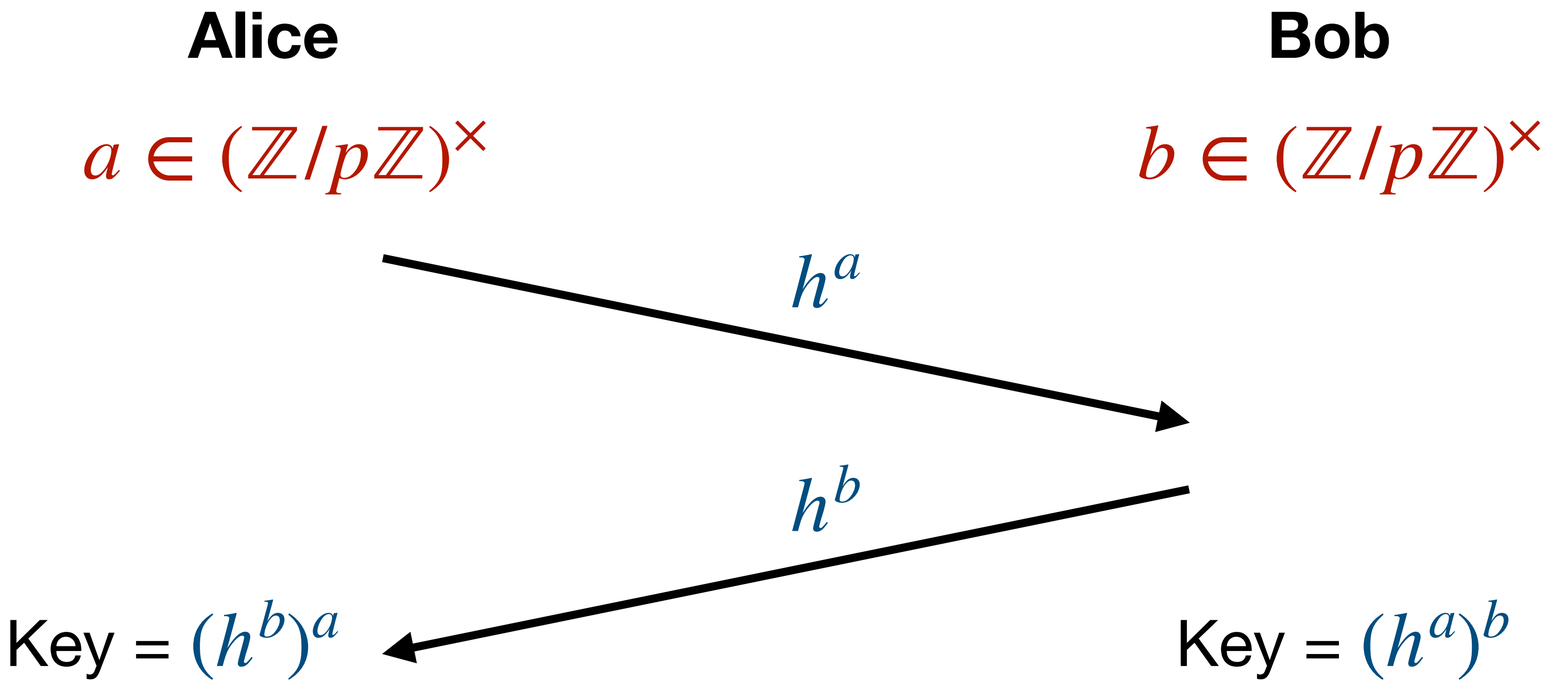
Faster SCALLOP from Non-Prime Conductor Suborders in Medium Sized Quadratic Fields

Joint work with Bill Allombert, Jean-François Biasse, Péter Kutas, Chris Leonardi, Aurel Page, Renate Scheidler and Márton Tot Bagi

Jonathan Komada Eriksen,
COSIC, KU Leuven

Diffie-Hellman

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



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 $(g_1 g_2) \star x = g_1 \star (g_2 \star x)$

Commutative: Refers to G being commutative

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 $(g_1 g_2) \star x = g_1 \star (g_2 \star x)$

Commutative: Refers to G being commutative

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

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

h^a

h^b

Key = $(h^b)^a$ $\quad$ Key = $(h^a)^b$

Setup parameters:

A commutative group G
acting on X
a fixed $x \in X$

$a \in G$ $\quad$ $b \in G$

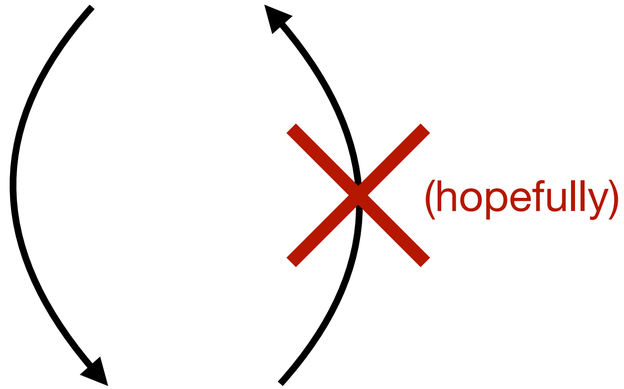
$a \star x$

$b \star x$

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

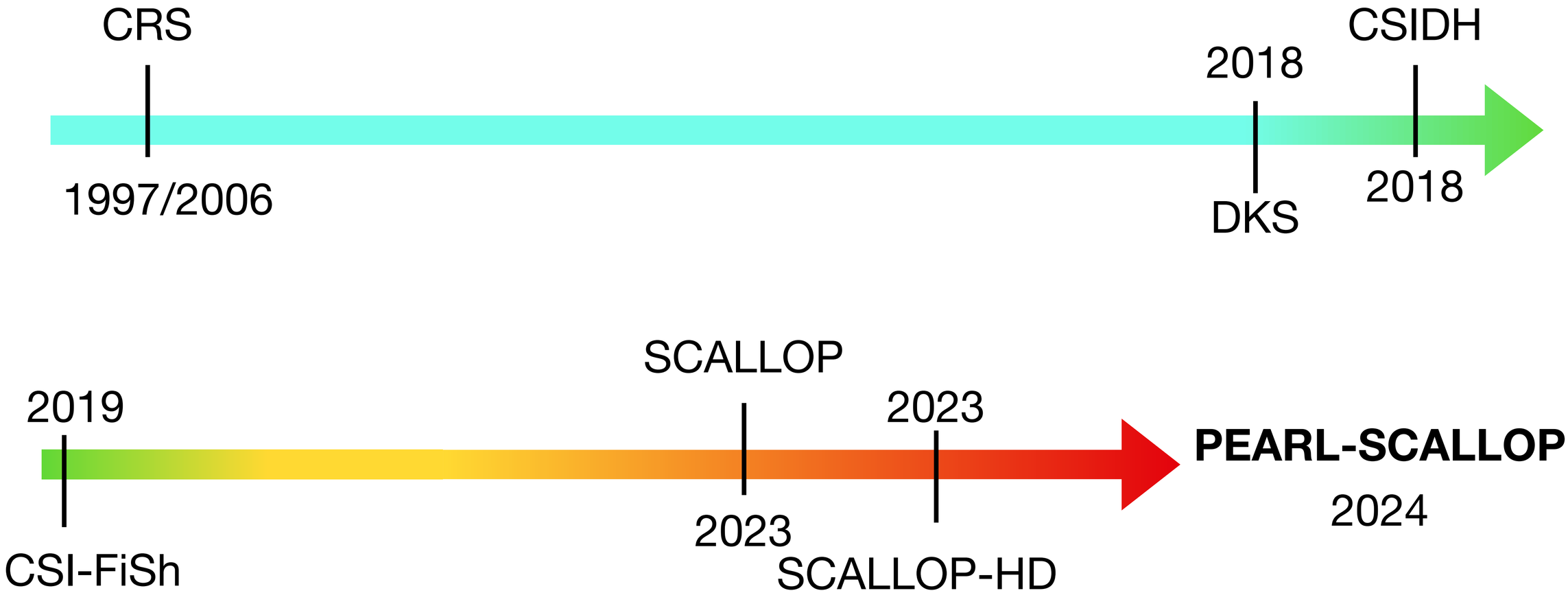
Hard problems:

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

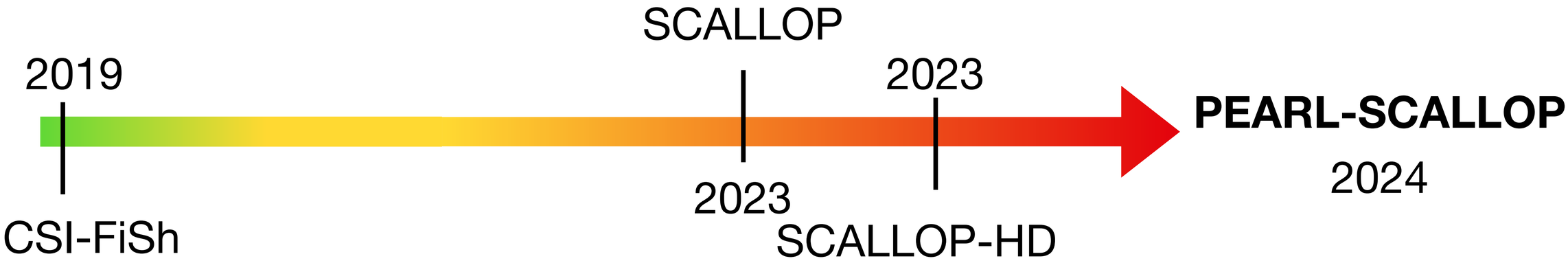


Vectorisation: given $a \star x, x$, find a

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:

$$X = \{(E, \pi_p) \mid \pi_p \text{ satisfying } \pi_p^2 = [-p]\}/\sim$$

The action:

$$G \times X \to X$$

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

Example

Let $\pi^2 = -53$

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

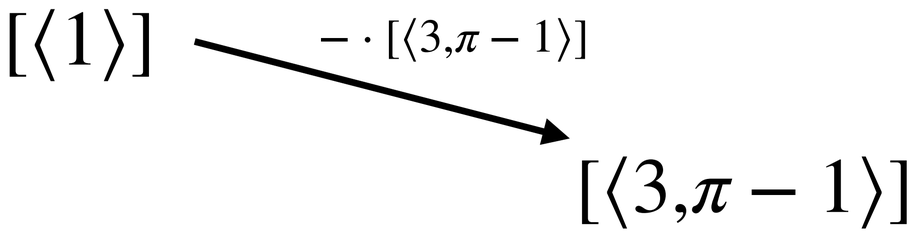
$$[\langle 1 \rangle], [\langle 2, \pi - 1 \rangle], [\langle 3, \pi - 1 \rangle], [\langle 13, \pi - 5 \rangle], [\langle 17, \pi - 7 \rangle], [\langle 23, \pi - 4 \rangle]$$

Example

Let $\pi^2 = -53$

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

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

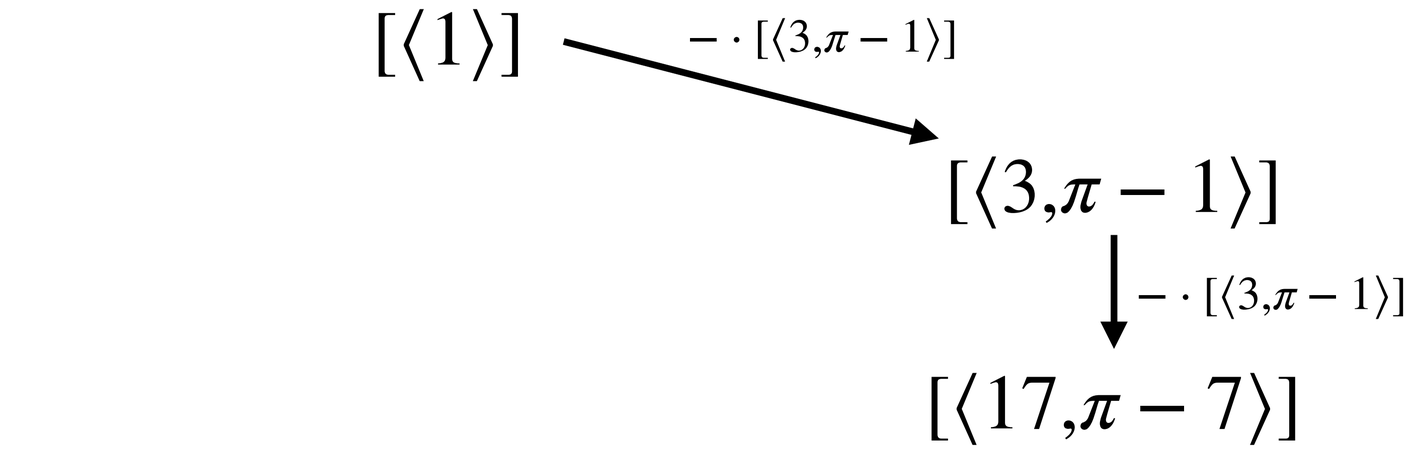


Example

Let $\pi^2 = -53$

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

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

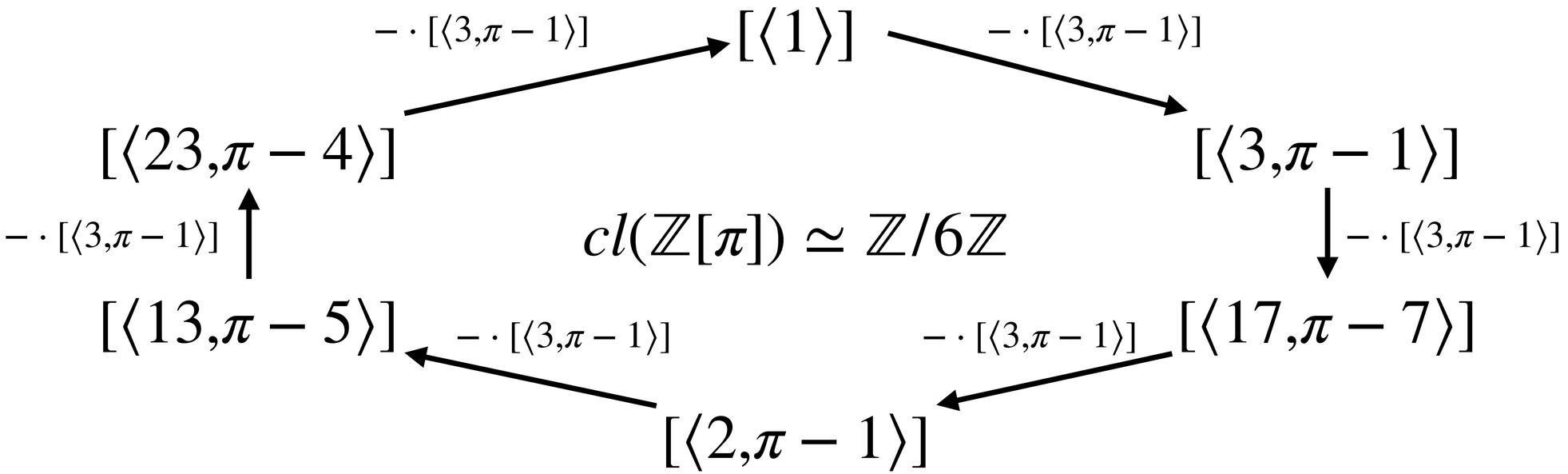


Example

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:

$$X = \{(E, \pi_p) \mid \pi_p \text{ satisfying } \pi_p^2 = [-p]\}/\sim$$

The action:

$$G \times X \to X$$

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

CRS/DKS/CSIDH, a restricted group action

$$X = \{(E, \pi_p) \mid \pi_p \text{ satisfying } \pi_p^2 = [-p]\}/\sim$$

$E/\mathbb{F}_p$ elliptic curve

CRS/DKS/CSIDH, a restricted group action

$$X = \{(E, \pi_p) \mid \pi_p \text{ satisfying } \pi_p^2 = [-p]\}/\sim$$

$E/\mathbb{F}_p$ elliptic curve

p-power Frobenius

$$\pi_p : E \to E$$

$$\pi_p((x, y)) = (x^p, y^p)$$

CRS/DKS/CSIDH, a restricted group action

$$X = \{(E, \pi_p) \mid \pi_p \text{ satisfying } \pi_p^2 = [-p]\}/\sim$$

$E/\mathbb{F}_p$ elliptic curve

p-power Frobenius

$$\pi_p : E \to E$$

$$\pi_p((x, y)) = (x^p, y^p)$$

Notice: for $(E, \pi_p) \in X$:

$$\iota : \mathbb{Z}[\sqrt{-p}] \hookrightarrow \mathrm{End}(E)$$

$$\iota(a + b\sqrt{-p}) = [a] + [b] \circ \pi_p$$

Is an (injective) ring-homomorphism!

CRS/DKS/CSIDH, a restricted group action

The group:

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

The set:

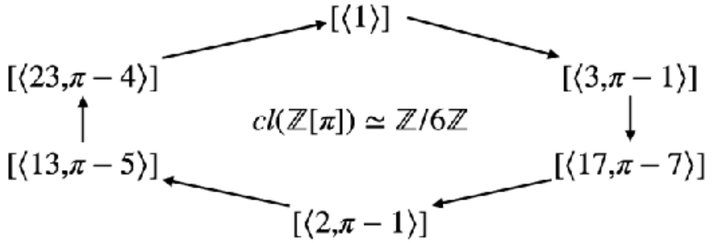
$$X = \{(E, \pi_p) \mid \pi_p \text{ satisfying } \pi_p^2 = [-p]\}/\sim$$

The action:

$$G \times X \to X$$

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

Class Group Action

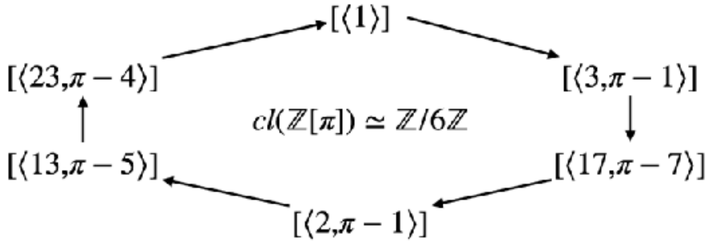


$\langle 2,\pi - 1\rangle \star -$

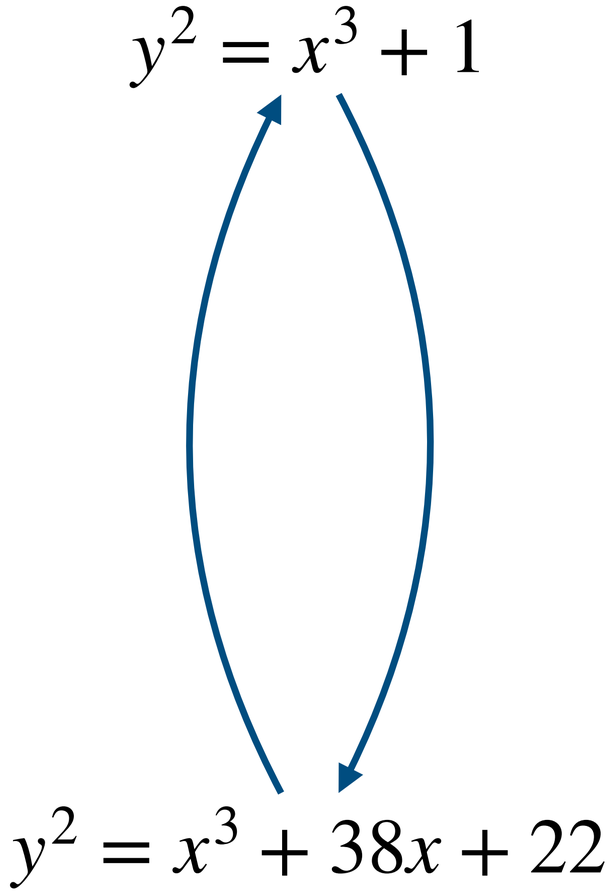
$$y^2 = x^3 + 1$$

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

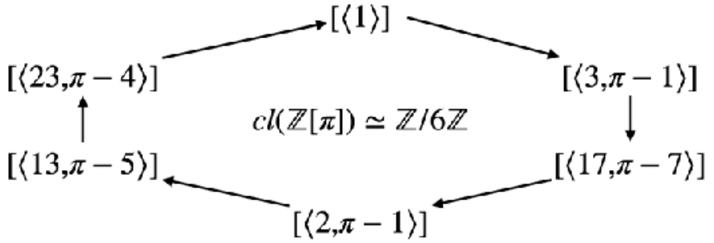
Class Group Action



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



Class Group Action



$y^2 = x^3 + 1$

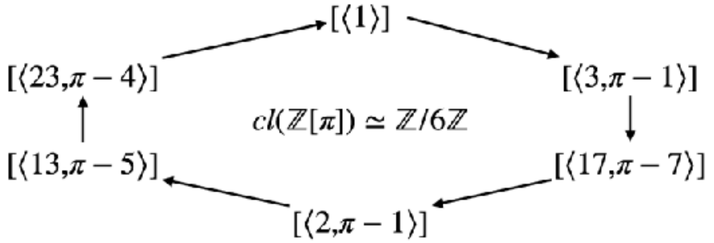
$y^2 = x^3 + 26$

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

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

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

Class Group Action



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

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

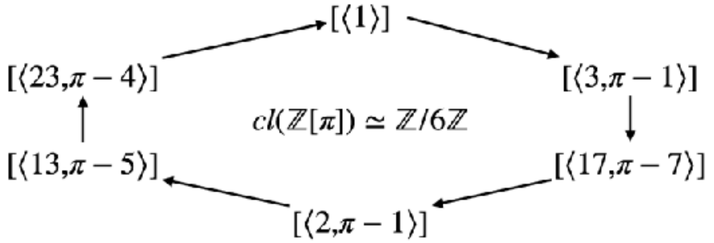
$y^2 = x^3 + 1$

$y^2 = x^3 + 26$

$y^2 = x^3 + 32x + 6$

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

Class Group Action



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

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

$y^2 = x^3 + 1$

$y^2 = x^3 + 22x + 5$

$y^2 = x^3 + 26$

$y^2 = x^3 + 24x + 42$

$y^2 = x^3 + 32x + 6$

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

CRS/DKS/CSIDH, a restricted group action

The action:

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

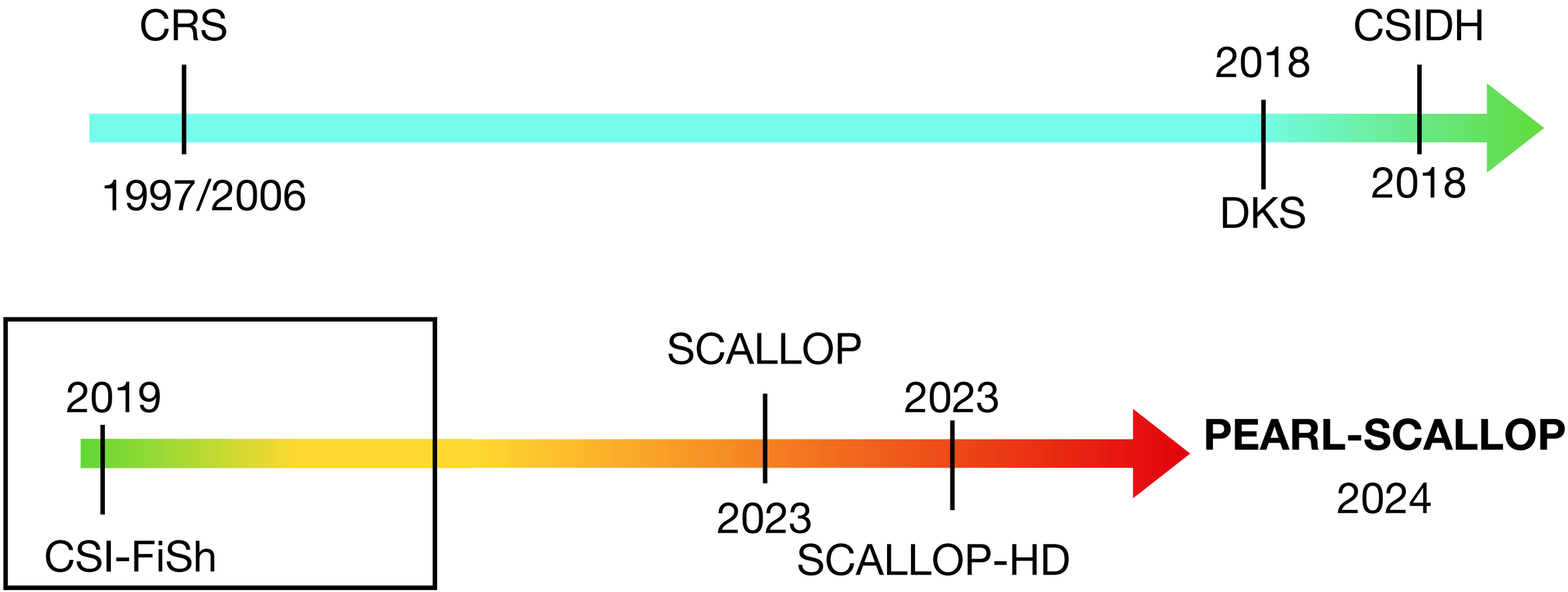
Can only compute **smooth degree** isogenies $\longleftrightarrow$ Can only compute the action of **smooth normed** ideals

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

Issue: Enough for key-exchange, but issue for essentially anything else

Group Action "Timeline"



CSi-FiSh: Turning a restricted GA into a GA

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

$$\begin{array}{ccccc} \mathbb{Z}^r & \longrightarrow & G & \longrightarrow & 0 \\ [1,0,\ldots,0] & \longrightarrow & g_1 & & \\ [0,1,\ldots,0] & \longrightarrow & g_2 & & \end{array}$$

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

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

CSi-FiSh: Turning a restricted GA into a GA

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

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

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

etc...

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

etc...

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

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

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: Turning a restricted GA into a GA

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

} Parameter generation

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

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

CSi-FiSh: Turning a restricted GA into a GA

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

} Parameter generation

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

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

Step 4: Evaluate the element $e - f$

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

CSi-FiSh: Turning a restricted GA into a GA

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

} Parameter generation

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

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

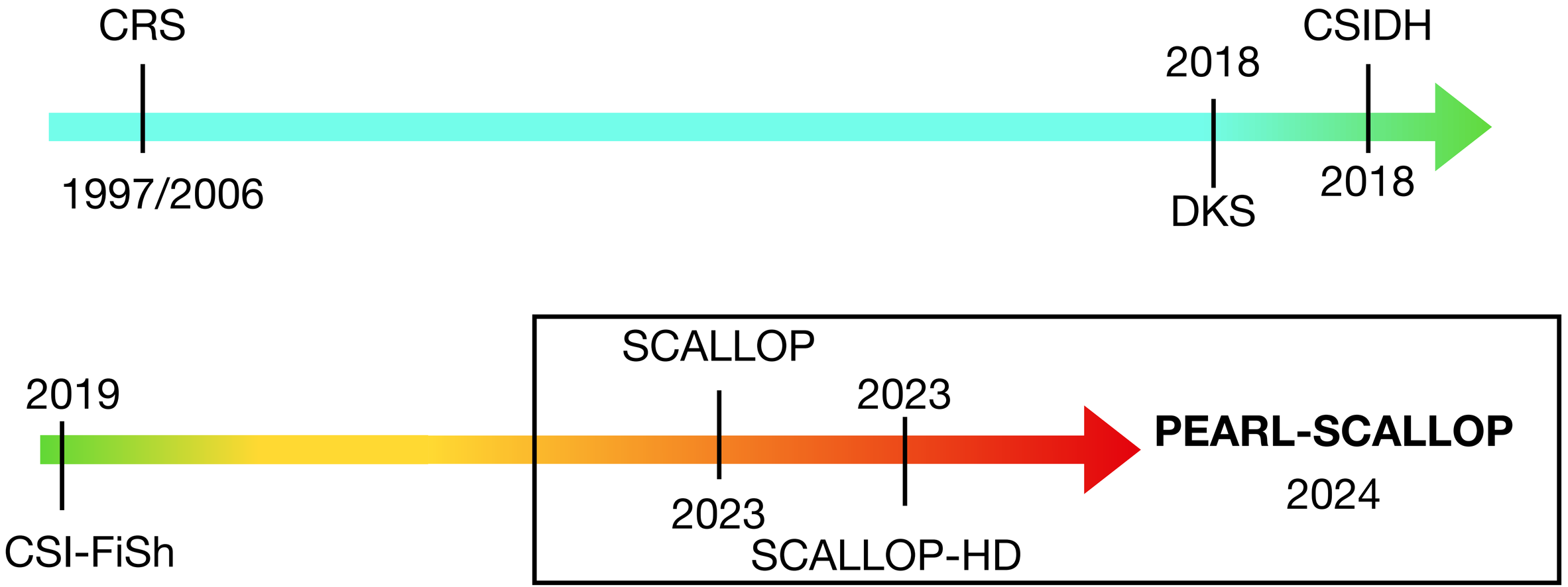
Step 4: Evaluate the element $e - f$

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

Result: CSIDH-512 can be made unrestricted!

Issue: For larger parameters, computing $Cl(\mathbb{Z}[\sqrt{-p}])$ is infeasible

Group Action "Timeline"



General orientations

$$\iota : \mathbb{Z}[\sqrt{-n}] \hookrightarrow \mathrm{End}(E)$$

$$\iota(a + b\sqrt{-n}) = [a] + [b] \circ \varphi$$

some $\varphi : E \to E$,
satisfying $\varphi^2 = [-n]$

$cl(\mathbb{Z}[\sqrt{-n}])$

$$G \times X \to X$$

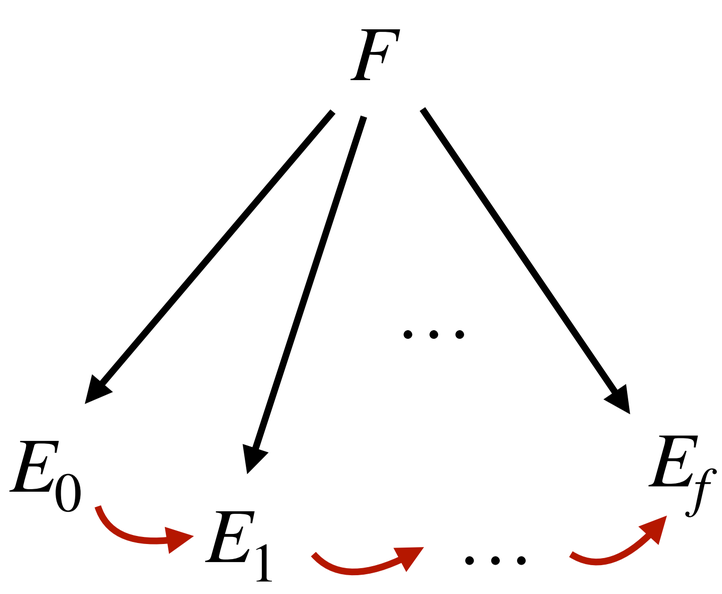
$$[\mathfrak{b}] \star (E, \iota) = \varphi_{\mathfrak{b}}(E), \varphi_{\mathfrak{b}}^{*}\iota))$$

$\{(E, \iota) \mid \iota$ orientation by $\mathbb{Z}[\sqrt{-n}]\}/\sim$

SCALLOP

Easy to compute class number!

$\iota : \mathbb{Z}[f\sqrt{-1}] \hookrightarrow \mathrm{End}(E)$



ISSUES:

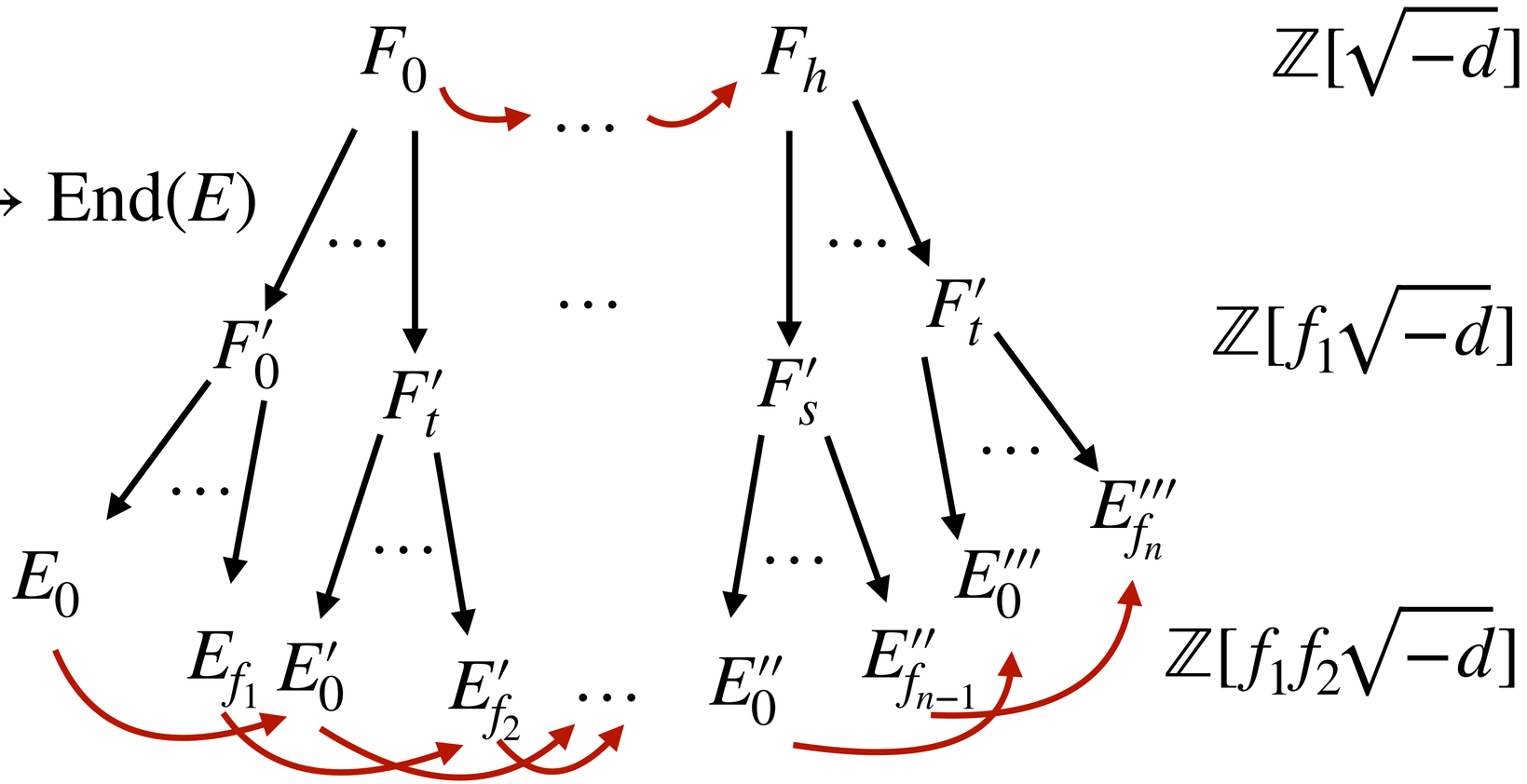
ι given by an isogeny

$\Rightarrow$ Need $\omega \in \mathbb{Z}[f\sqrt{-1}]$ of smooth norm

Recovering ascending isogeny enough to break protocol

PEARL-SCALLOP

$$\iota : \mathbb{Z}[f_1 \cdot \ldots \cdot f_n\sqrt{-d}] \hookrightarrow \mathrm{End}(E)$$



PREVIOUS ISSUES:

~~ι given by an isogeny~~

~~$\Rightarrow$ Need $\omega \in \mathbb{Z}[f\sqrt{-1}]$ of smooth norm~~

~~Recovering ascending isogeny enough to break protocol~~

$\Rightarrow$ Extra flexibility, so can find $n(\omega) = 2^e$

$\Rightarrow$ No clue which F_i is "on top"

PEARL-SCALLOP: Results

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

Infeasible to generate

CSIDH-2000+: We outline how to compute (feasible, but expensive)

PEARL-SCALLOP: Results

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

Infeasible to generate

CSIDH-2000+: We outline how to compute (feasible, but expensive)

For certain MPC protocols,
PEGASIS + PEARL-SCALLOP = 💖

Thank you!

Questions?