Effective Group Actions

The road to PEGASIS

Joint work with Pierrick Dartois, Tako Boris Fouotsa, Arthur Herlédan Le Merdy, Riccardo Invernizzi, Damien Robert, Ryan Rueger, Frederik Vercauteren, Benjamin Wesolowski

Jonathan Komada Eriksen,
COSIC, KU Leuven

Diffie-Hellman

Setup parameters: $H = \langle h \rangle$, a cyclic group of order p

Alice **Bob**

$a \in (\mathbb{Z}/p\mathbb{Z})^\times$

$\xrightarrow{h^a}$

Diffie-Hellman

Setup parameters: $H = \langle h \rangle$, a cyclic group of order p

Alice | **Bob**

$a \in (\mathbb{Z}/p\mathbb{Z})^\times$ | $b \in (\mathbb{Z}/p\mathbb{Z})^\times$

Alice → Bob: h^a

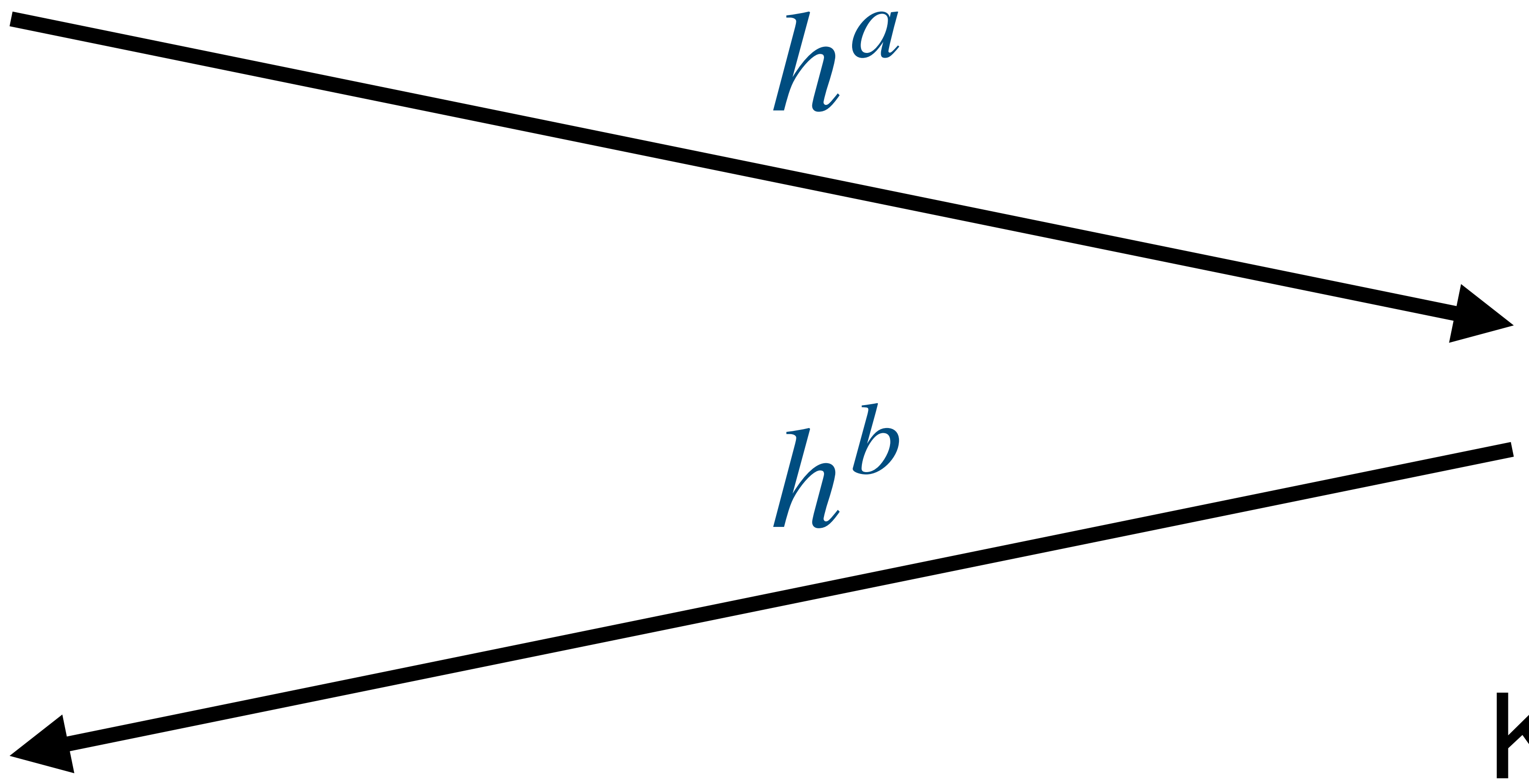
Bob → Alice: h^b

Diffie-Hellman

Setup parameters: $H = \langle h \rangle$, a cyclic group of order p

Alice | **Bob**

$a \in (\mathbb{Z}/p\mathbb{Z})^{\times}$ | $b \in (\mathbb{Z}/p\mathbb{Z})^{\times}$



Key = $(h^b)^a$ | Key = $(h^a)^b$

Group Actions

Group G, Set X

$$G \times X \to X$$
$$(g, x) \to g \star x$$

- For all $x \in X$, we have $1_G \star x = x$
- For all $x \in X$ and $g_1, g_2 \in G$, we have $(g_1 g_2) \star x = g_1 \star (g_2 \star x)$

Group Actions

Group G, Set X

$$G \times X \to X$$
$$(g, x) \to g \star x$$

- For all $x \in X$, we have $1_G \star x = x$
- For all $x \in X$ and $g_1, g_2 \in G$, we have $(g_1 g_2) \star x = g_1 \star (g_2 \star x)$

Free and Transitive: For all $x, y \in X$, there exists a unique $g \in G$ so $y = g \star x$

Group Actions

Group G, Set X

$$G \times X \to X$$
$$(g, x) \to g \star x$$

- For all $x \in X$, we have $1_G \star x = x$
- For all $x \in X$ and $g_1, g_2 \in G$, we have $(g_1 g_2) \star x = g_1 \star (g_2 \star x)$

Free and Transitive: For all $x, y \in X$, there exists a unique $g \in G$ so $y = g \star x$

Example: Let H be a cyclic group of order p.
Then $G = (\mathbb{Z}/p\mathbb{Z})^{\times}$ acts free and transitively on $X = H \backslash \{1_H\}$ by exponentiation

Diffie-Hellman as a group action

Setup parameters:

$H = \langle h \rangle$, a cyclic group of order p

Alice $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

Bob $b \in (\mathbb{Z}/p\mathbb{Z})^\times$

Alice → Bob: h^a

Bob → Alice: h^b

Key = $(h^b)^a$

Key = $(h^a)^b$

Setup parameters:

A group G, acting on X

a fixed $x \in X$

Alice $a \in G$

Bob

Alice → Bob: $a \star x$

Diffie-Hellman as a group action

Setup parameters:

$H = \langle h \rangle$, a cyclic group of order p

Alice		Bob
$a \in (\mathbb{Z}/p\mathbb{Z})^\times$		$b \in (\mathbb{Z}/p\mathbb{Z})^\times$
	h^a →	
	← h^b	
Key = $(h^b)^a$		Key = $(h^a)^b$

Setup parameters:

A group G, acting on X

a fixed $x \in X$

Alice		Bob
$a \in G$		$b \in G$
	$a \star x$ →	
	← $b \star x$	

Diffie-Hellman as a group action

Setup parameters:

$H = \langle h \rangle$, a cyclic group of order p

Alice $a \in (\mathbb{Z}/p\mathbb{Z})^\times$

Bob $b \in (\mathbb{Z}/p\mathbb{Z})^\times$

Alice → Bob: h^a

Bob → Alice: h^b

Key = $(h^b)^a$

Key = $(h^a)^b$

Setup parameters:

A group G, acting on X

a fixed $x \in X$

Alice $a \in G$

Bob $b \in G$

Alice → Bob: $a \star x$

Bob → Alice: $b \star x$

Key = $a \star (b \star x)$

Key = $b \star (a \star x)$

Hard problems:

Discrete logarithm: given h^a, h, find a

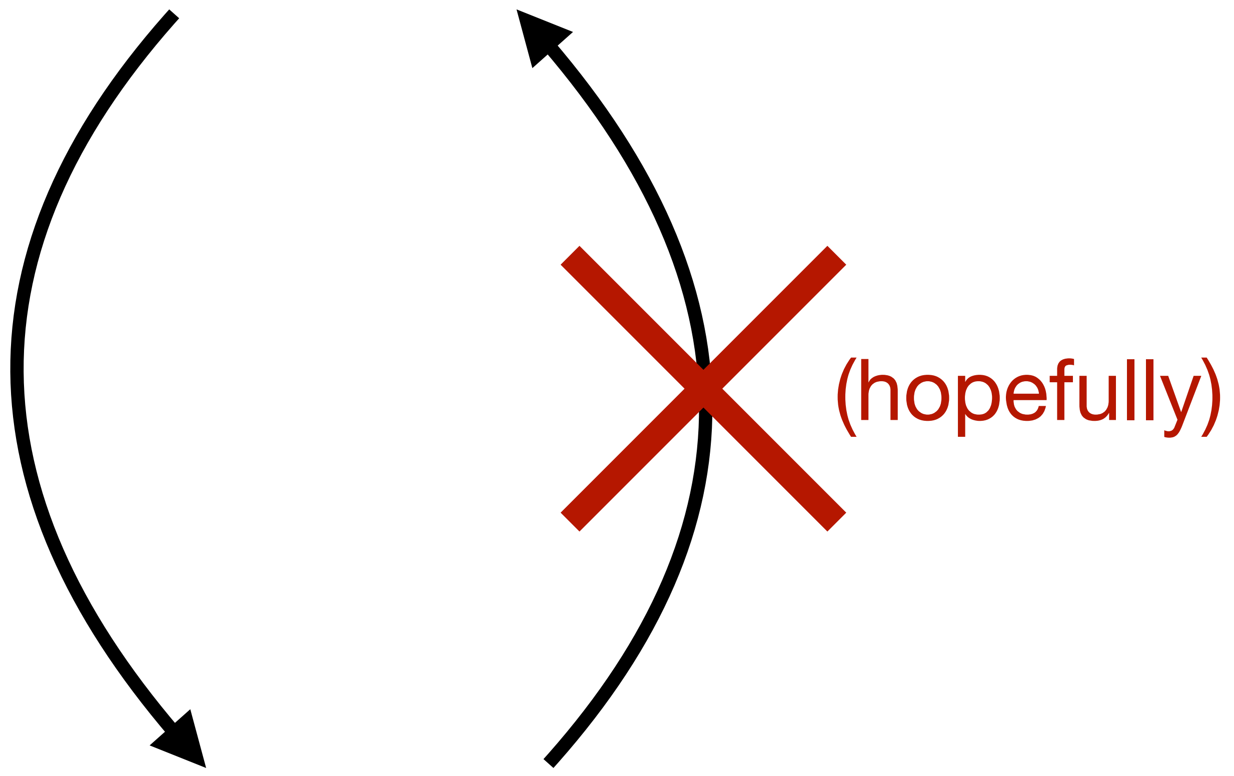
Hard problems:

Discrete logarithm: given h^a, h, find a

Vectorisation: given $a \star x, x$, find a

Hard problems:

Discrete logarithm: given h^a, h, find a



Vectorisation: given $a \star x, x$, find a

Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$

Peggy **Victor**

$$h_0 \xrightarrow{\;s\;} h_1$$

Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

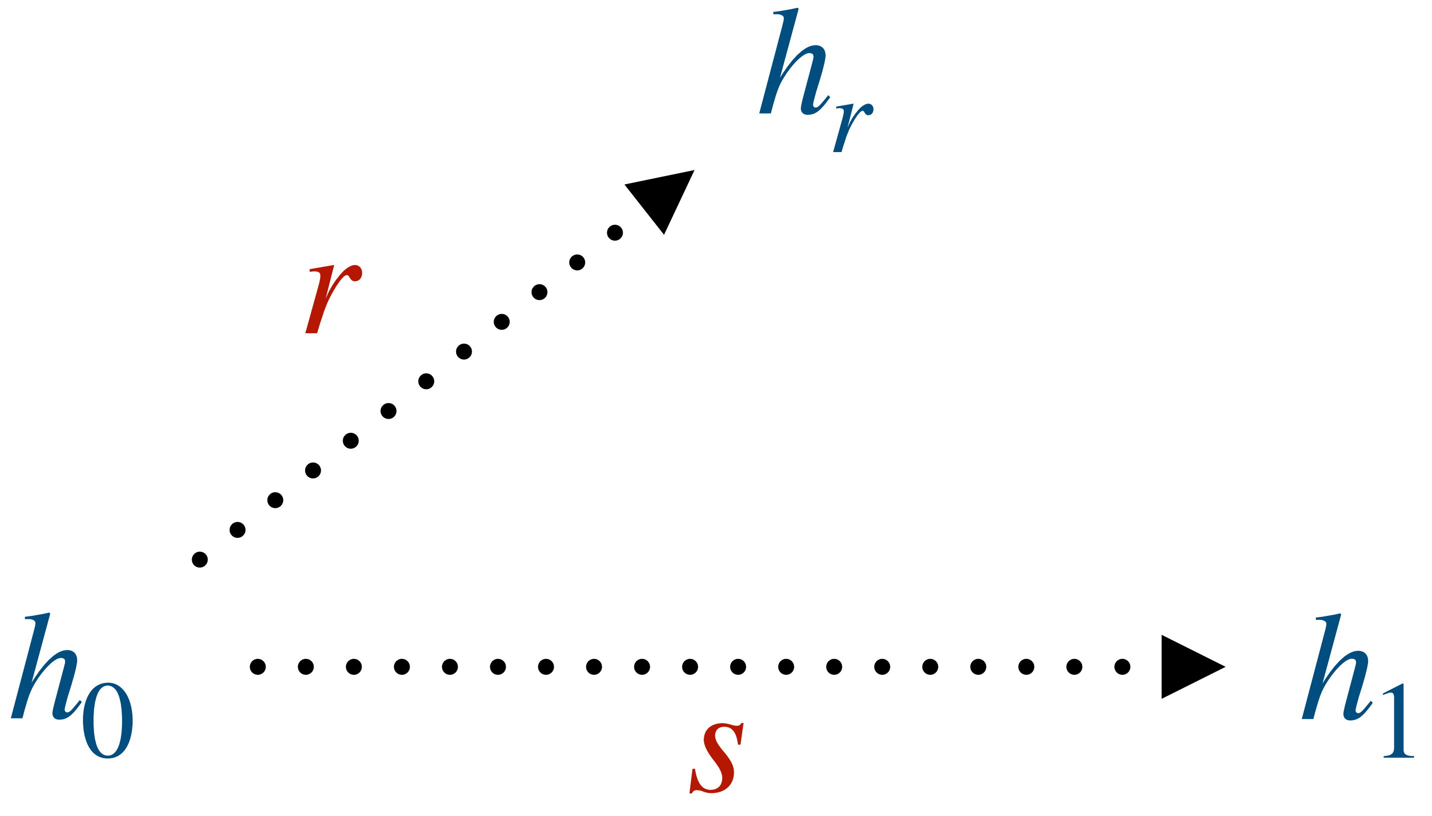
Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$

Peggy **Victor**

$r \in (\mathbb{Z}/p\mathbb{Z})^\times$

$h_r := h^r$ →



Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$

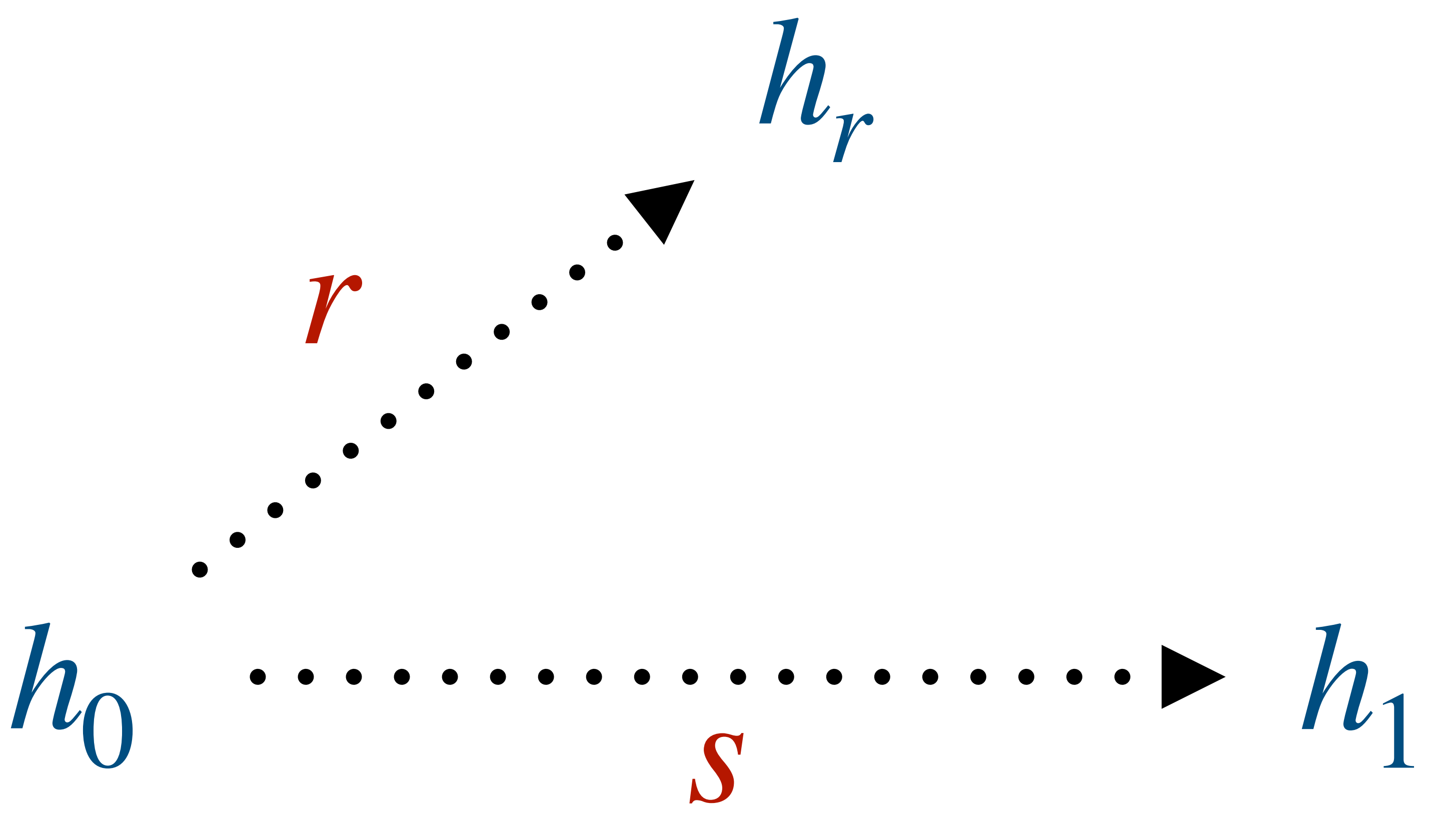
Peggy | **Victor**

$r \in (\mathbb{Z}/p\mathbb{Z})^\times$

$h_r := h^r$ →

$b \in \{0,1\}$

← b



Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$

Peggy | **Victor**

$r \in (\mathbb{Z}/p\mathbb{Z})^\times$

$h_r := h^r$ →

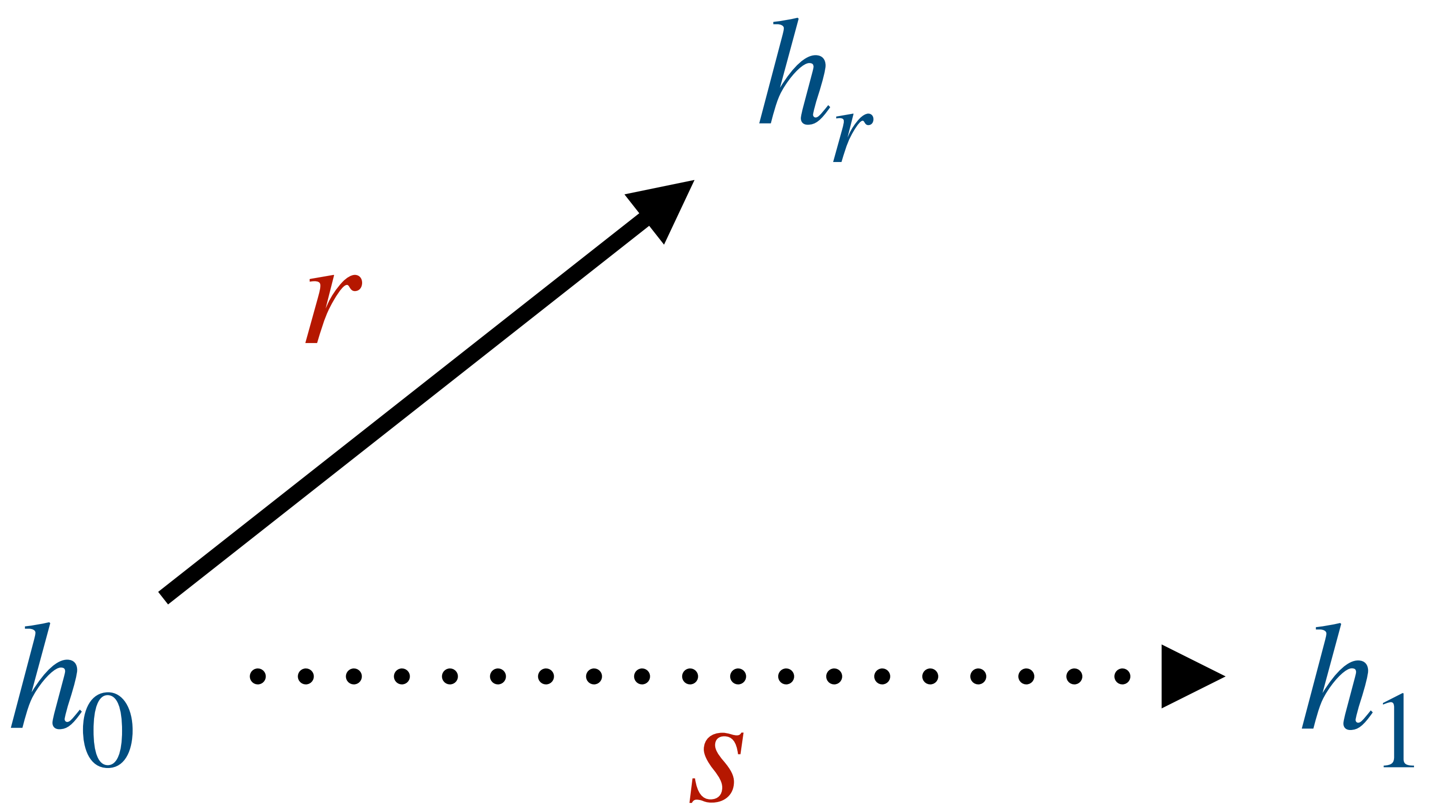
$b \in \{0,1\}$

← b

$c = rs^{-b}$

c →

$h_b^c \stackrel{?}{=} h_r$

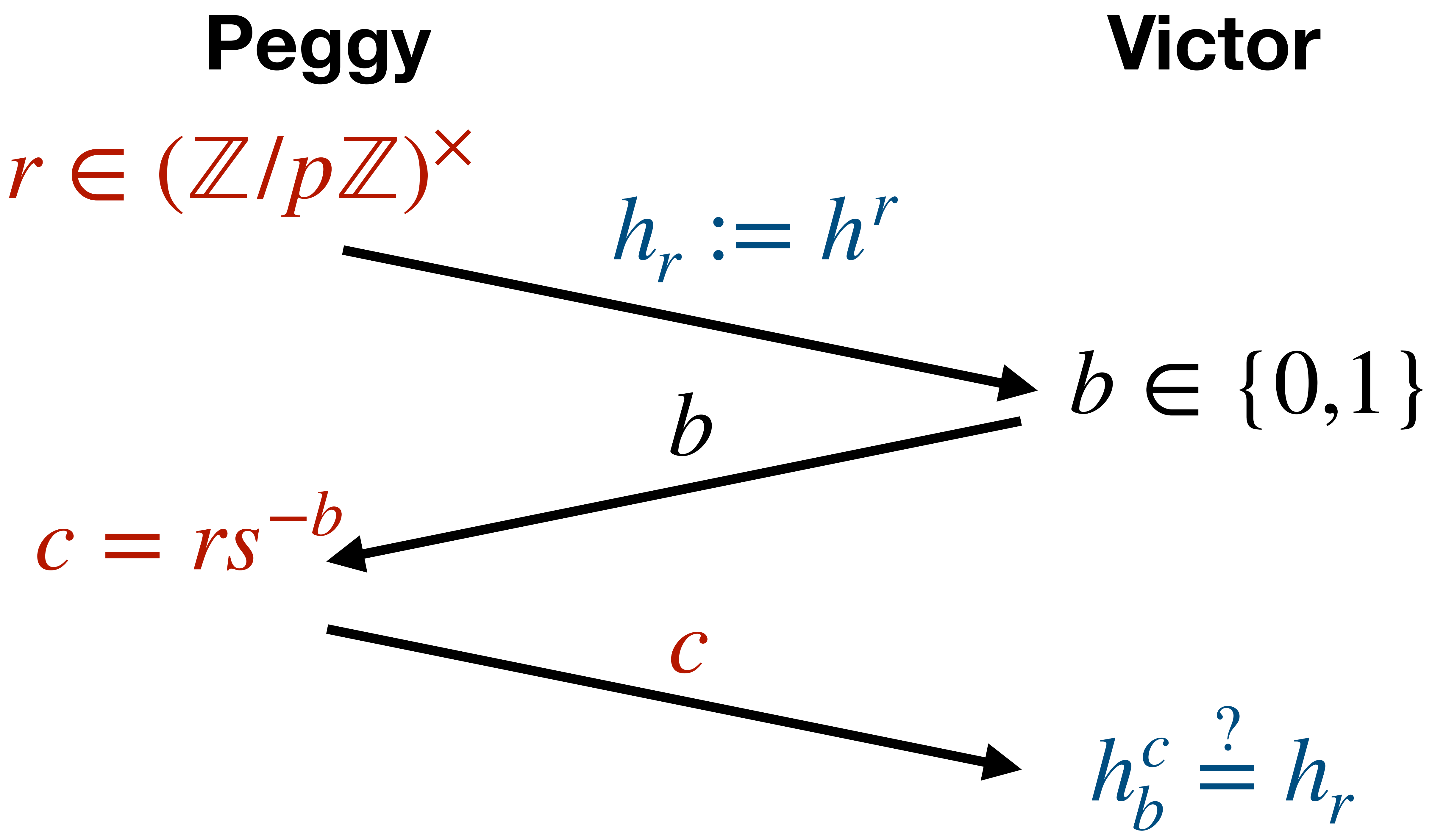


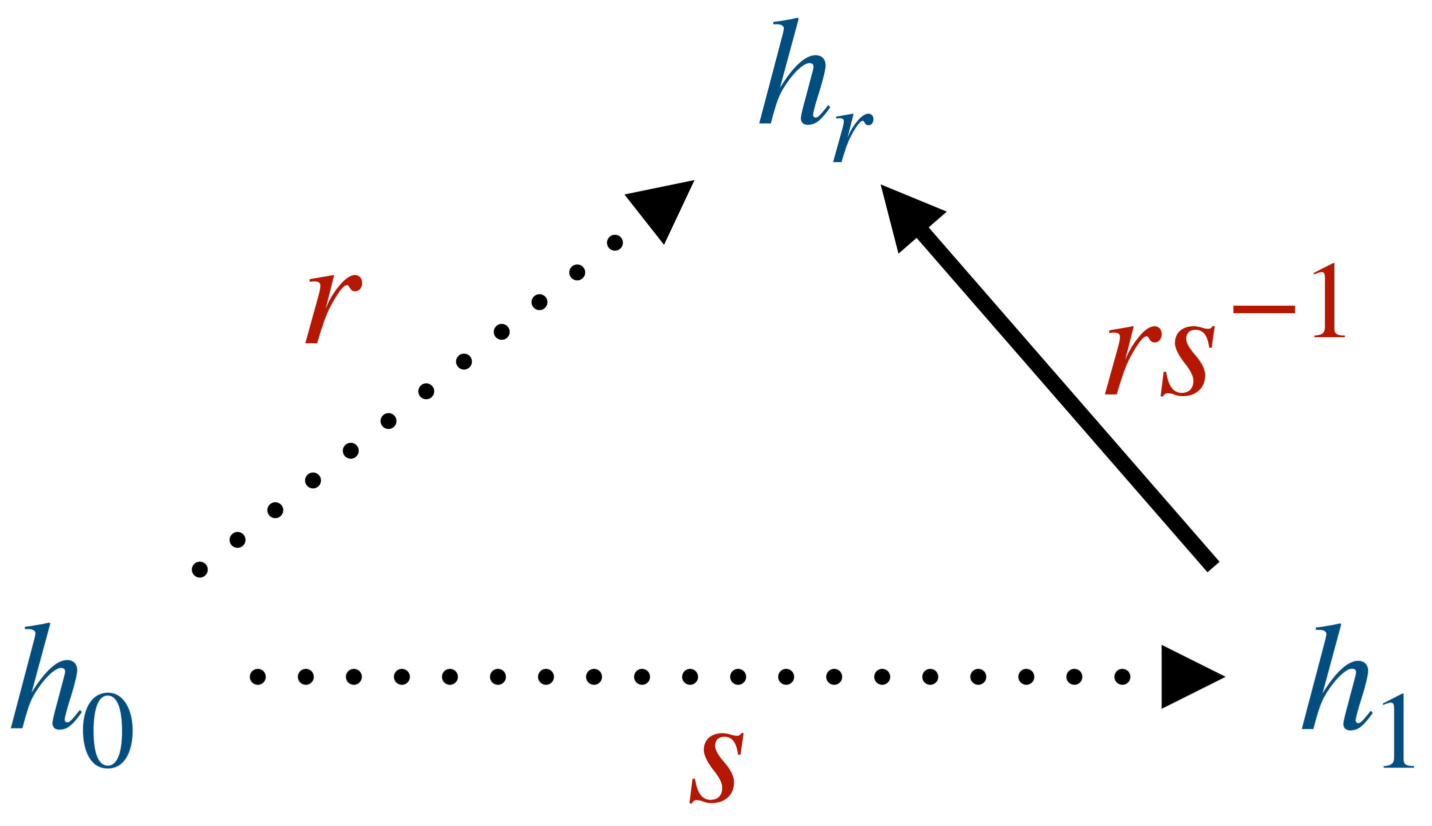
Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$





Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$

Peggy | **Victor**

$r \in (\mathbb{Z}/p\mathbb{Z})^\times$

→ $h_r := h^r$ →

$b \in \{0,1\}$

← b ←

$c = rs^{-b}$

→ c →

$h_b^c \stackrel{?}{=} h_r$

Setup: G acting on X, fixed $h_0 \in X$

Secret: $s \in G$

Public: $h_1 := s \star h_0$

Peggy | **Victor**

Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$

Peggy | **Victor**

$r \in (\mathbb{Z}/p\mathbb{Z})^\times$

$h_r := h^r$ →

$b \in \{0,1\}$

← b

$c = rs^{-b}$

c →

$h_b^c \stackrel{?}{=} h_r$

Setup: G acting on X, fixed $h_0 \in X$

Secret: $s \in G$

Public: $h_1 := s \star h_0$

Peggy | **Victor**

$r \in G$

$h_r := r \star h$ →

Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$
Public: $h_1 := h_0^s$

Peggy | **Victor**

$r \in (\mathbb{Z}/p\mathbb{Z})^\times$

$h_r := h^r$ →

$b \in \{0,1\}$

← b

$c = rs^{-b}$

c →

$h_b^c \stackrel{?}{=} h_r$

Setup: G acting on X, fixed $h_0 \in X$

Secret: $s \in G$
Public: $h_1 := s \star h_0$

Peggy | **Victor**

$r \in G$

$h_r := r \star h$ →

$b \in \{0,1\}$

← b

Protocols from DH: Binary Schnorr

Setup: $H = \langle h_0 \rangle$

Secret: $s \in (\mathbb{Z}/p\mathbb{Z})^\times$

Public: $h_1 := h_0^s$

Peggy — **Victor**

$r \in (\mathbb{Z}/p\mathbb{Z})^\times$

$h_r := h^r$ →

$b \in \{0,1\}$

← b

$c = rs^{-b}$

c →

$h_b^c \stackrel{?}{=} h_r$

Setup: G acting on X, fixed $h_0 \in X$

Secret: $s \in G$

Public: $h_1 := s \star h_0$

Peggy — **Victor**

$r \in G$

$h_r := r \star h$ →

$b \in \{0,1\}$

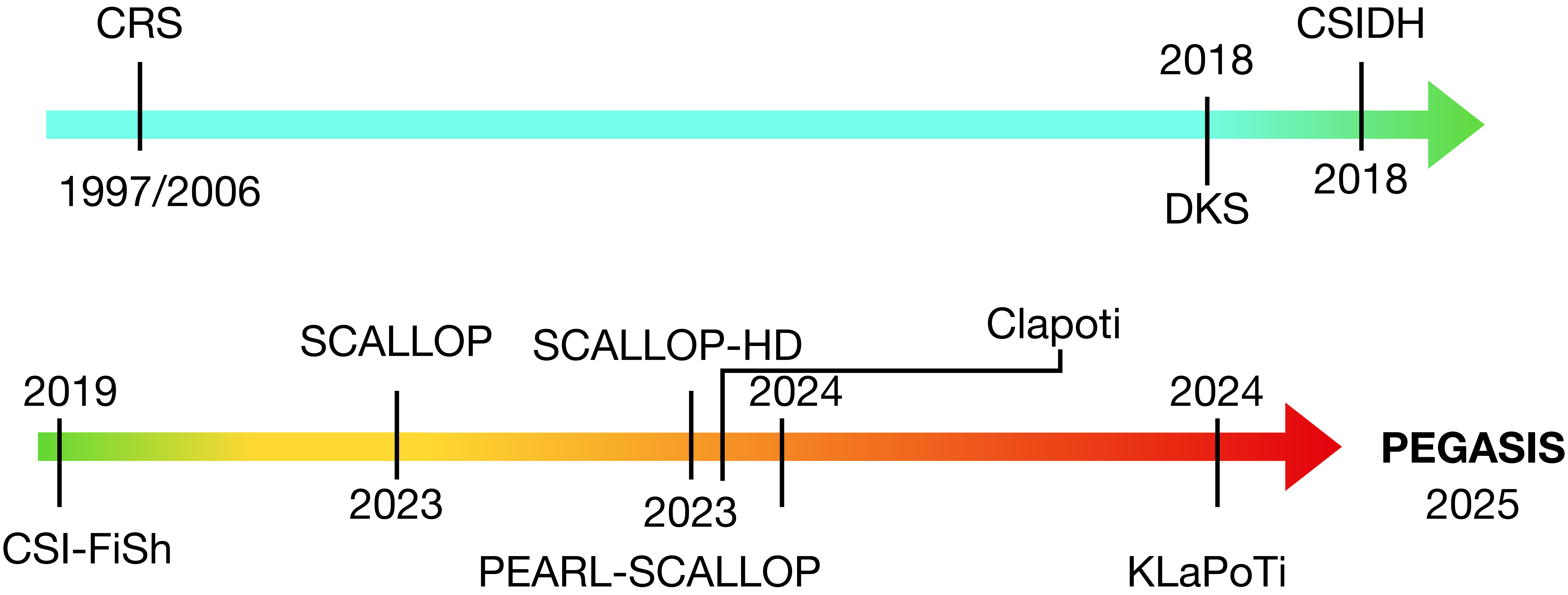
← b

$c = rs^{-b}$

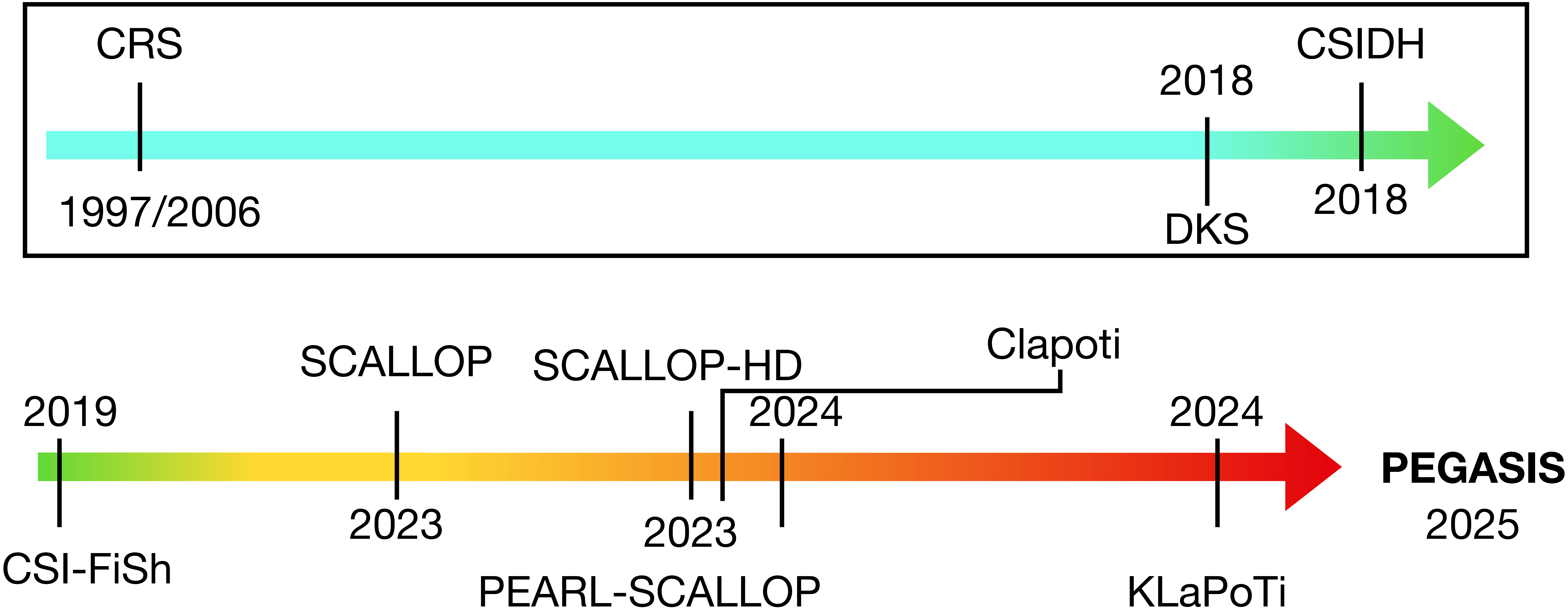
c →

$c \star h_b \stackrel{?}{=} h_r$

Group Action "Timeline"



Group Action "Timeline"



CRS/DKS/CSIDH, a restricted group action

The group:

$$G = cl(\mathbb{Z}[\pi]), \pi^2 = -p$$

The set:

$X = Ell$, a certain set of elliptic curves

The action:

$$G \times X \to X$$
$$[\mathfrak{b}] \star E = \phi_{\mathfrak{b}}(E)$$

CRS/DKS/CSIDH, a restricted group action

The group:

$G = cl(\mathbb{Z}[\pi]), \pi^2 = -p$

The set:

$X = Ell$, a certain set of elliptic curves

The action:

$$G \times X \to X$$
$$[\mathfrak{b}] \star E = \phi_{\mathfrak{b}}(E)$$

The Class Group

(Assume $\mathbb{Z}[\pi] = \mathfrak{O}_K$ is integrally closed)

For any ideal $\mathfrak{a} \subset \mathfrak{O}_K$, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

In a unique way (up to ordering)

The Class Group

(Assume $\mathbb{Z}[\pi] = \mathfrak{O}_K$ is integrally closed)

For any ideal $\mathfrak{a} \subset \mathfrak{O}_K$, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

In a unique way (up to ordering)

Adding **fractional ideals** makes $I(\mathfrak{O}_K)$ into a group.

The Class Group

(Assume $\mathbb{Z}[\pi] = \mathfrak{O}_K$ is integrally closed)

For any ideal $\mathfrak{a} \subset \mathfrak{O}_K$, we can write

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_r^{e_r}$$

In a unique way (up to ordering)

Adding **fractional ideals** makes $I(\mathfrak{O}_K)$ into a group.

The **class group** is defined as

$$cl(\mathfrak{O}_K) := I(\mathfrak{O}_K)/P(\mathfrak{O}_K)$$

Where $P(\mathfrak{O}_K) < I(\mathfrak{O}_K)$ is the subgroup of principal ideals

Example

Let $\pi^2 = -53$

$cl(\mathbb{Z}[\pi])$ can be given the representatives

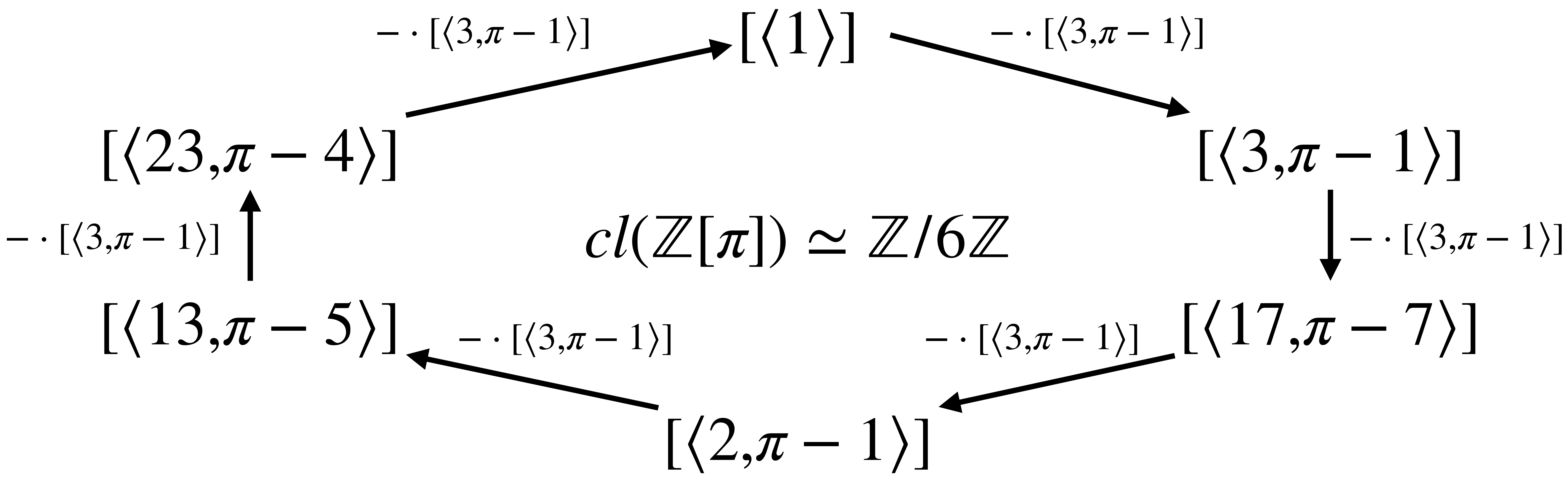
$$[\langle 1 \rangle], [\langle 2, \pi - 1 \rangle], [\langle 3, \pi - 1 \rangle], [\langle 13, \pi - 5 \rangle], [\langle 17, \pi - 7 \rangle], [\langle 23, \pi - 4 \rangle]$$

Example

Let $\pi^2 = -53$

$cl(\mathbb{Z}[\pi])$ can be given the representatives

$$[\langle 1\rangle], [\langle 2,\pi-1\rangle], [\langle 3,\pi-1\rangle], [\langle 13,\pi-5\rangle], [\langle 17,\pi-7\rangle], [\langle 23,\pi-4\rangle]$$



CRS/DKS/CSIDH, a restricted group action

The group:

$G = cl(\mathbb{Z}[\pi]), \pi^2 = -p$

The set:

$X = Ell$, a certain set of elliptic curves

The action:

$$G \times X \to X$$
$$[\mathfrak{b}] \star E = \phi_{\mathfrak{b}}(E)$$

CRS/DKS/CSIDH, a restricted group action

The group:

$G = cl(\mathbb{Z}[\pi]), \pi^2 = -p$

The set:

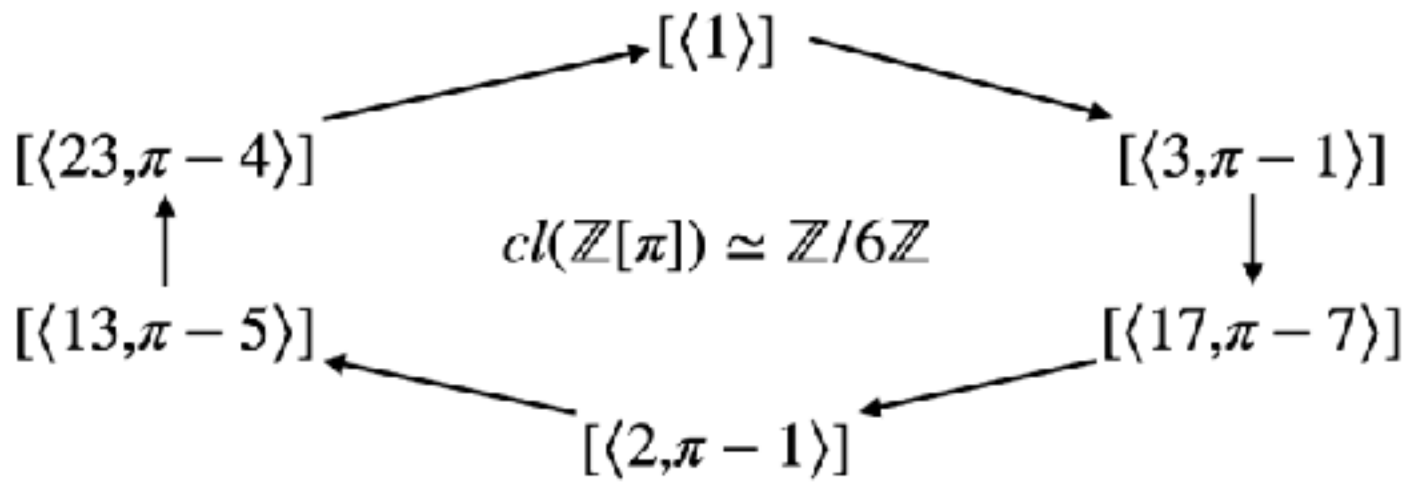
$X = Ell$, a certain set of elliptic curves

The action:

$G \times X \to X$

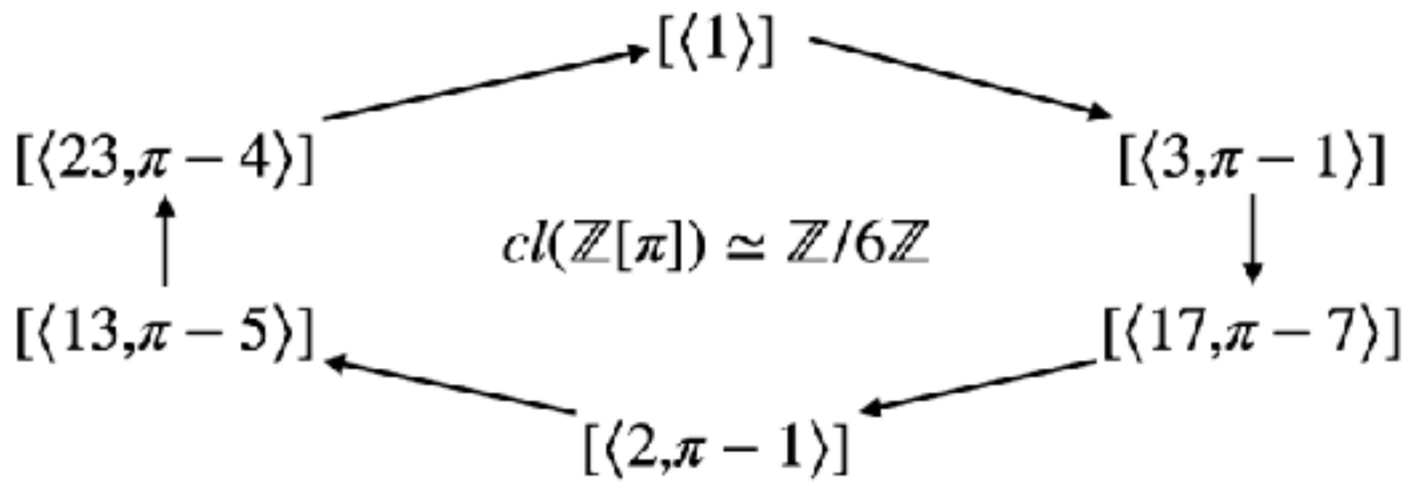
$[\mathfrak{b}] \star E = \phi_{\mathfrak{b}}(E)$

Class Group Action



$$y^2 = x^3 + 1$$

Class Group Action

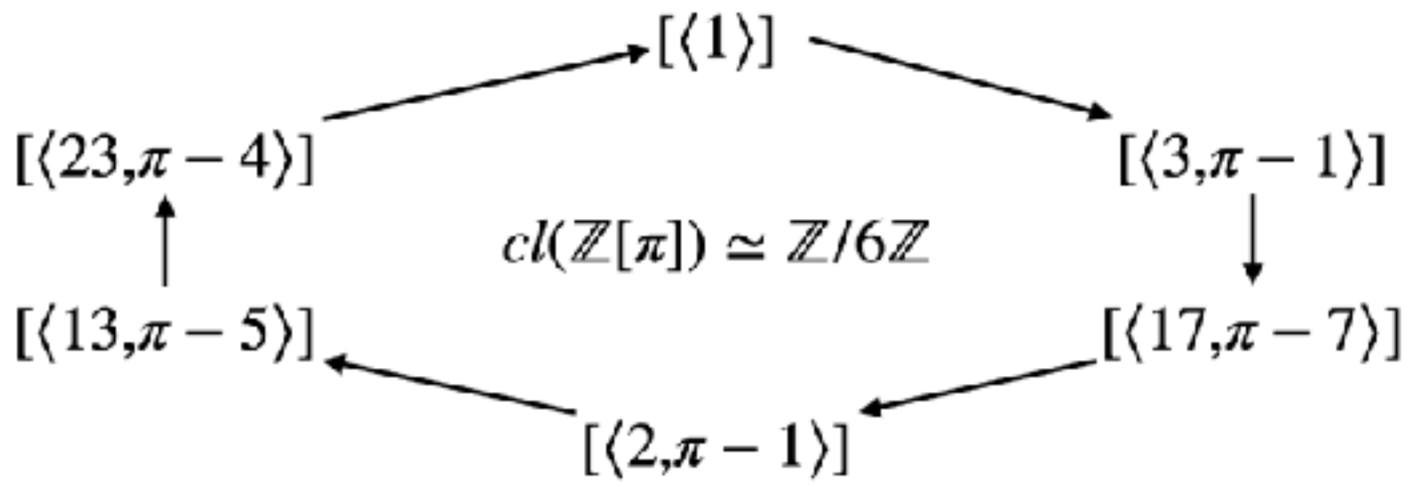


$\langle 2, \pi - 1 \rangle \star -$

$$y^2 = x^3 + 1$$

$$y^2 = x^3 + 38x + 22$$

Class Group Action



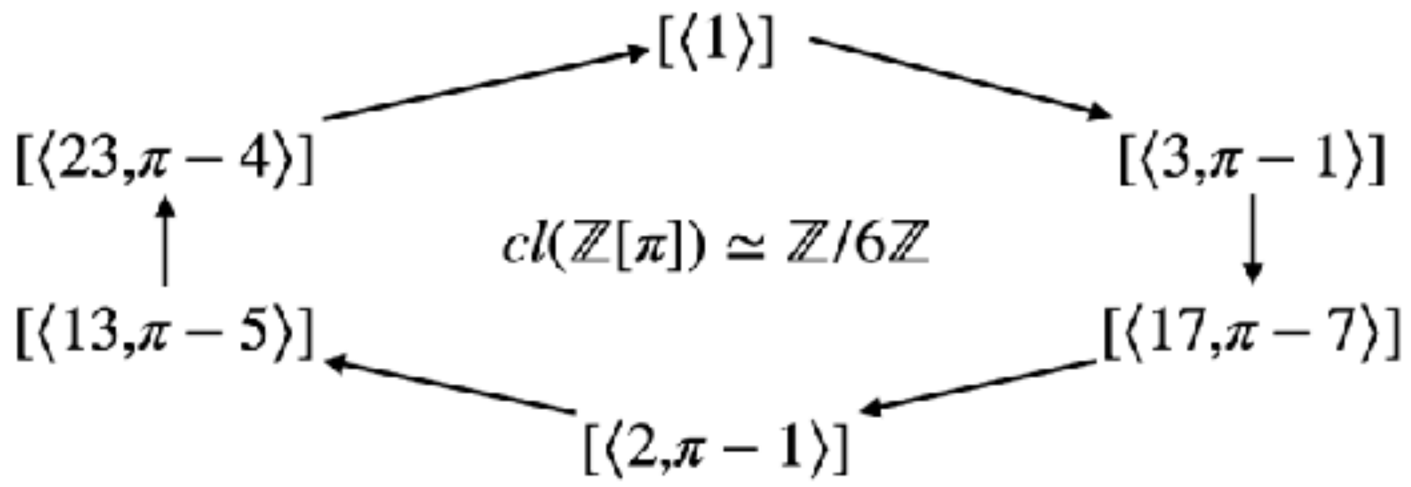
$\langle 2, \pi - 1 \rangle \star -$

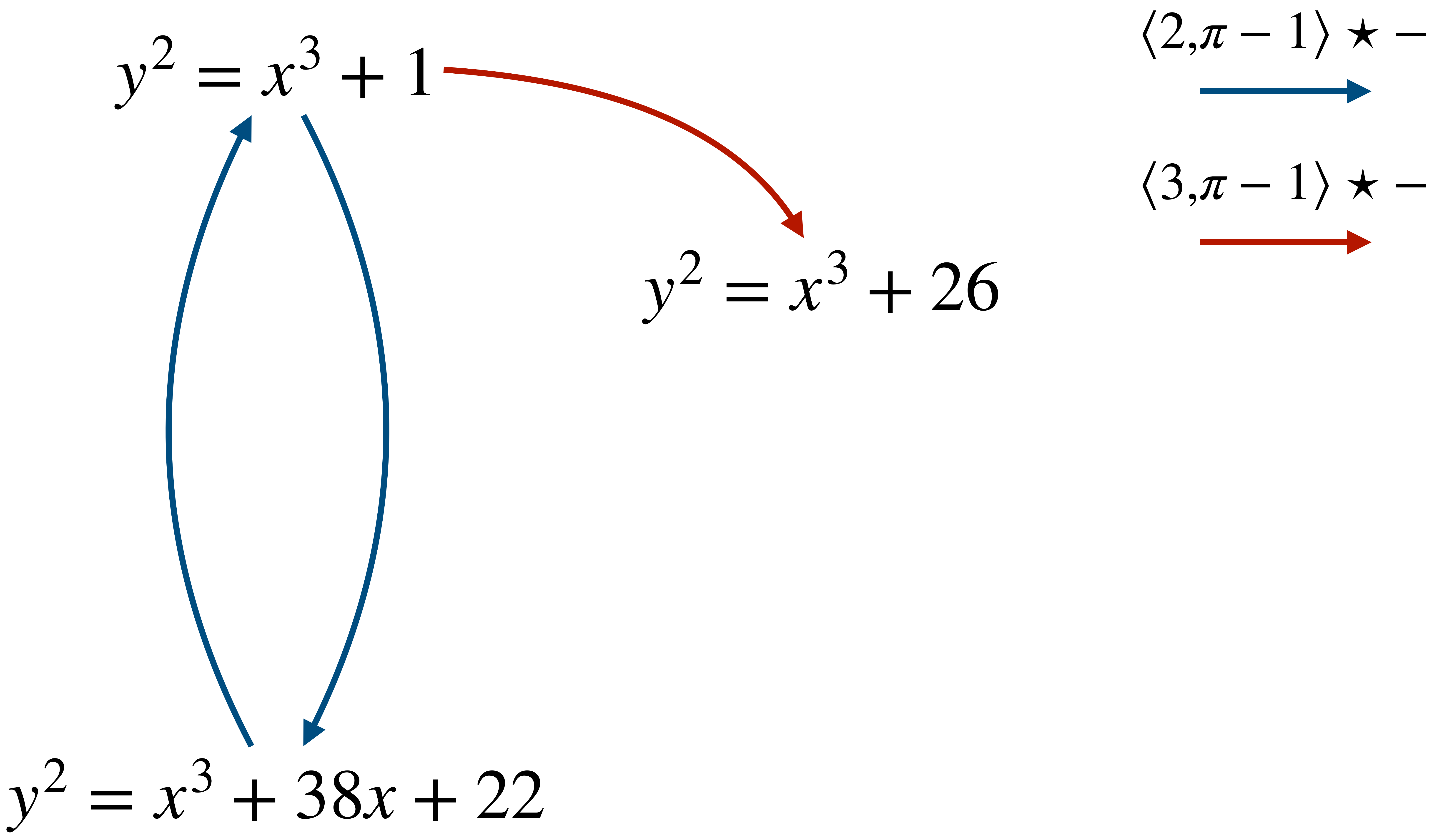
$\langle 3, \pi - 1 \rangle \star -$

$$y^2 = x^3 + 1$$

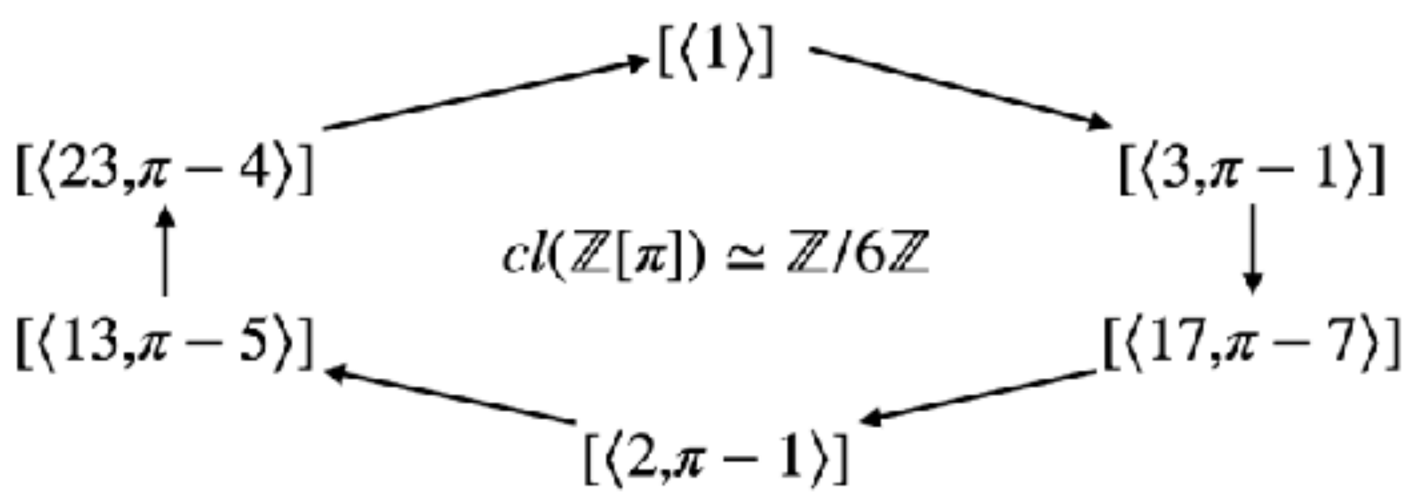
$$y^2 = x^3 + 38x + 22$$

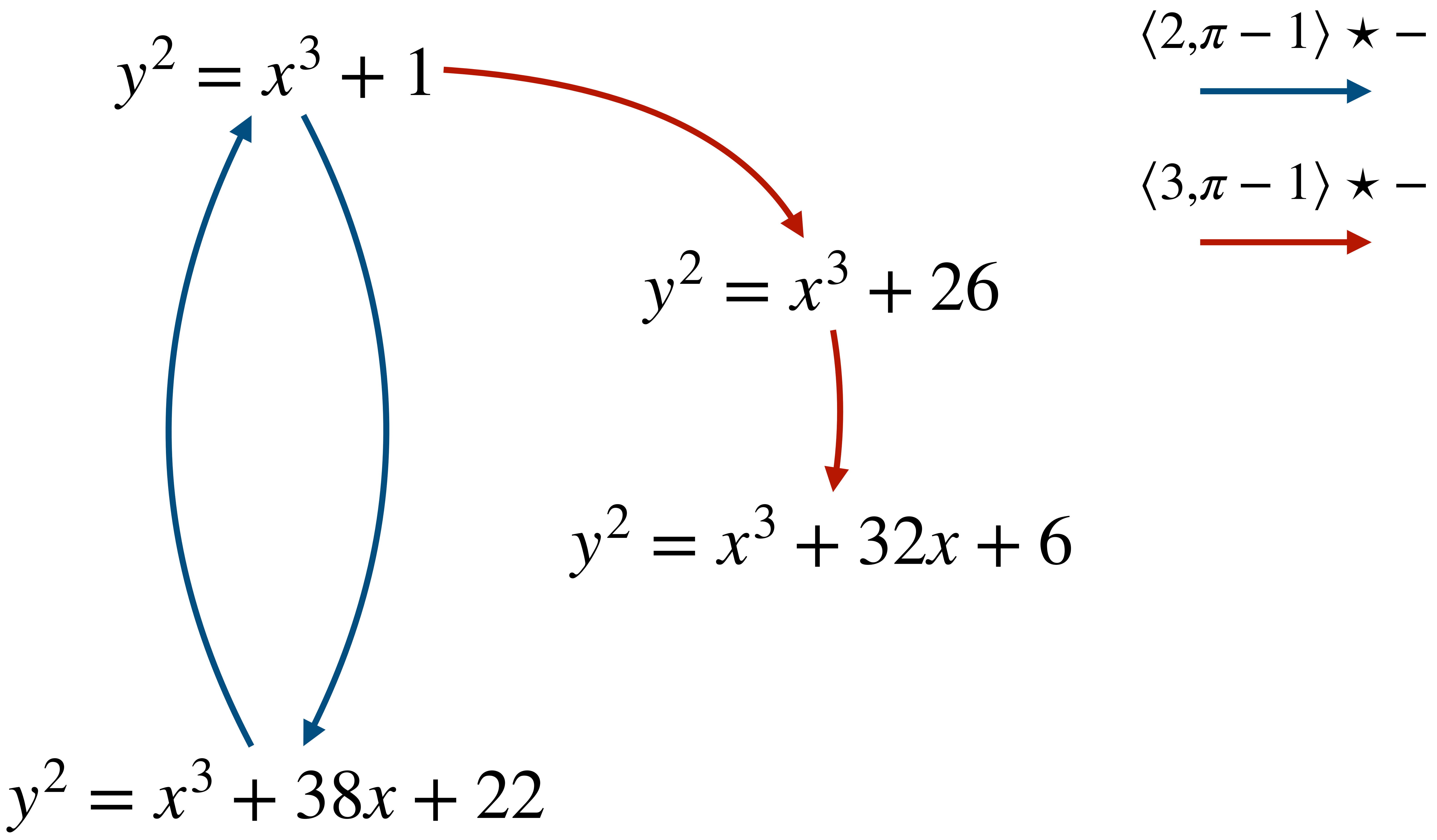
Class Group Action



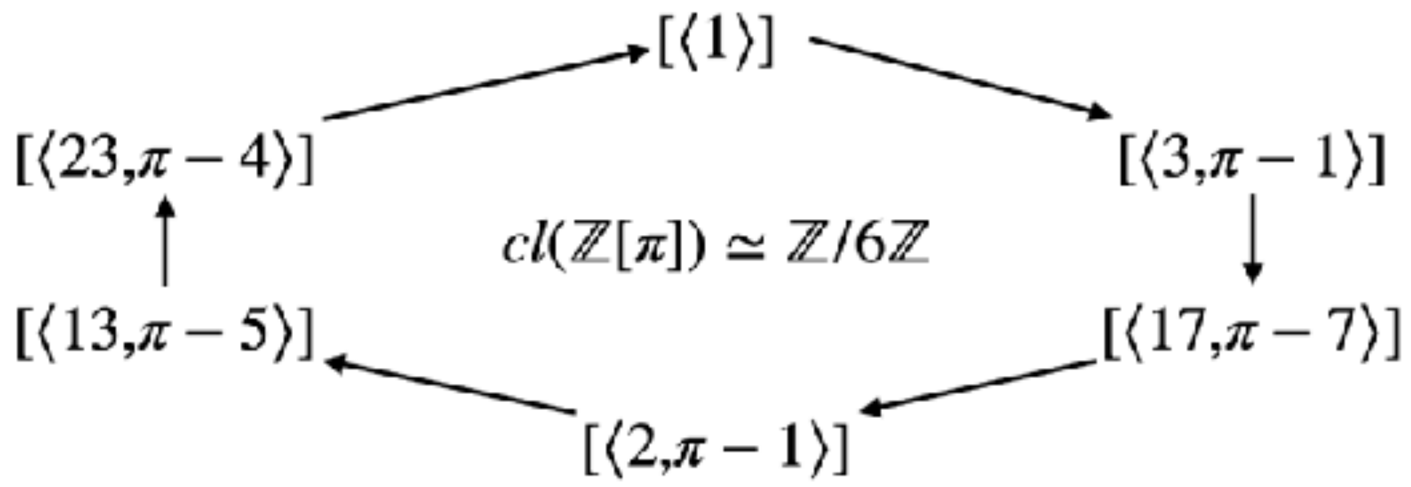


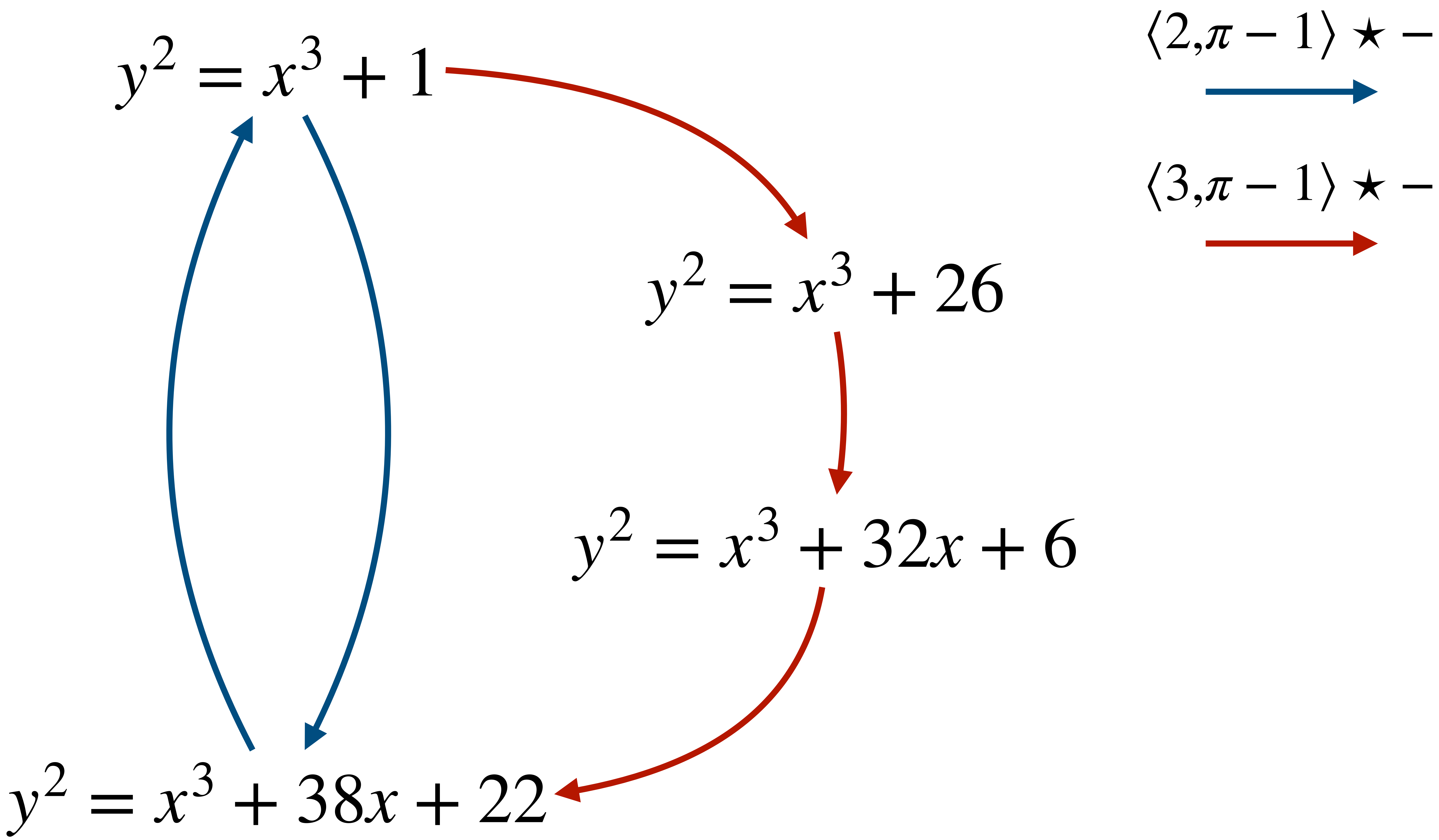
Class Group Action



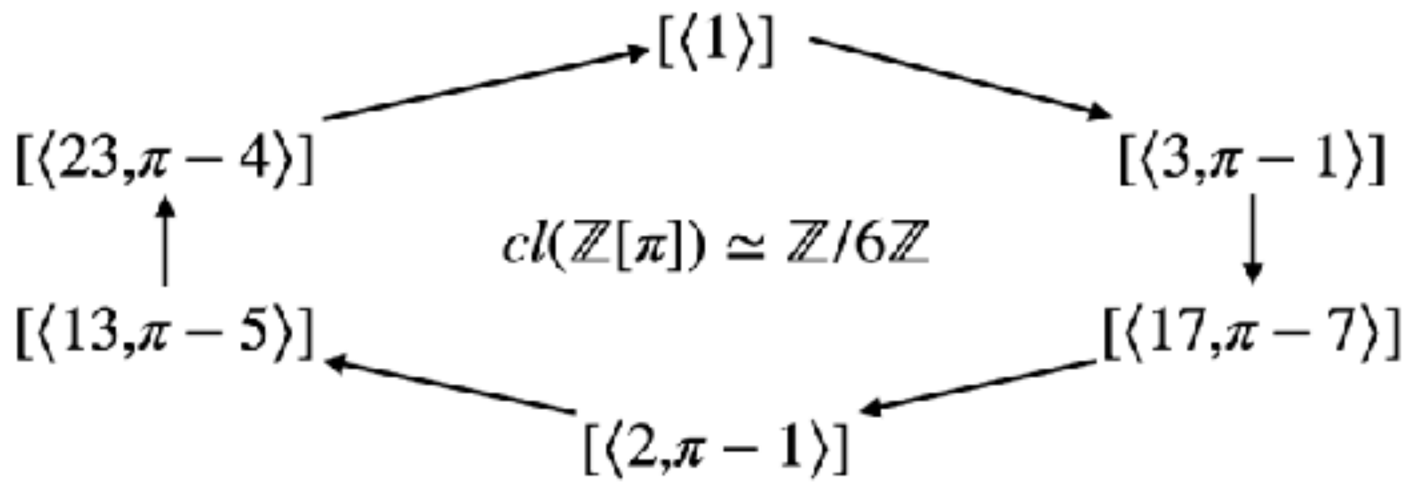


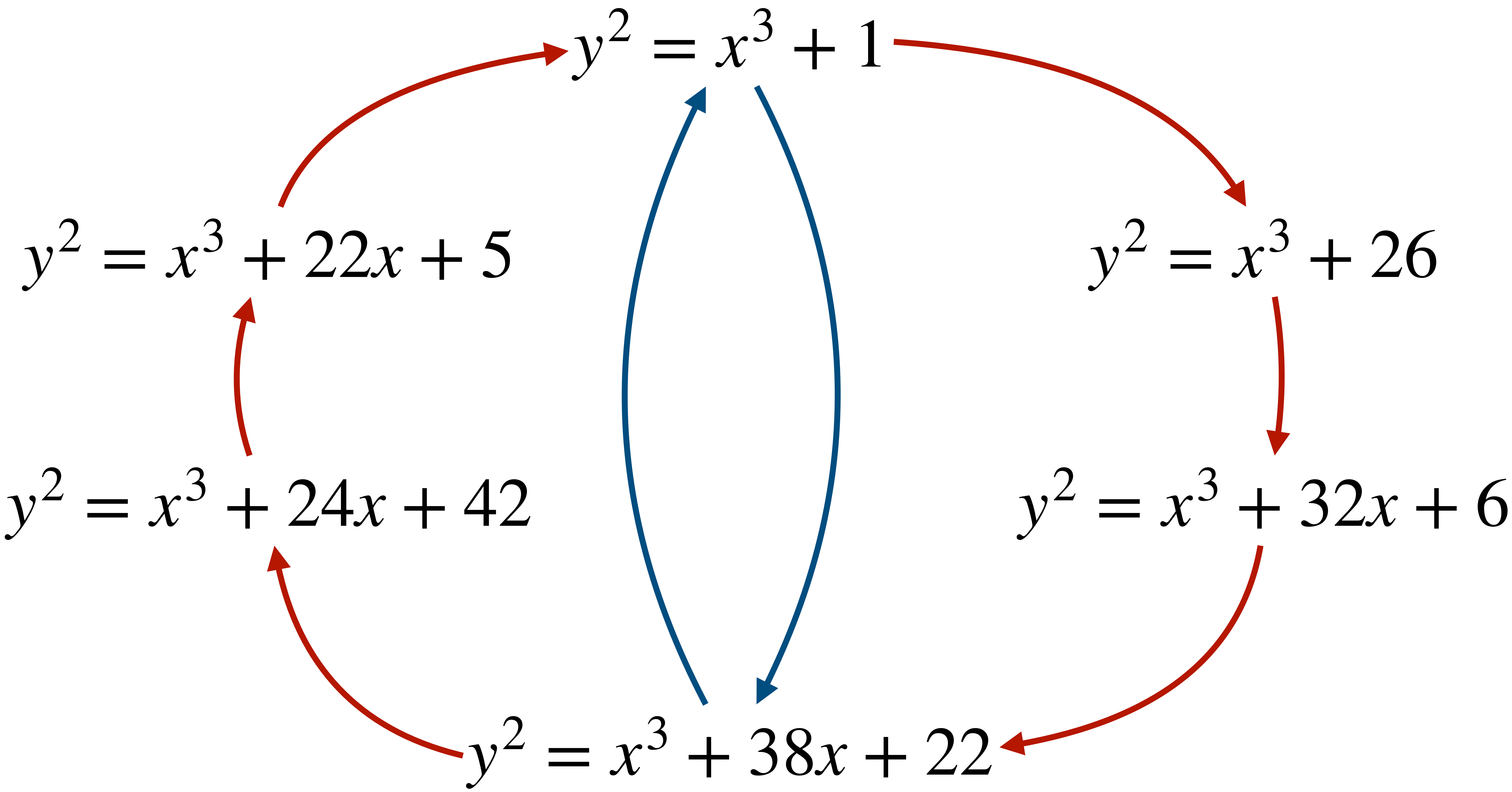
Class Group Action





Class Group Action





$\langle 2, \pi - 1 \rangle \star -$

$\langle 3, \pi - 1 \rangle \star -$

CRS/DKS/CSIDH, a restricted group action

The action:

$$G \times X \to X$$
$$[\mathfrak{b}] \star E = \phi_{\mathfrak{b}}(E)$$

Can only compute **smooth degree** isogenies ⟷ Can only compute the action of **smooth normed** ideals

CRS/DKS/CSIDH, a restricted group action

The action:

$$G \times X \to X$$
$$[\mathfrak{b}] \star E = \phi_{\mathfrak{b}}(E)$$

Can only compute **smooth degree** isogenies ⟷ Can only compute the action of **smooth normed** ideals

Fix generators $G = \langle g_1, g_2, \ldots, g_r \rangle$, a vector $e = [e_1, \ldots, e_r] \in \mathbb{Z}^r$ represents the element $g = g_1^{e_1} g_2^{e_2} \ldots g_r^{e_r}$.

CRS/DKS/CSIDH, a restricted group action

The action:

$$G \times X \to X$$
$$[\mathfrak{b}] \star E = \phi_{\mathfrak{b}}(E)$$

Can only compute **smooth degree** isogenies ⟷ Can only compute the action of **smooth normed** ideals

Fix generators $G = \langle g_1, g_2, \ldots, g_r \rangle$, a vector $e = [e_1, \ldots, e_r] \in \mathbb{Z}^r$ represents the element $g = g_1^{e_1} g_2^{e_2} \ldots g_r^{e_r}$.

Can evaluate the action of $e \in \mathbb{Z}^r$ whenever $||e||$ is small

Binary Schnorr with CSIDH

Setup: $cl(\mathbb{Z}[\pi])$ acting on X, fixed $E_0 \in X$

Secret: $s = [s_1, \ldots s_2] \in \mathbb{Z}^r$

Public: $E_1 := s \star E_0$

$e = [e_1, \ldots, e_r] \in \mathbb{Z}^r, e_i \in \{-1,0,1\}$

$E_r := e \star E_0$

$b \in \{0,1\}$

b

$c = e - b \cdot s$

c

$c \star E_b \stackrel{?}{=} E_r$

Binary Schnorr with CSIDH

Example: Secret: $s = [1, -1, 0]$

Round 1

$e = [1, 1, -1]$

$E_r := e \star E_0$ →

Binary Schnorr with CSIDH

Example: Secret: $s = [1, -1, 0]$

Round 1

$e = [1, 1, -1]$

$E_r := e \star E_0$

$b = 1$

b

$c = e - b \cdot s$
$= [0, 2, -1]$

Binary Schnorr with CSIDH

Attacker saw:

$c = [0,2,-1]$

Example: Secret: $s = [1,-1,0]$

Round 1

$e = [1,1,-1]$

$E_r := e \star E_0$ →

$b = 1$

← b

$c = e - b \cdot s$
$= [0,2,-1]$

c →

$c \star E_b \stackrel{?}{=} E_r$

Binary Schnorr with CSIDH

Attacker saw:
$c = [0,2,-1]$

Example: Secret: $s = [1,-1,0]$

Round 1

$e = [1,1,-1]$

$E_r := e \star E_0$

$b = 1$

b

$c = e - b \cdot s$
$= [0,2,-1]$

c

$c \star E_b \stackrel{?}{=} E_r$

Round 2

$e = [-1,-1,1]$

$E_r := e \star E_0$

Binary Schnorr with CSIDH

Attacker saw:

$c = [0,2,-1]$

Example: Secret: $s = [1,-1,0]$

Round 1

$e = [1,1,-1]$

$E_r := e \star E_0$

$b = 1$

b

$c = e - b \cdot s$
$= [0,2,-1]$

c

$c \star E_b \stackrel{?}{=} E_r$

Round 2

$e = [-1,-1,1]$

$E_r := e \star E_0$

$b = 1$

b

$c = e - b \cdot s$
$= [-2,0,1]$

Binary Schnorr with CSIDH

Attacker saw:

$c = [0, 2, -1]$

$c = [-2, 0, 1]$

Oops...

Example: Secret: $s = [1, -1, 0]$

Round 1

$e = [1, 1, -1]$

$E_r := e \star E_0$

$b = 1$

b

$c = e - b \cdot s = [0, 2, -1]$

c

$c \star E_b \stackrel{?}{=} E_r$

Round 2

$e = [-1, -1, 1]$

$E_r := e \star E_0$

$b = 1$

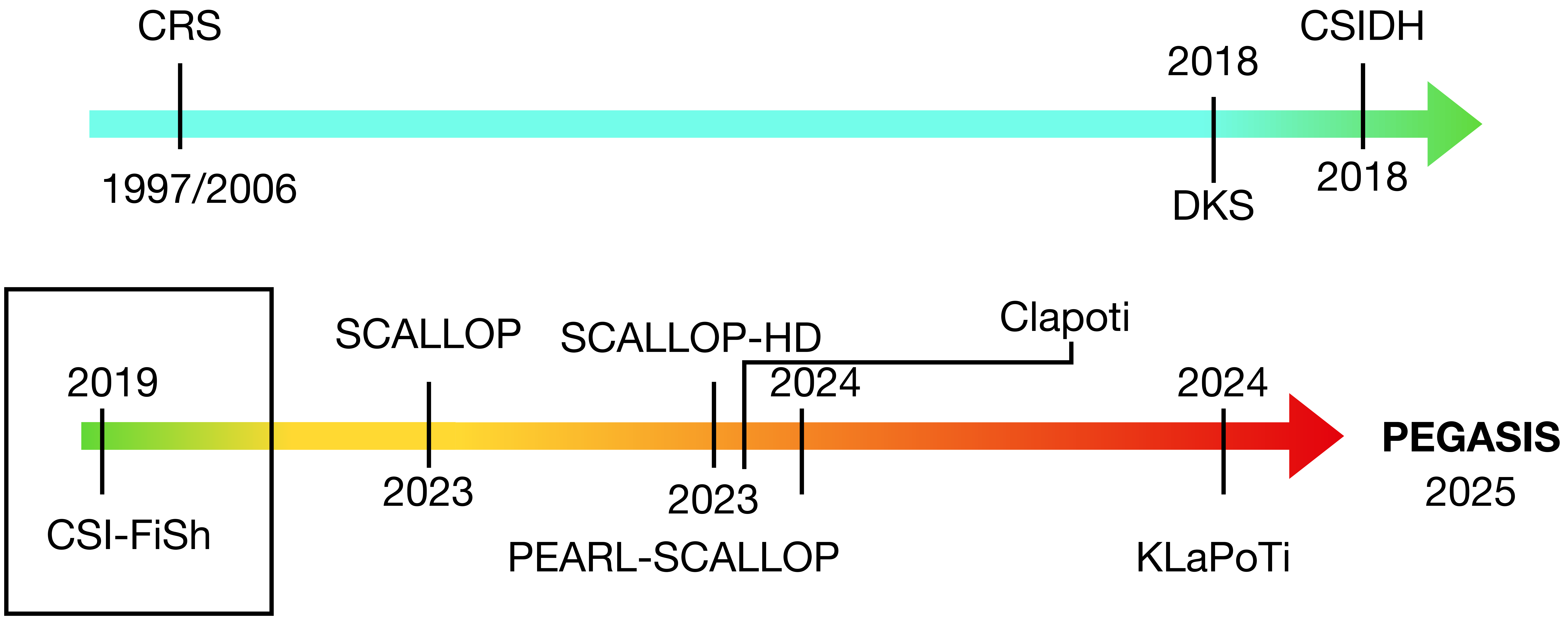
b

$c = e - b \cdot s = [-2, 0, 1]$

c

$c \star E_b \stackrel{?}{=} E_r$

Group Action "Timeline"



CSi-FiSh: REGA -> EGA

$$G = \langle g_1, g_2, \ldots, g_r \rangle$$

$$\mathbb{Z}^r \longrightarrow G \longrightarrow 0$$

$$[1,0,\ldots,0] \longrightarrow g_1$$

$$[0,1,\ldots,0] \longrightarrow g_2$$

Assume $G = \langle g_1 \rangle$, order N

Goal: Evaluate a "uniformly random" element of the form $[d,0,\ldots,0]$

CSi-FiSh: REGA -> EGA

$$G = \langle g_1, g_2, \ldots, g_r \rangle$$

$$0 \longrightarrow \mathbb{Z}^r \longrightarrow \mathbb{Z}^r \longrightarrow G \longrightarrow 0$$

$$[1,0,\ldots,0] \longrightarrow g_1$$

$$[0,1,\ldots,0] \longrightarrow g_2$$

etc...

Assume $G = \langle g_1 \rangle$, order N

For each g_i, compute s_i, so that $g_i = g_1^{s_i}$

CSi-FiSh: REGA -> EGA

$G = \langle g_1, g_2, \ldots, g_r \rangle$

$$0 \longrightarrow \mathbb{Z}^r \longrightarrow \mathbb{Z}^r \longrightarrow G \longrightarrow 0$$

$$[1,0,\ldots,0] \longrightarrow g_1$$
$$[0,1,\ldots,0] \longrightarrow g_2$$

etc...

$$[1,0,\ldots,0] \longrightarrow [N,0,\ldots,0]$$
$$[0,1,\ldots,0] \longrightarrow [s_2, -1,\ldots,0]$$

etc...

Assume $G = \langle g_1 \rangle$, order N

For each g_i, compute s_i, so that $g_i = g_1^{s_i}$

CSi-FiSh: REGA -> EGA

$G = \langle g_1, g_2, \ldots, g_r \rangle$

$$0 \longrightarrow \mathbb{Z}^r \longrightarrow \mathbb{Z}^r \longrightarrow G \longrightarrow 0$$

$$[1,0,\ldots,0] \longrightarrow g_1$$
$$[0,1,\ldots,0] \longrightarrow g_2$$

etc...

$G \simeq \mathbb{Z}^r / L,$

$$[1,0,\ldots,0] \longrightarrow [N,0,\ldots,0]$$
$$[0,1,\ldots,0] \longrightarrow [s_2, -1,\ldots,0]$$

etc...

$$L = \begin{pmatrix} N & 0 & 0 & \ldots & 0 \\ s_2 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_r & 0 & 0 & \ldots & -1 \end{pmatrix}$$

Assume $G = \langle g_1 \rangle$, order N

For each g_i, compute s_i, so that $g_i = g_1^{s_i}$

CSi-FiSh: REGA -> EGA

Goal: Evaluate a "uniformly random" element of the form $e = [d, 0, \ldots, 0]$

Step 1: Compute a bunch of DLOGs in G

$$G \simeq \mathbb{Z}^r / L,$$

$$L = \begin{pmatrix} N & 0 & 0 & \ldots & 0 \\ s_2 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_r & 0 & 0 & \ldots & -1 \end{pmatrix}$$

CSi-FiSh: REGA -> EGA

Goal: Evaluate a "uniformly random" element of the form $e = [d,0,\ldots,0]$

Step 1: Compute a bunch of DLOGs in G

Step 2: Compute reduced basis of L

One time computations!

$$G \simeq \mathbb{Z}^r / L,$$

$$L = \begin{pmatrix} N & 0 & 0 & \ldots & 0 \\ s_2 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_r & 0 & 0 & \ldots & -1 \end{pmatrix}$$

CSi-FiSh: REGA -> EGA

Goal: Evaluate a "uniformly random" element of the form $e = [d, 0, \ldots, 0]$

Step 1: Compute a bunch of DLOGs in G

One time computations!

Step 2: Compute reduced basis of L

$G \simeq \mathbb{Z}^r / L,$

Step 3: Compute $f \in L$ closest to e

$$L = \begin{pmatrix} N & 0 & 0 & \ldots & 0 \\ s_2 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_r & 0 & 0 & \ldots & -1 \end{pmatrix}$$

CSi-FiSh: REGA -> EGA

Goal: Evaluate a "uniformly random" element of the form $e = [d, 0, \ldots, 0]$

Step 1: Compute a bunch of DLOGs in G

One time computations!

Step 2: Compute reduced basis of L

$$G \simeq \mathbb{Z}^r / L,$$

Step 3: Compute $f \in L$ closest to e

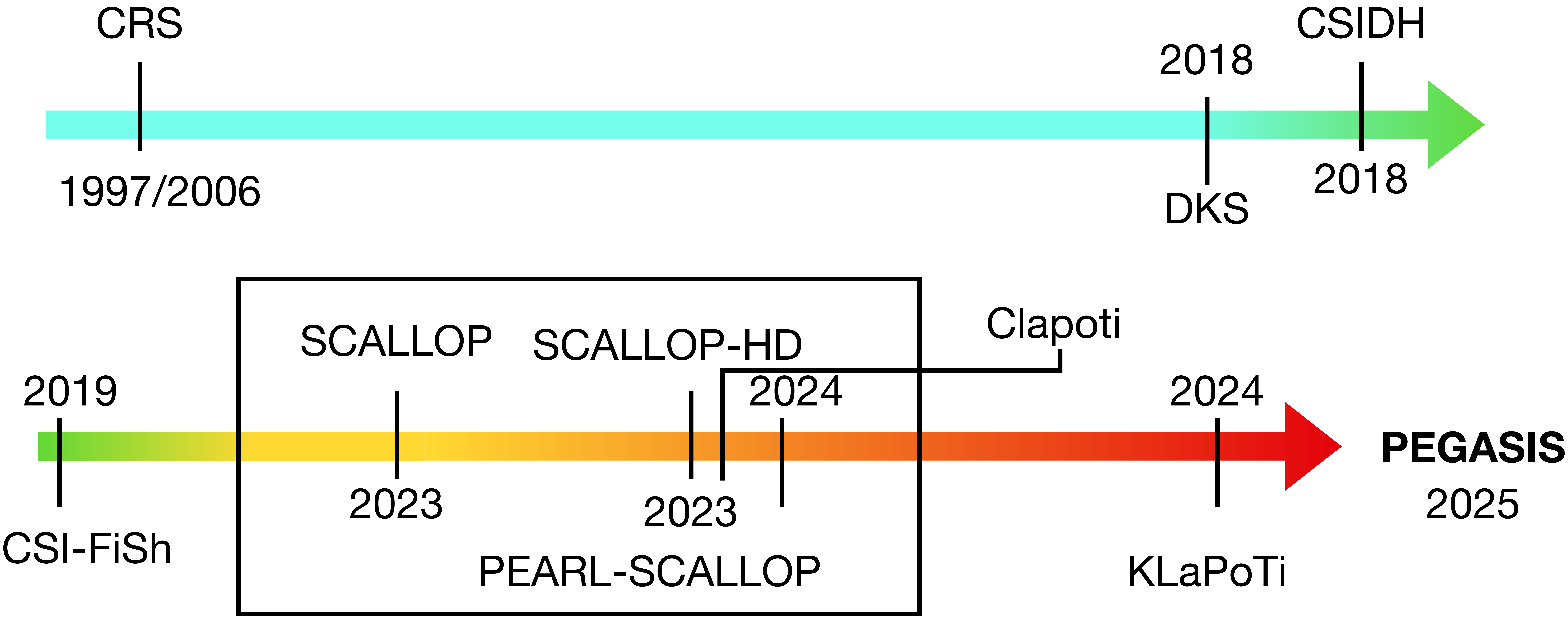
$$L = \begin{pmatrix} N & 0 & 0 & \ldots & 0 \\ s_2 & -1 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ s_r & 0 & 0 & \ldots & -1 \end{pmatrix}$$

Step 4: Evaluate the element $e - f$

Result: CSIDH-512 can be made unrestricted!

Debated quantum security :(

Group Action "Timeline"



SCALLOP++

Step 1: Compute a bunch of DLOGs in G ✅

$$G = \langle g_1, g_2, \ldots, g_r \rangle$$

Step 2: Compute reduced basis of L

Step 3: Compute $f \in L$ closest to e

Step 4: Evaluate the element $e - f$

SCALLOP++

$$G = \langle g_1, g_2, \ldots, g_r \rangle$$

Step 1: Compute a bunch of DLOGs in G

Step 2: Compute reduced basis of L

Step 3: Compute $f \in L$ closest to e

Step 4: Evaluate the element $e - f$

Security level	SCALLOP	SCALLOP-HD	PEARL-SCALLOP
CSIDH-512	35 sec	1 min, 28 sec	30 sec
CSIDH-1024	12 min, 30 sec	19 min	58 sec
CSIDH-1536	-	-	11 min, 50 sec

SCALLOP++

Step 1: Compute a bunch of DLOGs in G ✓

Step 2: Compute reduced basis of L

Step 3: Compute $f \in L$ closest to e

Step 4: Evaluate the element $e - f$

✗

$$G = \langle g_1, g_2, \ldots, g_r \rangle$$

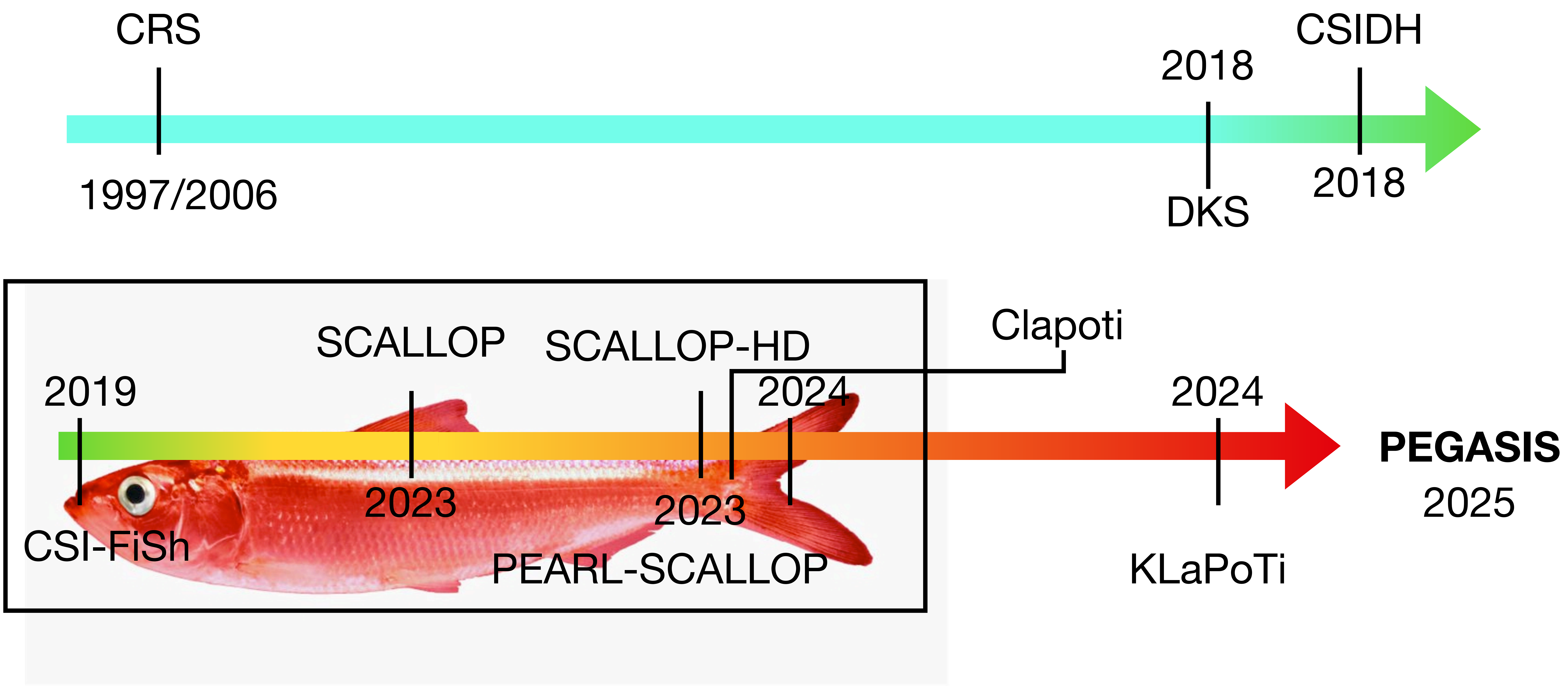
CSIDH-2000+:

r too large
- Step 2 infeasible

r too small
- Step 4 infeasible

Security level	SCALLOP	SCALLOP-HD	PEARL-SCALLOP
CSIDH-512	35 sec	1 min, 28 sec	30 sec
CSIDH-1024	12 min, 30 sec	19 min	58 sec
CSIDH-1536	-	-	11 min, 50 sec

Group Action "Timeline"

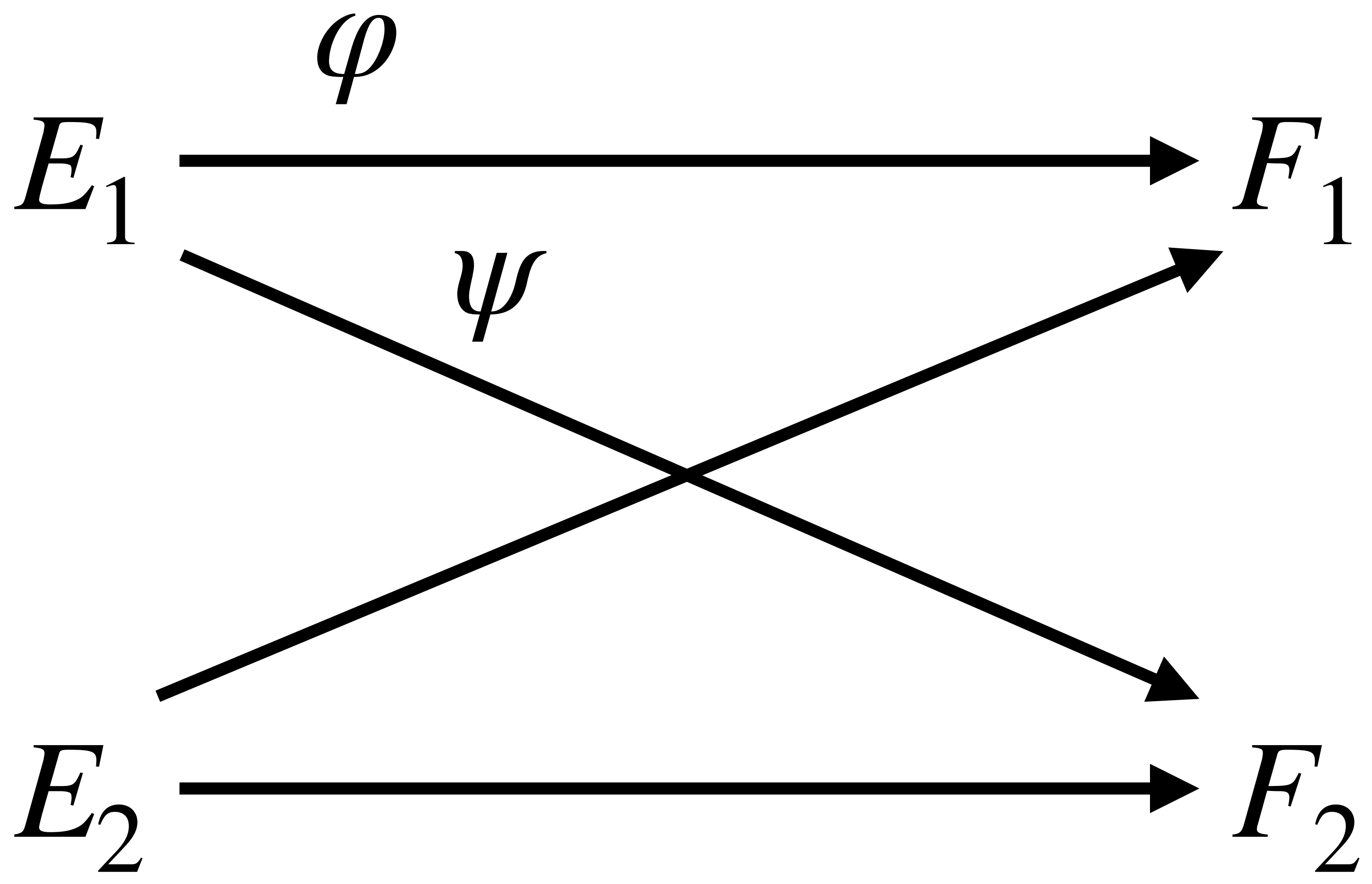


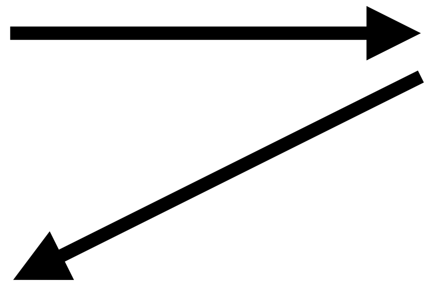
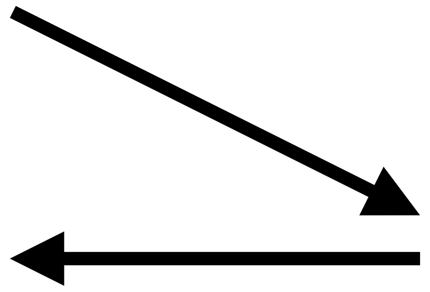
Interlude: Abelian Varieties in Isogeny-Based Cryptography

$$\Phi : E_1 \times E_2 \to F_1 \times F_2$$

Interlude: Abelian Varieties in Isogeny-Based Cryptography

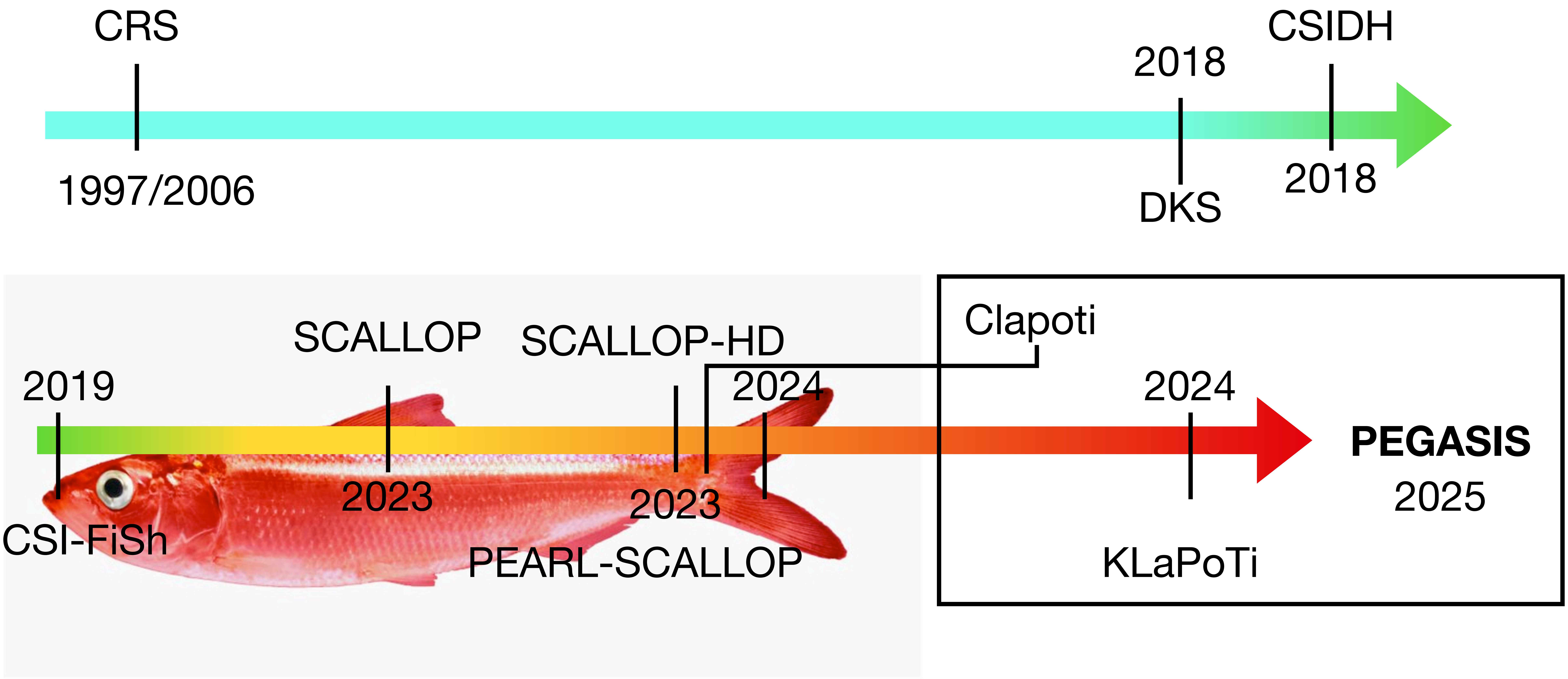
Φ :



If  $=$  , then $\deg \Phi = \deg \varphi + \deg \psi$

Overly simplified: Can evaluate arbitrary degree φ,
by embedding it in higher dimensional isogenies.

Group Action "Timeline"



Clapoti

Goal: Evaluate action of $[\mathfrak{a}]$

Assume we have: $\mathfrak{b}, \mathfrak{c}$, satisfying:

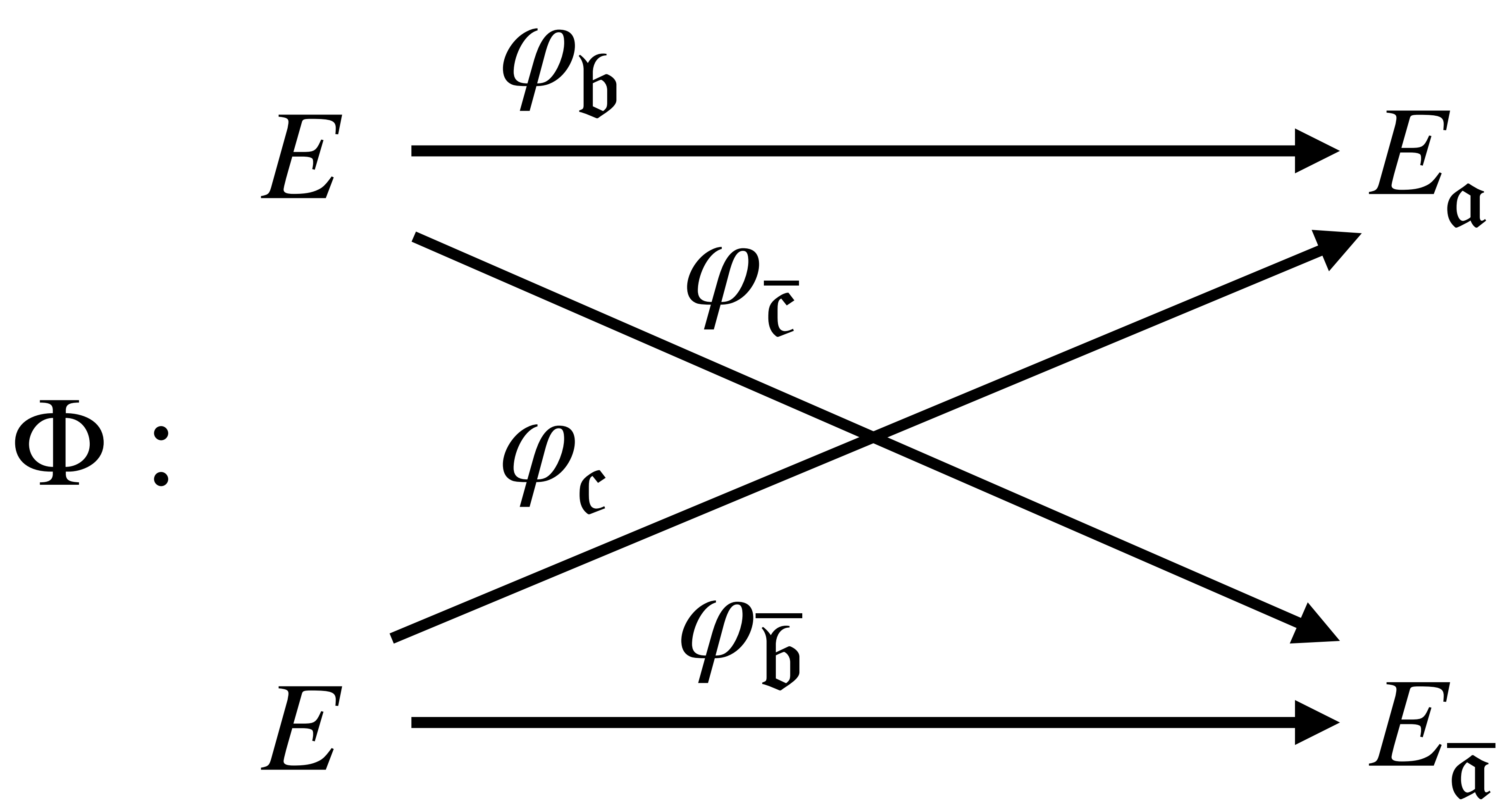
- $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$
- $n(\mathfrak{b}) + n(\mathfrak{c}) = 2^e$

Clapoti

Goal: Evaluate action of $[\mathfrak{a}]$

Assume we have: $\mathfrak{b}, \mathfrak{c}$, satisfying:

- $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$
- $n(\mathfrak{b}) + n(\mathfrak{c}) = 2^e$

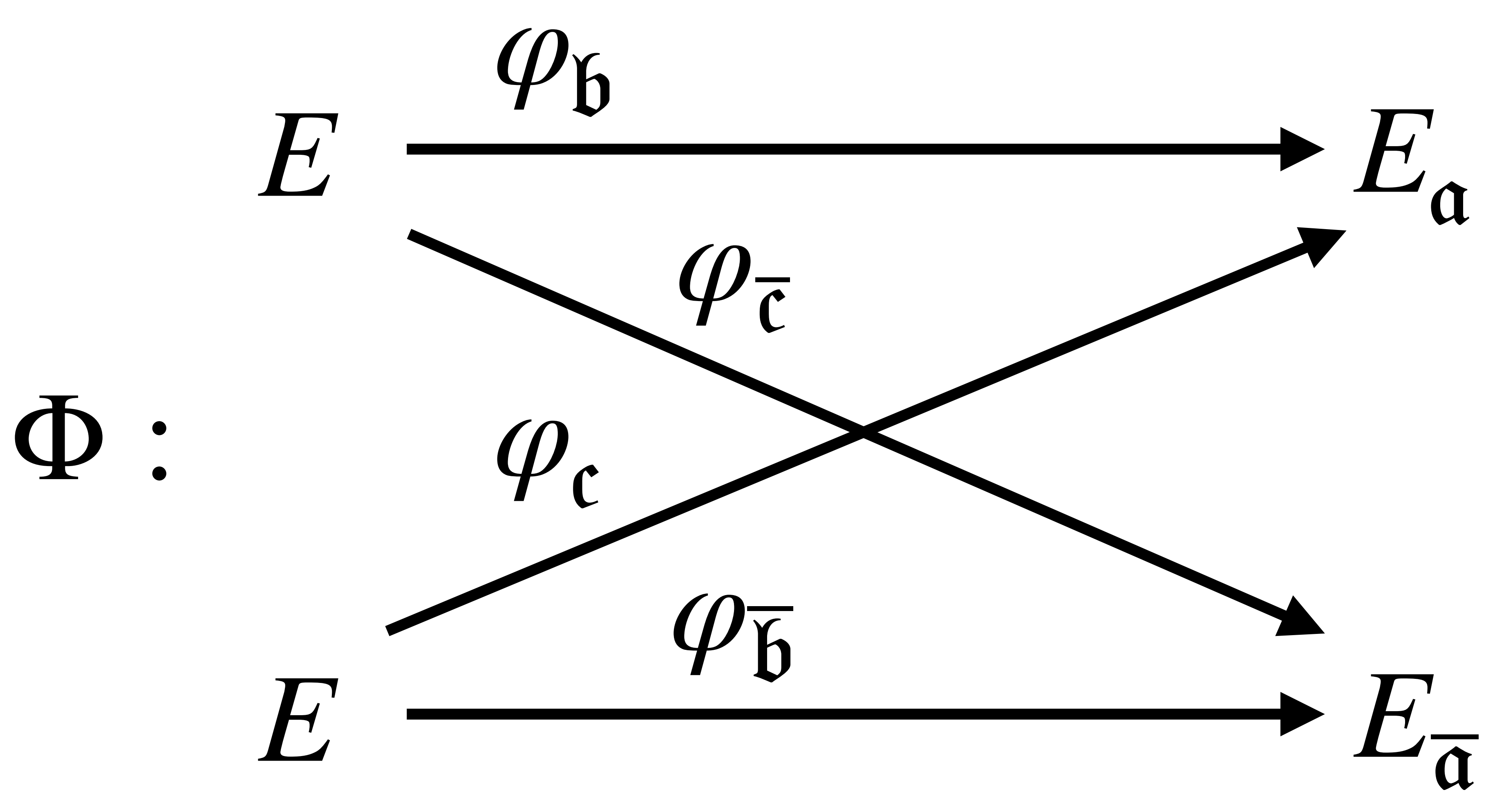


Clapoti

Goal: Evaluate action of $[\mathfrak{a}]$

Assume we have: $\mathfrak{b}, \mathfrak{c}$, satisfying:

- $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$
- $n(\mathfrak{b}) + n(\mathfrak{c}) = 2^e$



Can compute Φ from $\ker \Phi = \{(n(\mathfrak{b})P, \gamma(P)) \in E \times E \mid P \in E[2^e]\}$

$\gamma = \varphi_{\mathfrak{b}} \circ \varphi_{\overline{\mathfrak{c}}}$

Clapoti/KLaPoTi/PEGASIS

Goal: Evaluate action of $[\mathfrak{a}]$

Assume we have: $\mathfrak{b}, \mathfrak{c}$, satisfying:
- $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$
- $n(\mathfrak{b}) + n(\mathfrak{c}) = 2^e$

- **Clapoti:** Can drop this requirement on $\mathfrak{b}, \mathfrak{c}$, by going to dimension 8
  - Isogenies in dimension 8 are (for now) not practical

Clapoti/KLaPoTi/PEGASIS

Goal: Evaluate action of $[\mathfrak{a}]$

Assume we have: $\mathfrak{b}, \mathfrak{c}$, satisfying:

- $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$
- $n(\mathfrak{b}) + n(\mathfrak{c}) = 2^e$

- **Clapoti:** Can drop this requirement on $\mathfrak{b}, \mathfrak{c}$, by going to dimension 8
  - Isogenies in dimension 8 are (for now) not practical

- **KLaPoTi:** Finding $\mathfrak{b}, \mathfrak{c}$ can be done with a known algorithm (KLPT)!
  - 2^e needs to be quite large (compared to $disc(\mathbb{Z}[\pi])$)

Clapoti/KLaPoTi/PEGASIS

Goal: Evaluate action of $[\mathfrak{a}]$

Assume we have: $\mathfrak{b}, \mathfrak{c}$, satisfying:

- $[\mathfrak{a}] = [\mathfrak{b}] = [\mathfrak{c}]$
- $n(\mathfrak{b}) + n(\mathfrak{c}) = 2^e$

- **Clapoti:** Can drop this requirement on $\mathfrak{b}, \mathfrak{c}$, by going to dimension 8
  - Isogenies in dimension 8 are (for now) not practical

- **KLaPoTi:** Finding $\mathfrak{b}, \mathfrak{c}$ can be done with a known algorithm (KLPT)!
  - 2^e needs to be quite large (compared to $disc(\mathbb{Z}[\pi])$)

- **PEGASIS:** Original Clapoti + several tricks = works in dimension 4
  - Seems to be the right middle ground!

PEGASIS - Results

Paper	Impl.	500	1000	1500	2000	4000
SCALLOP [21]*	C++	35 s	750 s	–	–	–
SCALLOP-HD [15]*	Sage	88 s	1140 s	–	–	–
PEARL-SCALLOP [3]*	C++	30 s	58 s	710 s	–	–
KLaPoTi [49]	Sage	207 s	–	–	–	–
	Rust	1.95 s	–	–	–	–
PEGASIS (This work)	Sage	1.53 s	4.21 s	10.5 s	21.3 s	121 s

PEGASIS works over $\mathbb{F}_p$, and can be instantiated Frobenius!

Conclusion: (Unrestricted) effective group actions now exists, enabling many (so far, theoretical) constructions!

Thank you!

Questions?