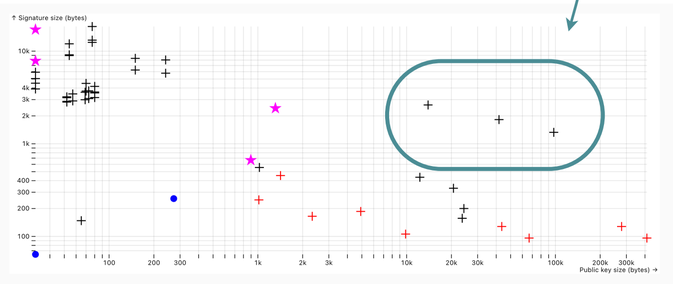
$$\mathscr{I} \times \mathrm{Gr}_k \to \mathrm{Gr}_k$$
$$(\mu, C) \mapsto \mu(C)$$

Hamming

LESS(-FM)

Rank

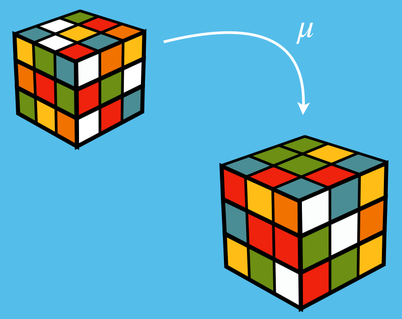
MEDS & **ALTEQ**



KU LEUVEN

1

Code Equivalence



2

From Curves To Codes

$$\begin{array}{ccc} \mathbf{ISO} & \rightarrow & \mathit{GEN} \\ \downarrow & & \downarrow \\ \mathit{METR} & \rightarrow & \mathbf{IES} \end{array}$$

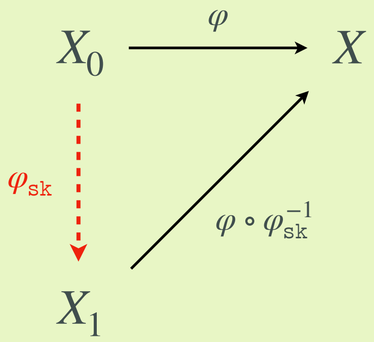
3

(*and back again*)

$$\begin{array}{ccc} \mathbf{OSI} & \leftarrow & \mathit{GEN} \\ \uparrow & & \uparrow \\ \mathit{METR} & \leftarrow & \mathbf{IES} \end{array}$$

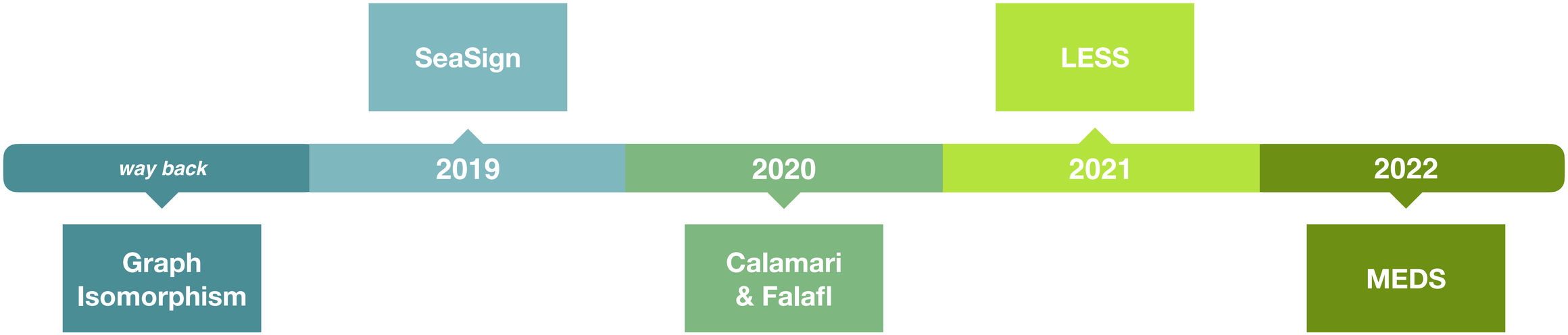
From Curves To Codes

The Triangle

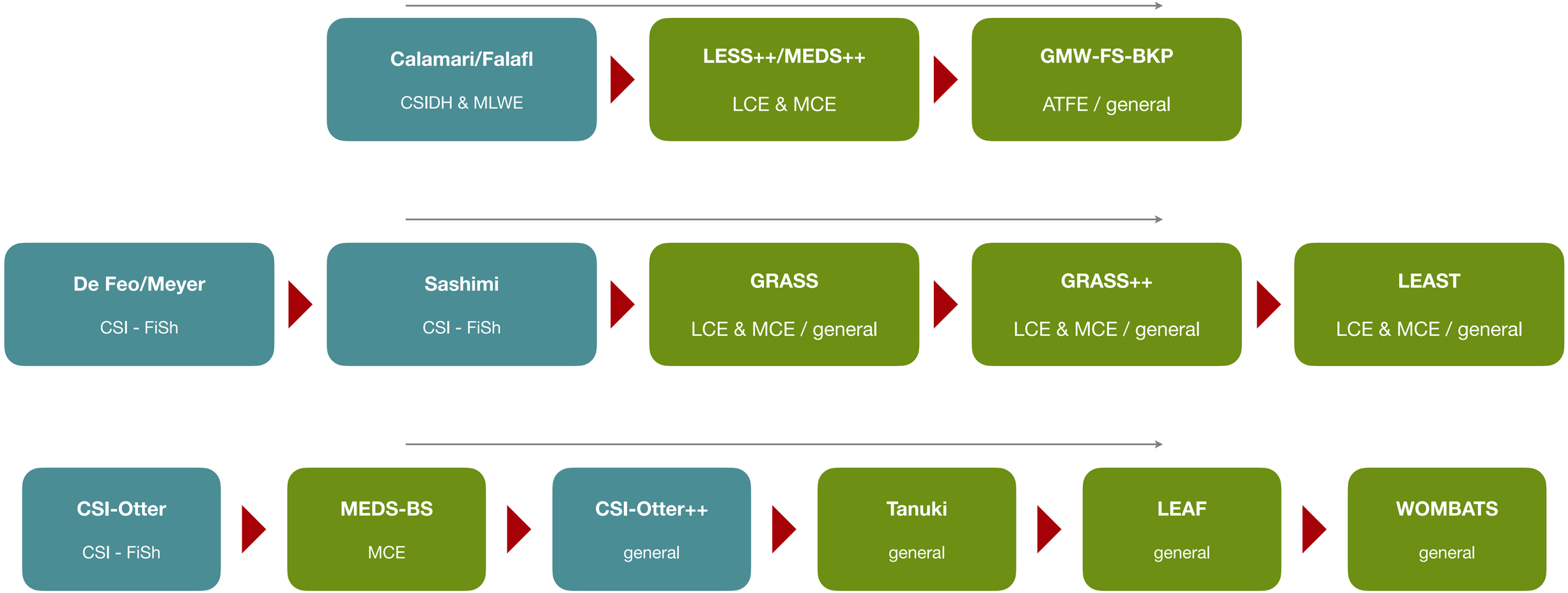


Given a public element X_0

- secret (iso)morphism $\varphi_{\mathtt{sk}} : X_0 \to X_1$
- public key X_1, commit with random $\varphi : X_0 \to X$
- challenged by bit: either show φ or $\varphi \circ \varphi_{\mathtt{sk}}^{-1}$
- zero-knowledge proof of $\varphi_{\mathtt{sk}}$



From Curves To Codes



2

From Curves To Codes

CSI-Otter++

general

CSI-fish with **O**r-proof **T**wisted **Thre**-**E**-**R**ound protocol

Tanuki

general

Three-move **I**ndistinguishable signing with **UN**iform-weight challenge from **K**rypto group **A**ction (**TIUNKA**, then shuffle)

Capybara/Tsubaki

Compact **A**ction factorization **P**roofs **Y**ielded **B**y **A** **RA**ndom function and
Twist-**S**qa**U**re-**BA**sed twea**K** from **I**sogenies (sic)

Yi-Fu Lai

Incredibly **F**orced **A**cronym **I**nventor — **Y**et **U**niversally **L**iked (shuffled)

WOMBATS

general

KU LEUVEN

2

From Curves To Codes

Q Can we instantiate **CSI-Otter** with **qt-Pegasis?**

qtP is effective…

…but CSI-Otter needs order of class group, right?

A **Yes!**

(Vanzeir's Thesis, 2026)

	COMMUTATIVE			NON-COMMUTATIVE		
	REGA	**EGA**	**KEGA**	**REGA**	**EGA**	**KEGA**
action	CSIDH CORAL	PEGASIS qt-P	CSI-FISH* SCALLOP* KLaPoTi			LCE MCE
scheme	CSIDH MANY!	MORE!	De Feo-Meyer CSI-Otter	LESS/MEDS	ALL (?)	

! a significant part of **isogenists** have "forgotten" notion of **KEGA**

! as all isometries are **KEGA**, schemes are fuzzy about needs

KU LEUVEN

2

From Curves To Codes

!

a significant part of **isogenists** have “forgotten” notion of **KEGA**

!

as all isometries are **KEGA**, schemes are fuzzy about needs

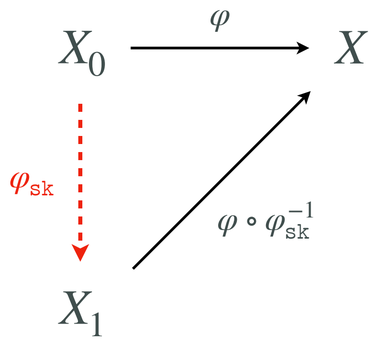
My Dream

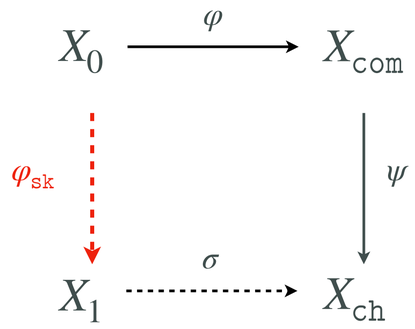
Q

Can we instantiate **Scheme X** with **Action Y?**

2

From Curves To Codes





Triangles

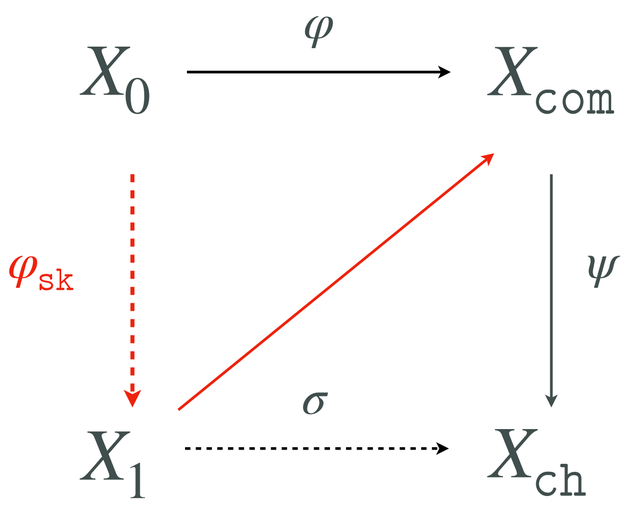
- 1-bit challenge, repeat $\approx \lambda$ times (plus tricks)
- theoretical lower bound on sig. size $\Omega(\lambda^2/\log \lambda)$

Squares

- λ-bit challenge, only one round!
- requires additional structure

2

From Curves To Codes



?

Signature as
$\sigma := \varphi_{\mathtt{sk}}^{-1} \circ \varphi \circ \psi$

!

Doesn't prove $\varphi_{\mathtt{sk}}$, only
$\varphi_{\mathtt{sk}}^{-1} \circ \varphi$

?

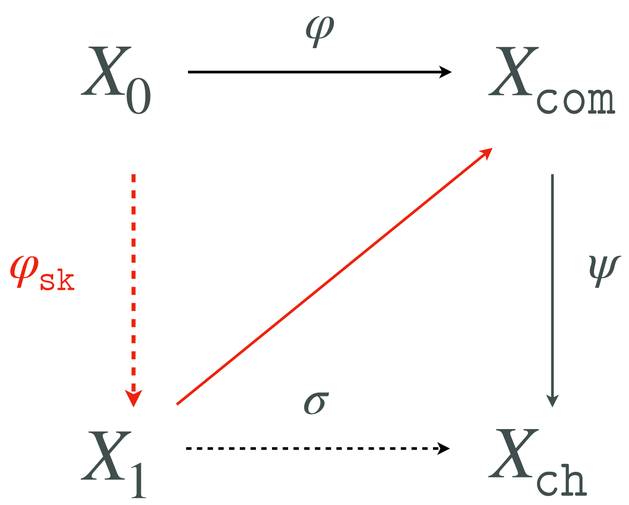
Different response
$\sigma : X_1 \to X_{\mathtt{ch}}$?

!

Implies **non-trivial**
$\mu : X_1 \to X_1$ **(!)**

2

From Curves To Codes



My Dream (2)

1. Can we give an **invariant** or **impossibility result** for the *code equivalence* instantiation?
2. Can we deduce **concrete criteria** for *group action* properties to instantiate this?
3. If not, can we **pinpoint** where this approach fails between *category* and *group action*?

Category

1. must use object with non-trivial $\mathrm{End}(X_0)$
2. hardness assumption on computing $\mathrm{End}(X)$
3. knowledge of End is contagious
4. knowledge can transform signature σ
5. distinguishing invariant for σ for ZK-proof

Group Action

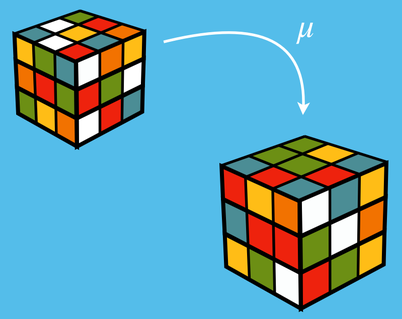
1. non-trivial stabilizer group of X_0, e.g. $g \star X_0 = X_0$
2. hard to compute for random set element X
3. knowledge of stab. is **contagious**
4. knowledge of stab. X_1 can transform σ
5. need stab. X_1 for **correct** signature (ZK)

Code Equivalence

1. must take starting code with non-trivial $\mathrm{Aut}(C_0)$
2. **Research Question**: hardness of computing $\mathrm{Aut}(C)$ for random C
3. knowledge of Aut is contagious
4. knowledge can transform signature σ
5. **Research Question**: distinguishing invariant for σ for ZK-proof?

1

Code Equivalence



2

From Curves To Codes

$$\begin{array}{ccc} \mathbf{ISO} & \rightarrow & \mathit{GEN} \\ \downarrow & & \downarrow \\ \mathit{METR} & \rightarrow & \mathbf{IES} \end{array}$$

3

(*and back again*)

$$\begin{array}{ccc} \mathit{METR} & \leftarrow & \mathbf{IES} \\ \uparrow & & \uparrow \\ \mathbf{OSI} & \leftarrow & \mathit{GEN} \end{array}$$

3

(and back again)

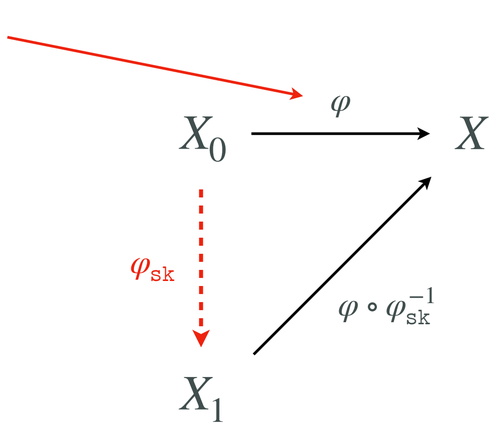
My Dream (3)

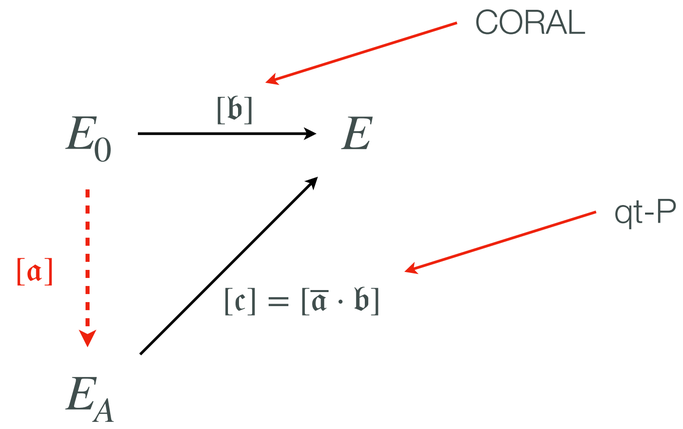
Mix-and-Match: combine restricted and effective group actions in advanced protocols

1. Using qt-Pegasis, we can instantiate a significant amount of advanced protocols (see Dream (1))
2. However, many group action evaluations in these protocols do **not** require effectiveness!
3. Replace these evaluations by **faster** (restricted) evaluations, using CORAL

MEDS:
sample φ smart so evaluation is faster

(effectively, we move from EGA to REGA!)





using class group actions, similarly go from EGA (qt-P) to REGA (CORAL)

(and back again)

Code Equivalence

$$C \sim D$$

There is an isometry $\mu \in \mathcal{I}$ such that $D = \mu(C)$.

E-Code Equivalence

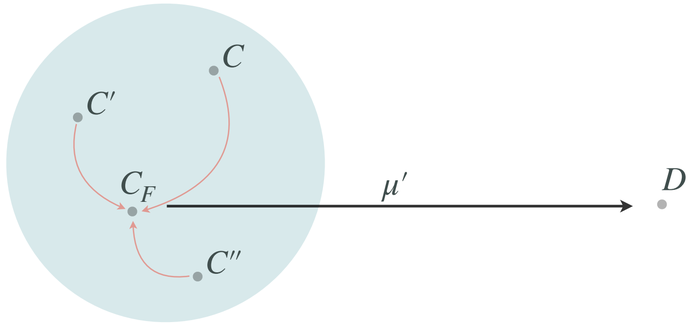
$$C \sim_E D$$

There is an isometry $\mu \in E \subseteq \mathcal{I}$ such that $D = \mu(C)$.

canonical form

Let F be a subgroup of $E \subseteq \mathcal{I}$ such that $\sim_F$ is easy, but $\sim_E$ is hard.
Let $C \sim_E D$ with $\mu(C) = D$,

- Let $F\mu = \{\gamma \circ \mu \mid \gamma \in F\}$, then *any* $\chi \in F\mu$ can prove $C \sim_E D$
- Commit to *canonical representation* $C_F \sim_F C$
  - C_F efficiently computable given C
  - C_F is the same for all codes in $F(C) = \{\gamma(C) \mid \gamma \in F\}$
- response can now be μ' such that $D = \mu'(C_F)$



Round 1
8.4 kilobyte

Round 2
2.6 kilobyte

3

(and back again)

Group Factorisation

Let G acting on X be a cryptographic group action, and let $G = G_1 \rtimes G_2$. Assume the associated decomposition $g \to (g_1, g_2)$ is efficient.

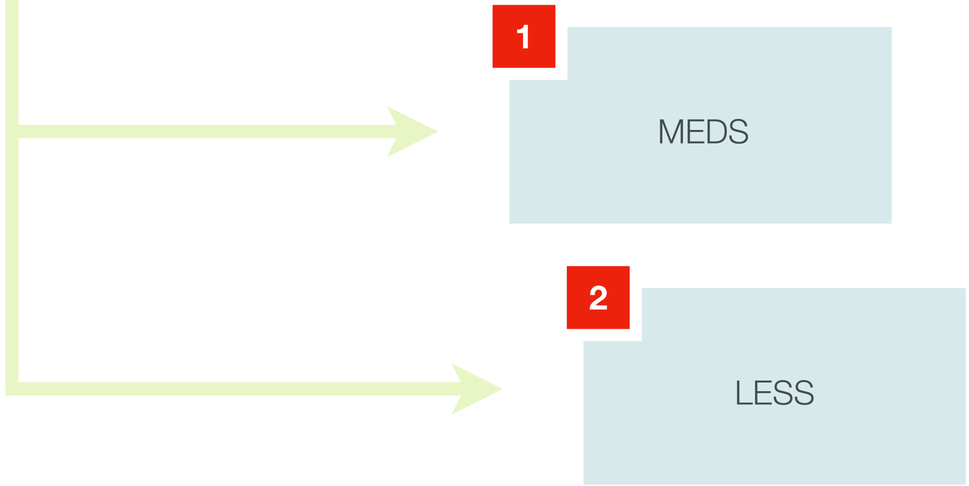
- if vectorisation for the action by G_1 is *easy,* but by G_2 is *hard,*
- and there exists efficient algorithm $\mathtt{OE}$ acting as *canonical representation*

$$x_1 = (g_1, e) \star x_0 \qquad \Rightarrow \qquad x_1 = \mathtt{OE}(x_0, x_1) \star x_0$$

- then can often use g_2 as a response, instead of full $g = (g_1, g_2)$

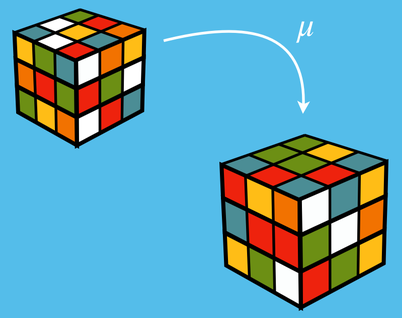
Q

Group factorisation
or canonical forms
beyond code equivalence?



1

Code Equivalence



2

From Curves To Codes

$$\begin{array}{ccc} \mathbf{ISO} & \rightarrow & \mathit{GEN} \\ \downarrow & & \downarrow \\ \mathit{METR} & \rightarrow & \mathbf{IES} \end{array}$$

3

(*and back again*)

$$\begin{array}{ccc} \mathbf{SEI} & \leftarrow & \mathit{METR} \\ \uparrow & & \uparrow \\ \mathit{NEG} & \leftarrow & \mathbf{OSI} \end{array}$$

Any Questions?