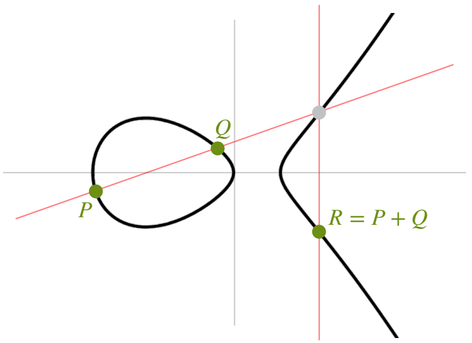
PART 2

from 2 to 2^{1000} isogenies

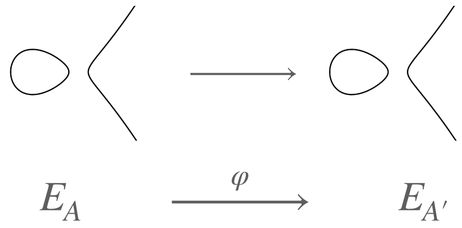
In part 1: elliptic curves, isogenies in general



Elliptic Curves

- have seen elliptic curves $E_A : y^2 = x^3 + Ax^2 + x$
- have seen scalar multiplication $P \mapsto [n]P$
- have done x-only arithmetic $x(P) \mapsto x([n]P)$

arithmetic on the curve
(enough for pre-quantum ECDSA)

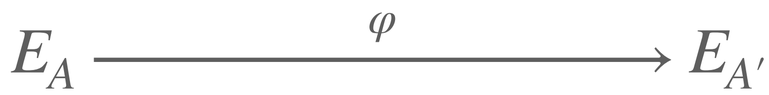


Isogenies

- have seen (general) isogenies $E_A \to E_{A'}$
- computed 2-isogenies with kernel $(\alpha,0) \in E[2]$
- have seen paths in 2-isogeny graph $G_2(\mathbb{F}_q)$

isogenies between curves
(post-quantum stuff!)

Goal:
do an isogeny
of degree 2^{1000}



Goal: do an isogeny of degree 2^{1000}

1

a point $P \in E_A$ of order 2
gives us a 2-isogeny
$E_A \to E_{A'}$

2

a point $P \in E_A$ of order 2^n
gives us a2^n-isogeny
$E_A \to E_{A'}$

Goal: do an isogeny of degree 2^{1000}

1

a point $P \in E_A$ of order 2
gives us a 2-isogeny
$E_A \to E_{A'}$

2

a point $P \in E_A$ of order 2^n
gives us a 2^n-isogeny
$E_A \to E_{A'}$

---

problem...

computing a 2^n-isogeny using
Velu's formulas would take $\mathcal{O}(2^n)$

this is **very slow**

Goal: do an isogeny of degree 2^{1000}

1

a point $P \in E_A$ of order 2
gives us a 2-isogeny
$E_A \to E_{A'}$

2

a point $P \in E_A$ of order 2^n
gives us a 2^n-isogeny
$E_A \to E_{A'}$

---

problem...

computing a 2^n-isogeny using
Velu's formulas would take $\mathcal{O}(2^n)$

this is **very slow**

solution!

any isogeny of degree $\prod_i \ell_i^{e_i}$
can be decomposed into
isogenies of degree ℓ_i

Goal: do an isogeny of degree 2^{1000}

1

a point $P \in E_A$ of order 2
gives us a 2-isogeny
$E_A \to E_{A'}$

2

a point $P \in E_A$ of order 2^n
gives us a 2^n-isogeny
$E_A \to E_{A'}$

---

problem...

computing a 2^n-isogeny using Velu's formulas would take $\mathcal{O}(2^n)$

this is **very slow**

solution!

any isogeny of degree $\prod_i \ell_i^{e_i}$

can be decomposed into isogenies of degree ℓ_i

so our 2^n-isogeny φ given by $P \in E_A$

$$E_A \xrightarrow{\quad\varphi\quad} E_{A'}$$

can also be written as

$$\underbrace{E_A \to E_1 \to \ldots \to E_{n-1} \to E_{A'}}_{n \text{ isogenies of degree } 2}$$

from 2 to 2^{128}

Goal: do an isogeny of degree 2^{1000}

more problems...

- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?

Goal: do an isogeny of degree 2^{1000}

more problems...

- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?
- **problem:** such a point $P = (x, y)$ probably doesn't have $x, y \in \mathbb{F}_{q'}$ so not in $E(\mathbb{F}_q)$
- this would make computations very slow!

Goal: do an isogeny of degree 2^{1000}

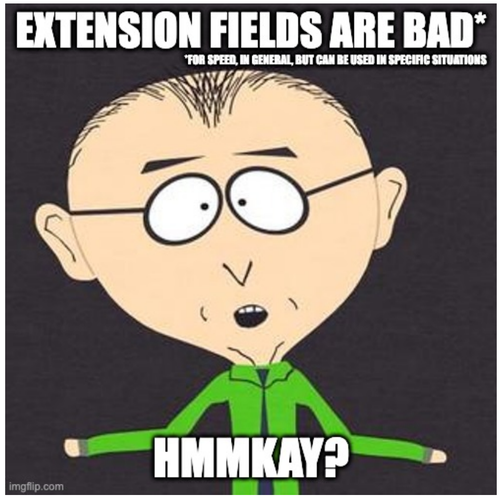
more problems...

- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?
- **problem:** such a point $P = (x, y)$ probably doesn't have $x, y \in \mathbb{F}_{q'}$ so not in $E(\mathbb{F}_q)$
- this would make computations very slow!
- what is the largest f such that we can have a point $P \in E[2^f]$, e.g. of order 2^f ?

Goal: do an isogeny of degree 2^{1000}

more problems...

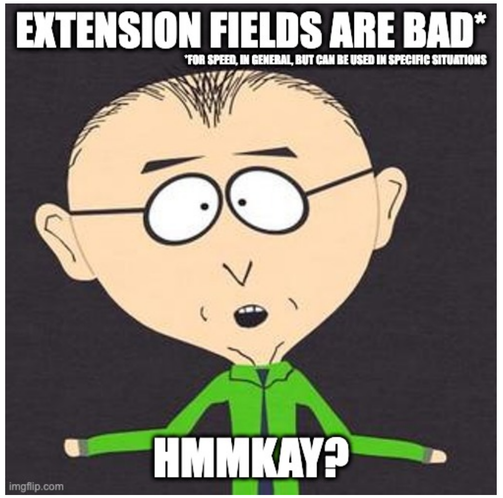
- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?
- **problem:** such a point $P = (x, y)$ probably doesn't have $x, y \in \mathbb{F}_{q'}$ so not in $E(\mathbb{F}_q)$
- this would make computations very slow!
- what is the largest f such that we can have a point $P \in E[2^f]$, e.g. of order 2^f ?



Goal: do an isogeny of degree 2^{1000}

more problems...

- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?
- **problem:** such a point $P = (x, y)$ probably doesn't have $x, y \in \mathbb{F}_{q'}$ so not in $E(\mathbb{F}_q)$
- this would make computations very slow!
- what is the largest f such that we can have a point $P \in E[2^f]$, e.g. of order 2^f ?

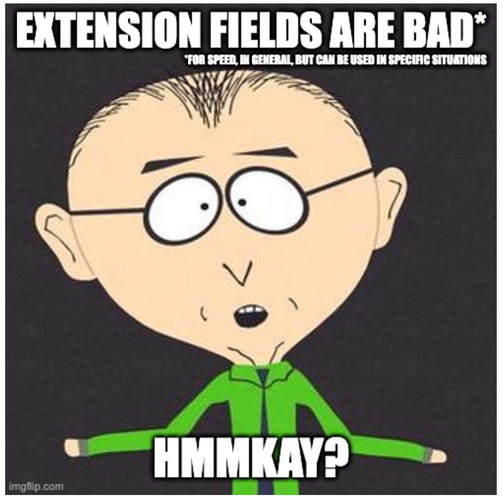


Fact: if $2^f \mid p + 1$ then $E[2^f] \subseteq E(\mathbb{F}_{p^2})$

Goal: do an isogeny of degree 2^{1000}

more problems...

- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?
- **problem:** such a point $P = (x, y)$ probably doesn't have $x, y \in \mathbb{F}_{q'}$ so not in $E(\mathbb{F}_q)$
- this would make computations very slow!
- what is the largest f such that we can have a point $P \in E[2^f]$, e.g. of order 2^f ?



Fact: if $2^f \mid p + 1$ then $E[2^f] \subseteq E(\mathbb{F}_{p^2})$

$$E_A \xrightarrow{\varphi} E_{A'}$$

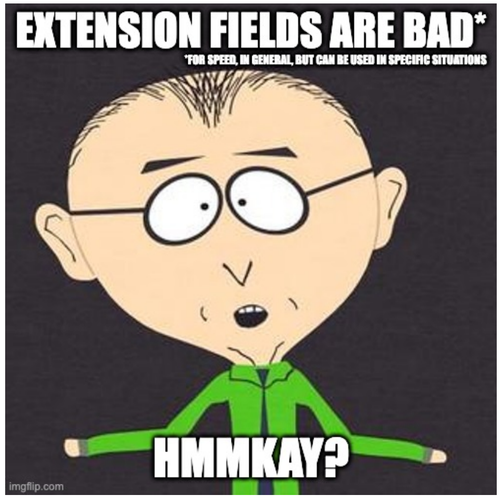
more solutions!

- for our prime p, we have $2^{128} \mid p + 1$, so we will write $f = 128$
- essentially, we can compute 2^f-isogenies given such a point $P \in E_A[2^f]$
- we compute a 2^{1000}-isogeny by splitting it up into 8 chunks of size 2^f

Goal: do an isogeny of degree 2^{1000}

more problems...

- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?
- **problem:** such a point $P = (x, y)$ probably doesn't have $x, y \in \mathbb{F}_{q'}$ so not in $E(\mathbb{F}_q)$
- this would make computations very slow!
- what is the largest f such that we can have a point $P \in E[2^f]$, e.g. of order 2^f ?



Fact: if $2^f \mid p + 1$ then $E[2^f] \subseteq E(\mathbb{F}_{p^2})$

more solutions!

- for our prime p, we have $2^{128} \mid p + 1$, so we will write $f = 128$
- essentially, we can compute 2^f-isogenies given such a point $P \in E_A[2^f]$
- we compute a 2^{1000}-isogeny by splitting it up into 8 chunks of size 2^f

$$E_A \xrightarrow{\varphi} E_{A'}$$

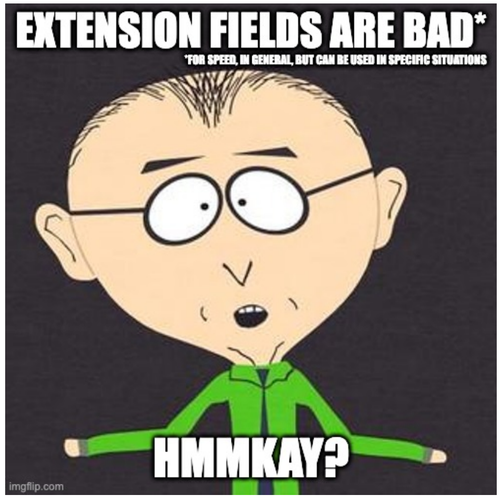
$$E_A \xrightarrow{\varphi_1} E^{(1)} \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_7} E^{(7)} \xrightarrow{\varphi_8} E_{A'}$$

degree 2^f

Goal: do an isogeny of degree 2^{1000}

more problems...

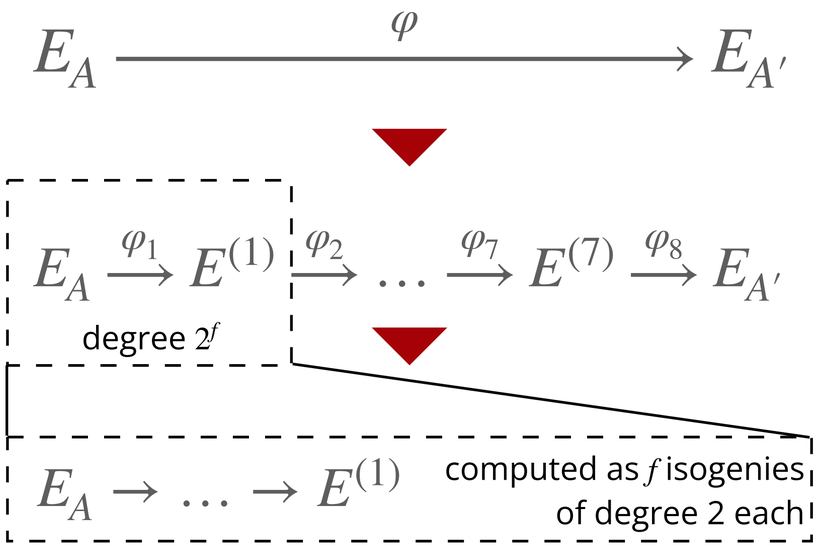
- we know how to do a 2-isogeny, given a point $P \in E_A[2]$
- we want to compute a 2^{1000} so we would need a point $P \in E_A[2^{1000}]$ or something...?
- **problem:** such a point $P = (x, y)$ probably doesn't have $x, y \in \mathbb{F}_{q'}$ so not in $E(\mathbb{F}_q)$
- this would make computations very slow!
- what is the largest f such that we can have a point $P \in E[2^f]$, e.g. of order 2^f ?



Fact: if $2^f \mid p + 1$ then $E[2^f] \subseteq E(\mathbb{F}_{p^2})$

more solutions!

- for our prime p, we have $2^{128} \mid p + 1$, so we will write $f = 128$
- essentially, we can compute 2^f-isogenies given such a point $P \in E_A[2^f]$
- we compute a 2^{1000}-isogeny by splitting it up into 8 chunks of size 2^f



Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!

E_1

P

$[2^3]P$

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

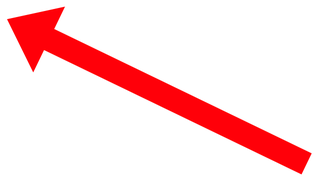
How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!

$$E_1$$

$$P$$

$$[2^3]P$$



order 2!!!

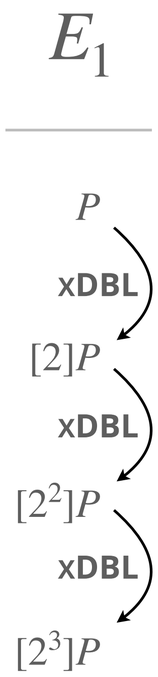
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!

$$E_1 \quad \to \quad E_2$$

P
xDBL
$[2]P$
xDBL
$[2^2]P$
xDBL
$[2^3]P$

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

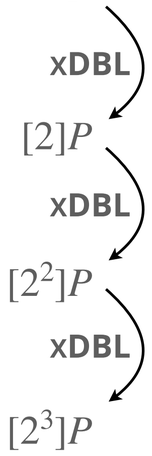
Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!

$$E_1 \quad \to \quad E_2$$

$$P \quad \mapsto \quad P'$$



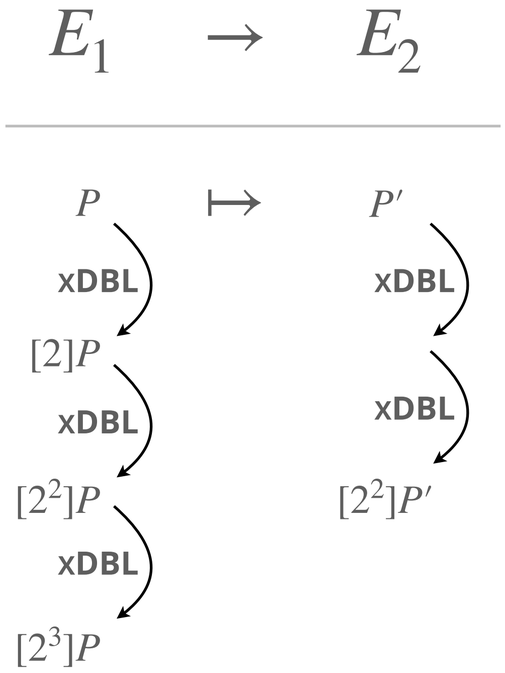
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



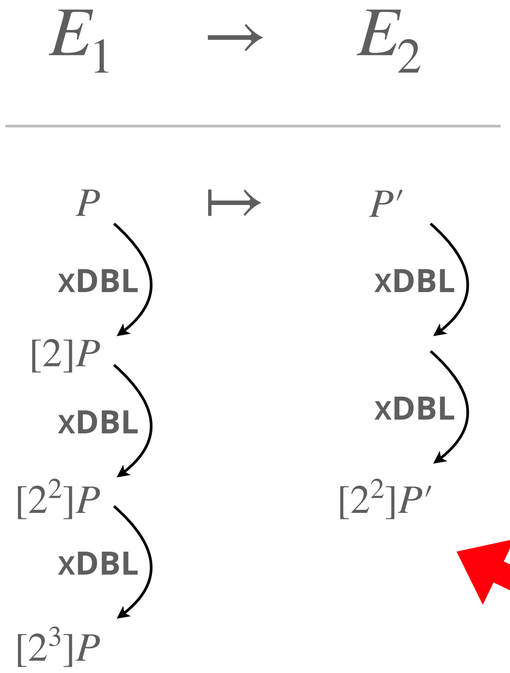
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



order 2!!!

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

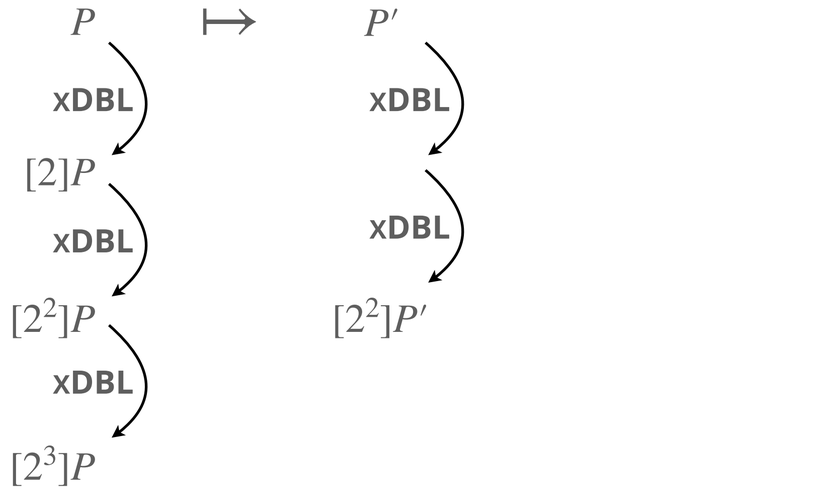
toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!

$$E_1 \to E_2 \to E_3$$



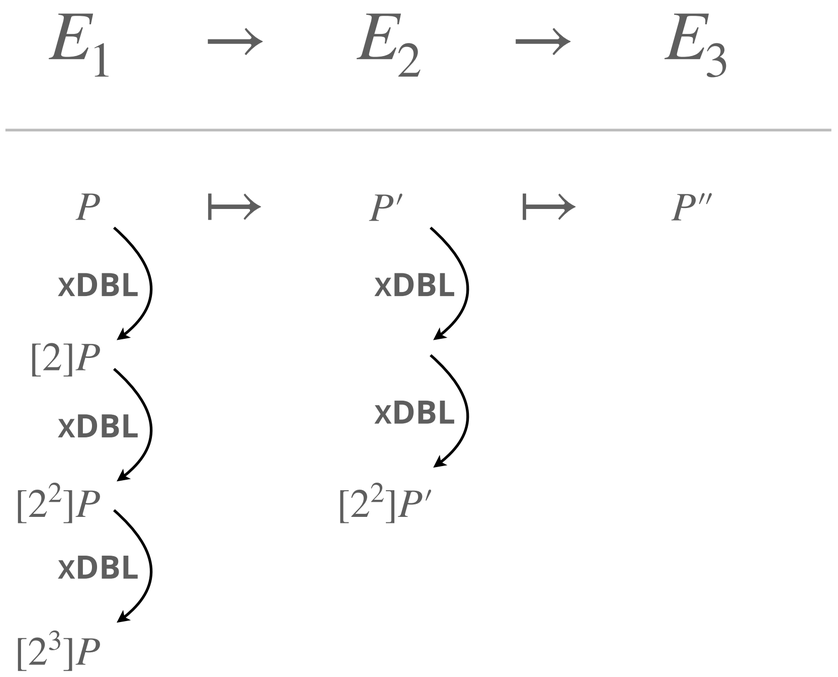
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



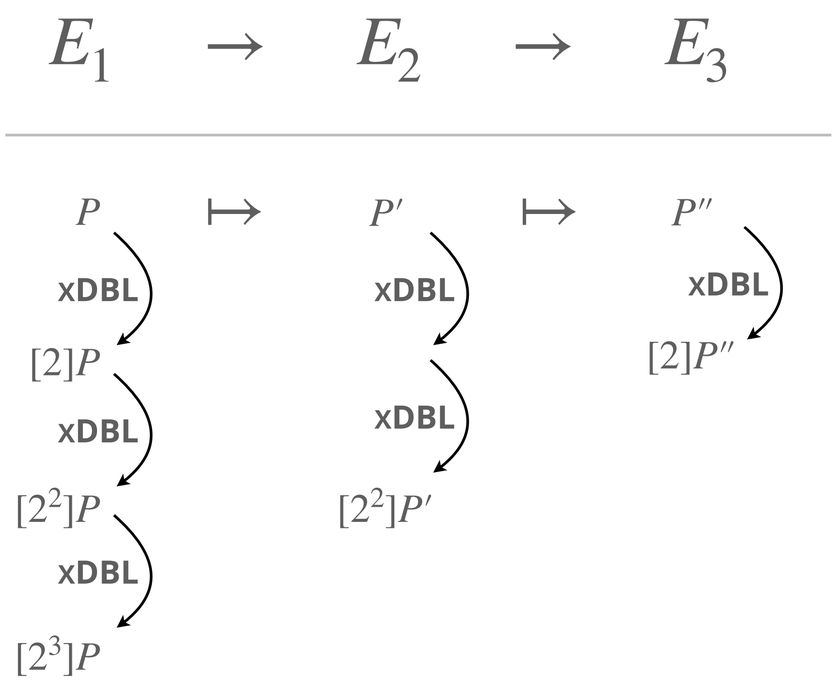
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$ of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the 2^f-isogeny given by P as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



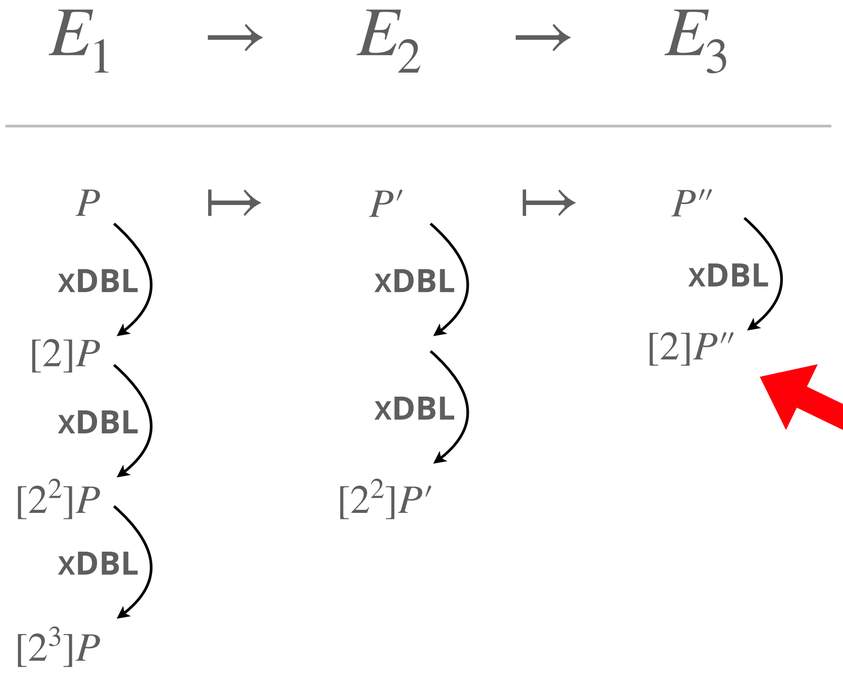
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$ of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the 2^f-isogeny given by P as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



order 2!!

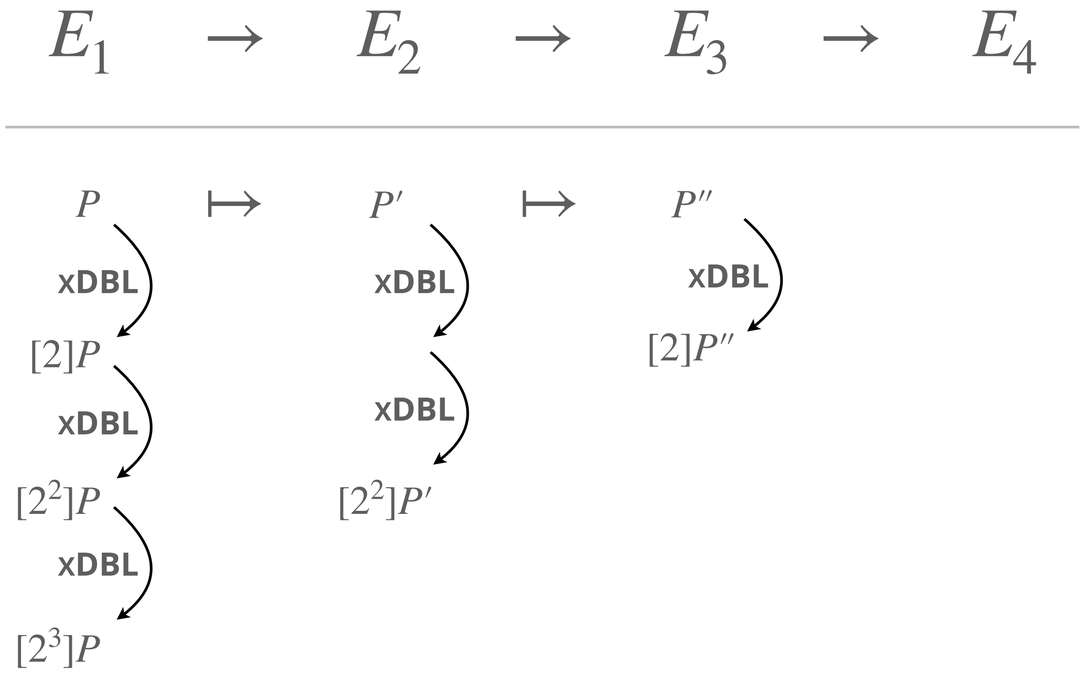
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$ of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the 2^f-isogeny given by P as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



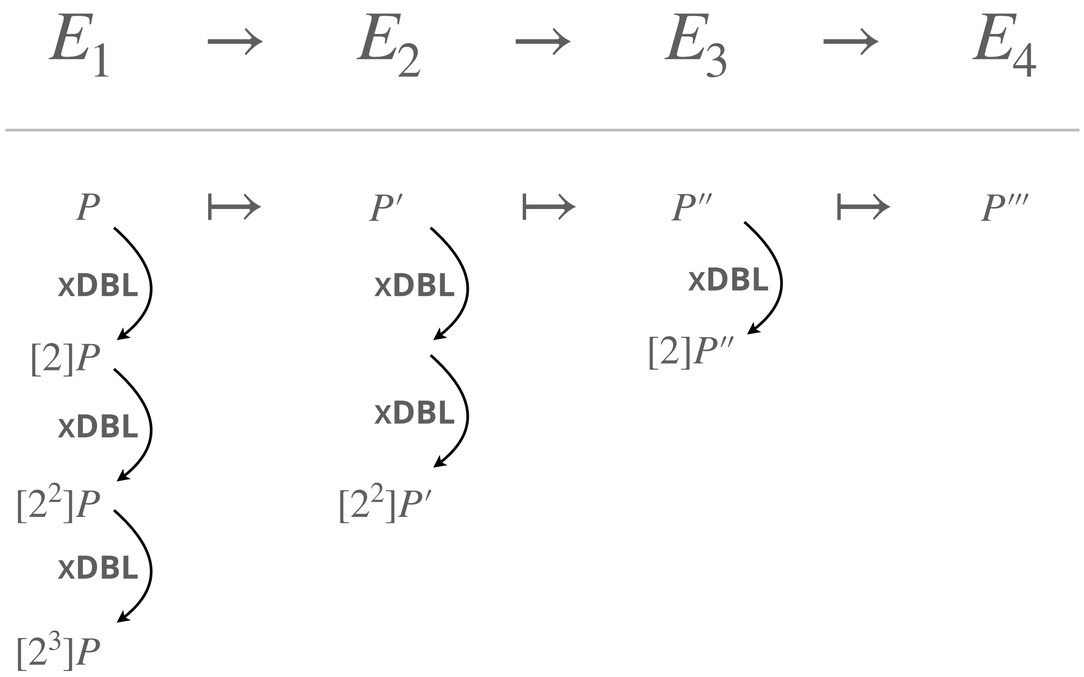
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$
of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the
2^f-isogeny given by P
as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



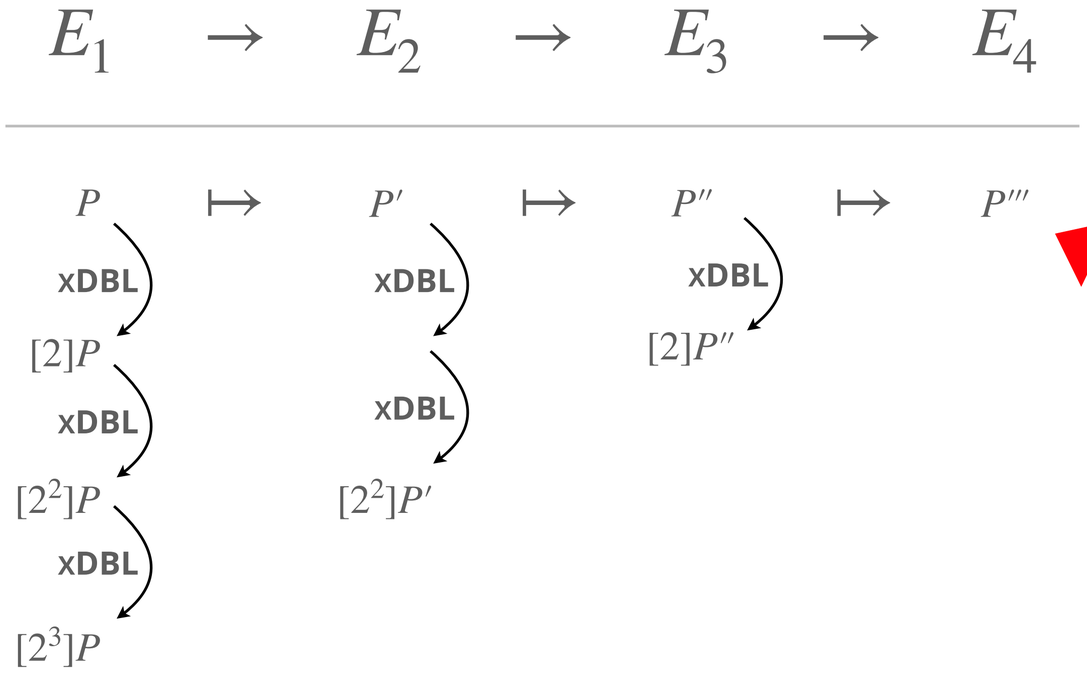
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

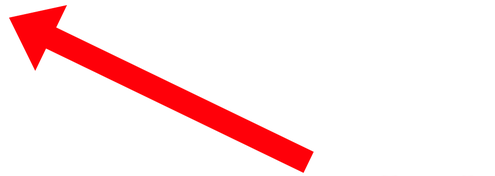
toy example

Assume $f = 4$, so we have point $P \in E_A$ of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the 2^f-isogeny given by P as those f isogenies of degree 2?

First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!





orc

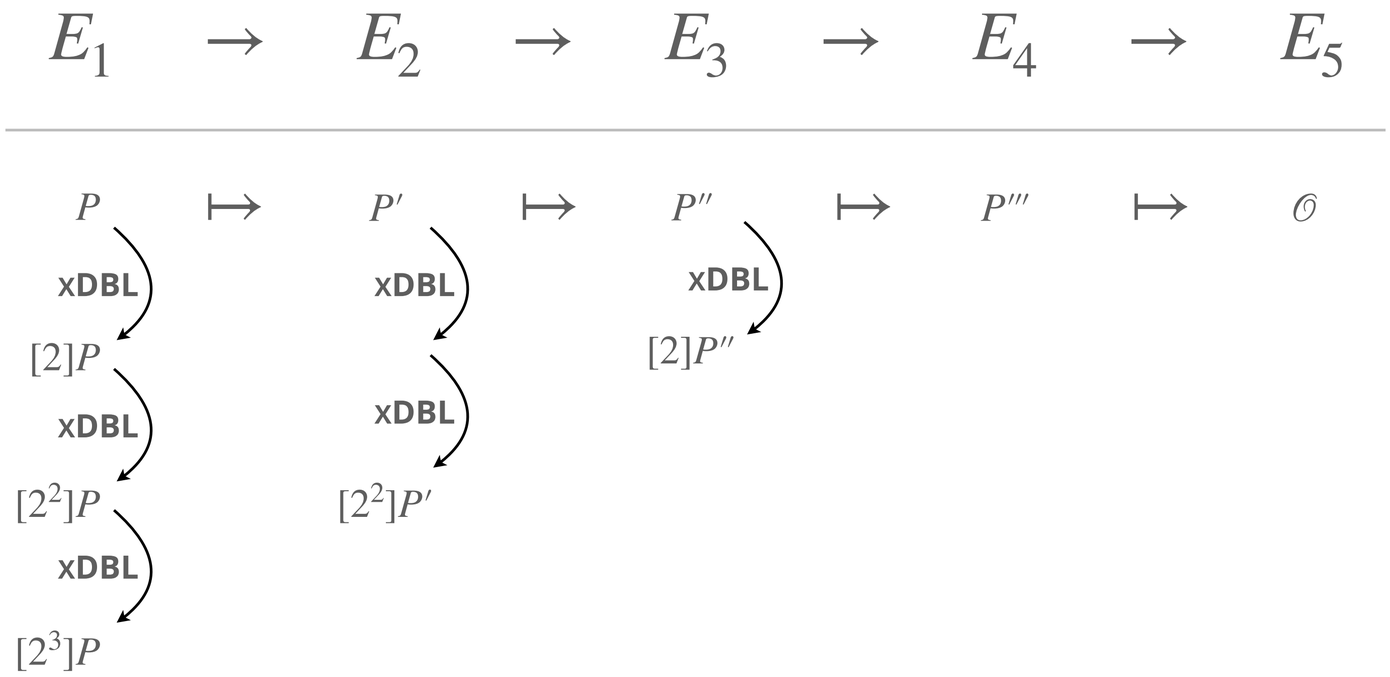
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ▶ Subgoal: do eight blocks of such isogenies

toy example

Assume $f = 4$, so we have point $P \in E_A$ of order $2^f = 16$ with $x, y \in \mathbb{F}_q$

How do we *actually* compute the 2^f-isogeny given by P as those f isogenies of degree 2?

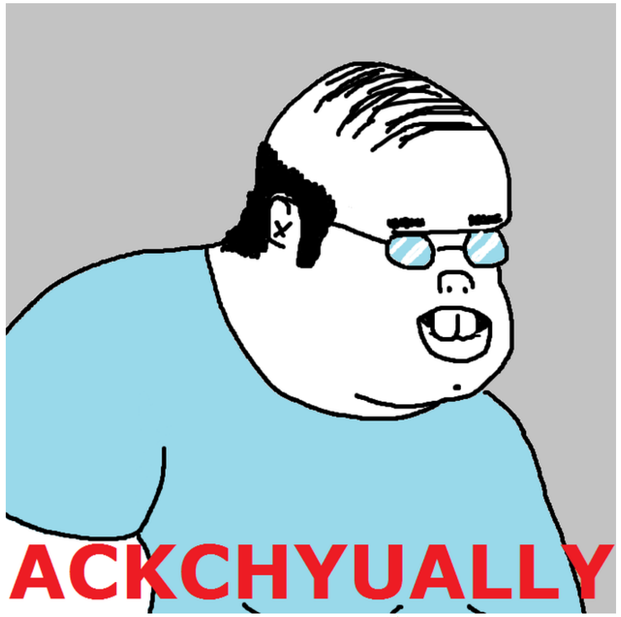
First step is easy:
$R := [2^{f-1}]P$ is a point of order 2
So we can use this for $E_1 \to E_2$
Then rinse and repeat!



Goal: do an isogeny of degree 2^{1000}

Subgoal: do an isogeny of degree 2^f

Subgoal: do eight blocks of such isogenies

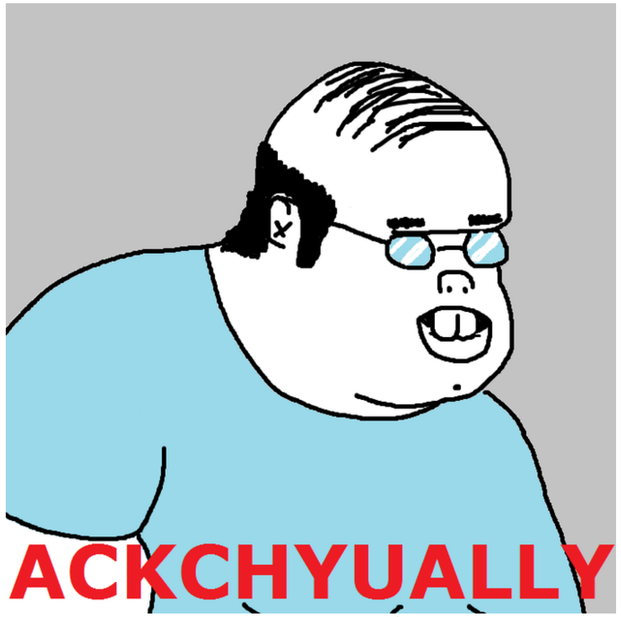


someone in the audience right now

Goal: do an isogeny of degree 2^{1000}

Subgoal: do an isogeny of degree 2^f ✓

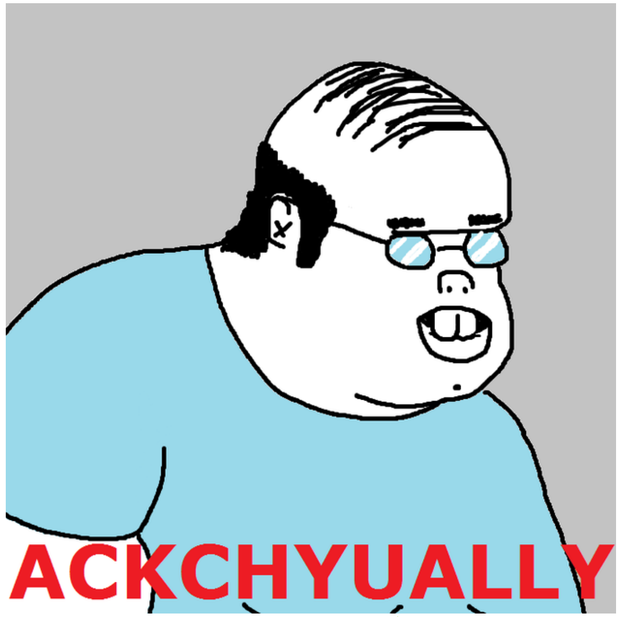
Subgoal: do eight blocks of such isogenies



someone in the audience right now

$$
\begin{array}{ccccccccc}
E_1 & \to & E_2 & \to & E_3 & \to & E_4 & \to & E_5 \\
\hline
P & \mapsto & P' & \mapsto & P'' & \mapsto & P''' & \mapsto & \mathcal{O} \\
\downarrow \text{xDBL} & & & & & & & & \\
[2]P & \mapsto & [2]P' & \mapsto & [2]P'' & & & & \\
\downarrow \text{xDBL} & & & & & & & & \\
[2^2]P & \mapsto & [2^2]P' & & & & & & \\
\downarrow \text{xDBL} & & & & & & & & \\
[2^3]P & & & & & & & &
\end{array}
$$

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies



someone in the audience right now

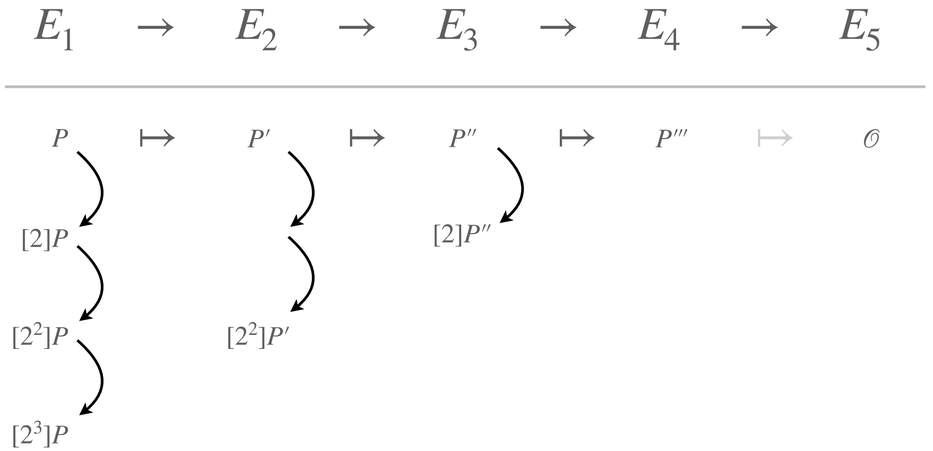
$$
\begin{array}{ccccccccc}
E_1 & \to & E_2 & \to & E_3 & \to & E_4 & \to & E_5 \\
\hline
P & \mapsto & P' & \mapsto & P'' & \mapsto & P''' & \mapsto & \mathcal{O} \\
\downarrow \text{xDBL} & & & & & & & & \\
[2]P & \mapsto & [2]P' & \mapsto & [2]P'' & & & & \\
\downarrow \text{xDBL} & & & & & & & & \\
[2^2]P & \mapsto & [2^2]P' & & & & & & \\
\downarrow \text{xDBL} & & & & & & & & \\
[2^3]P & & & & & & & &
\end{array}
$$

order 2!!!

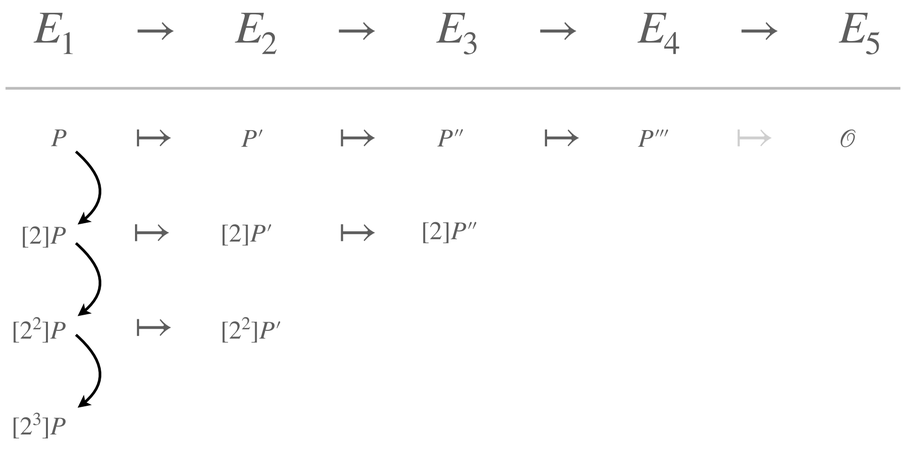
Which strategy is better?

(vote by raising hands)

Strategy 1: DBLs per curve, push 1 point



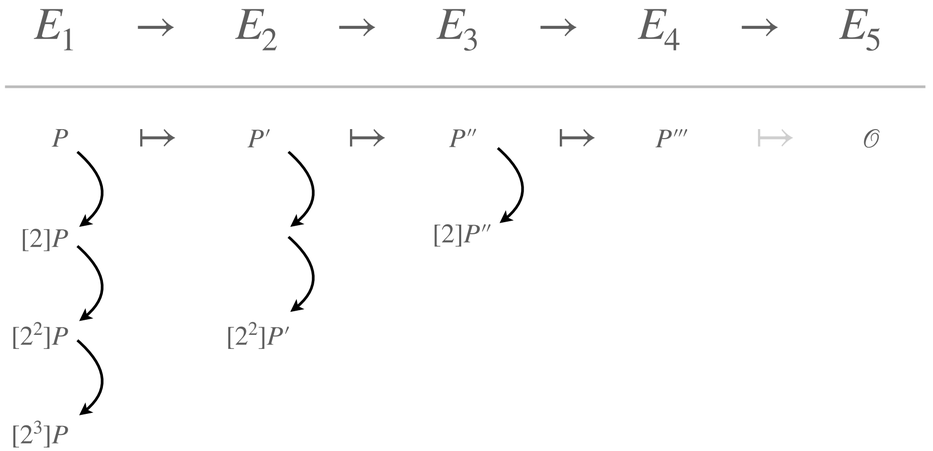
Strategy 2: DBL only on E_1, push all points



Which strategy is better?

(vote by raising hands)

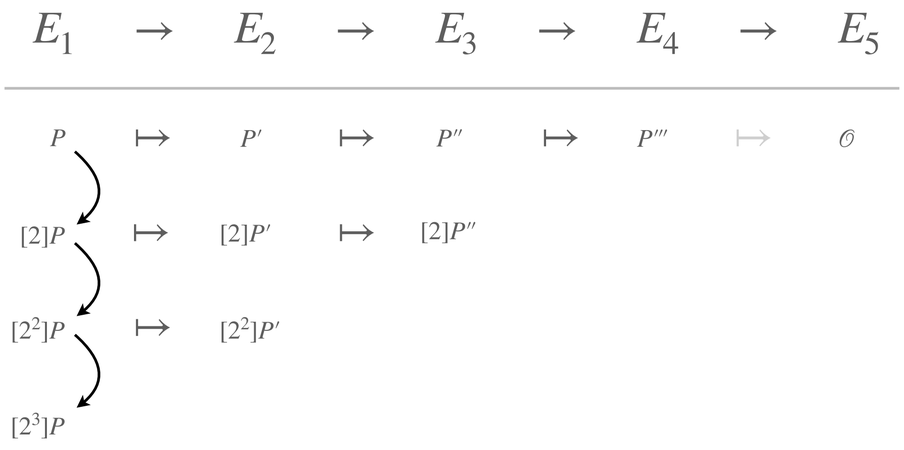
Strategy 1: DBLs per curve, push 1 point



in total:

6 DBLs
3 PUSH

Strategy 2: DBL only on E_1, push all points



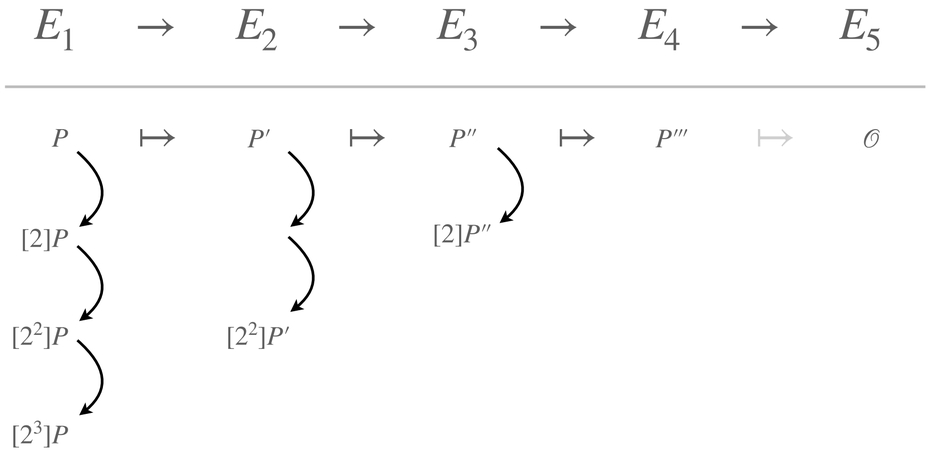
in total:

3 DBLs
6 PUSH

Which strategy is better?

(vote by raising hands)

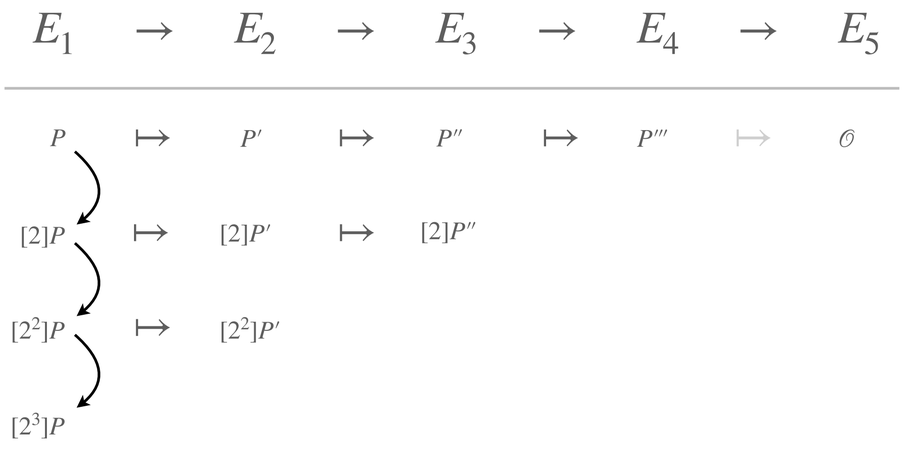
Strategy 1: DBLs per curve, push 1 point



in total:

6 DBLs
3 PUSH

Strategy 2: DBL only on E_1, push all points



in total:

3 DBLs
6 PUSH

Answer: Completely depends on ratio between

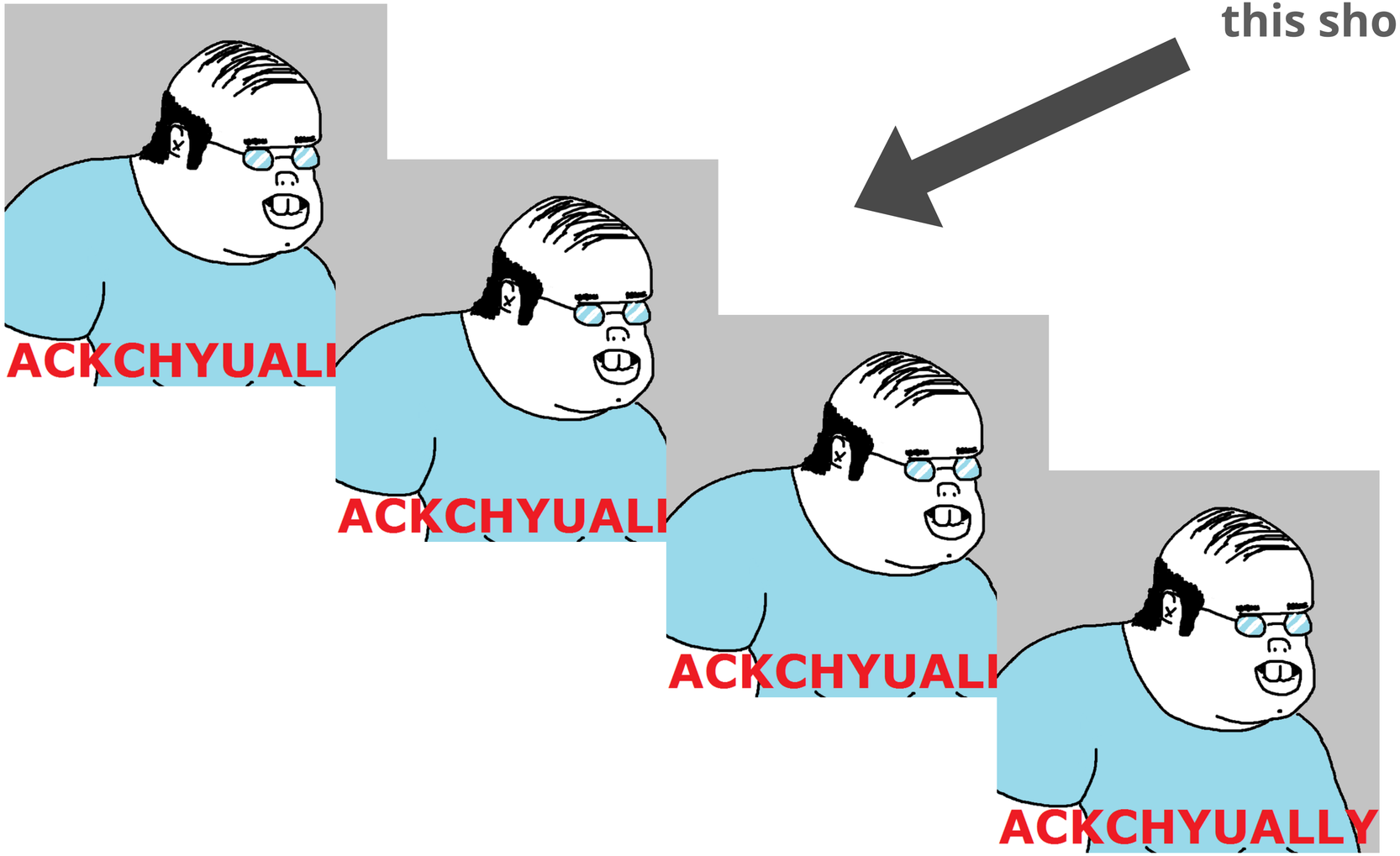
- cost of DBL ⟩ in our case: 4M + 5S
- cost of push ↦ in our case: 4M

Goal: do an isogeny of degree 2^{1000}

Subgoal: do an isogeny of degree 2^f

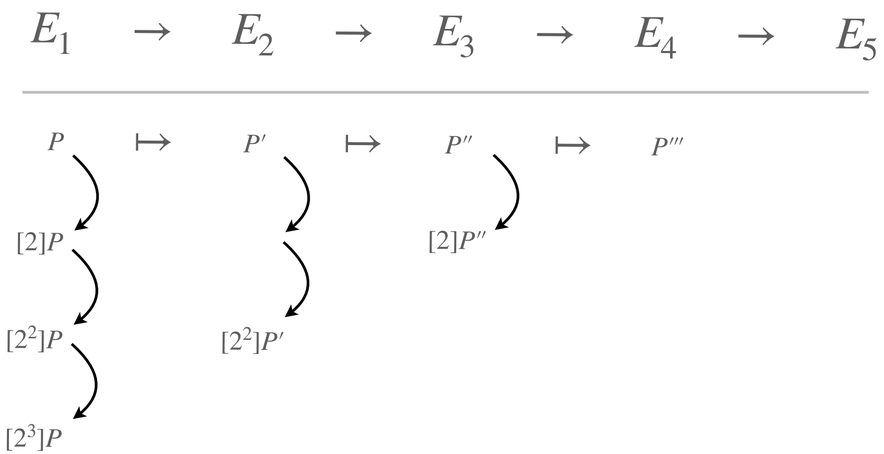
Subgoal: do eight blocks of such isogenies

this should be you right now



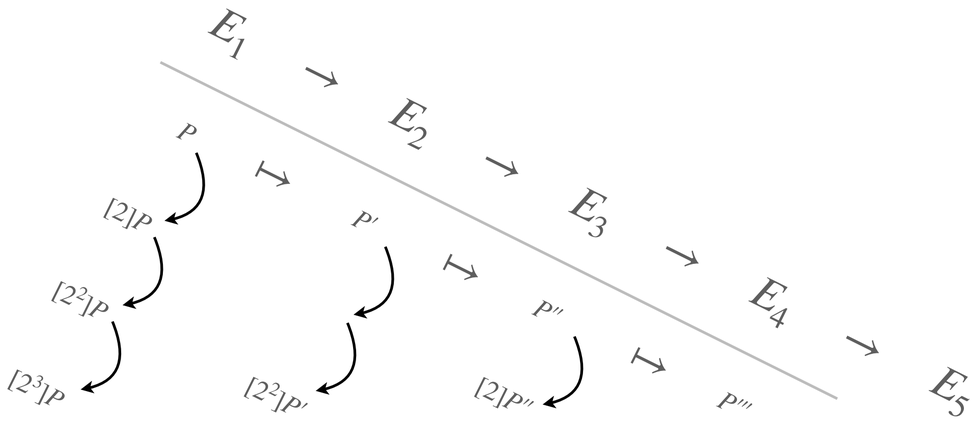
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Can we do “better” strategies?



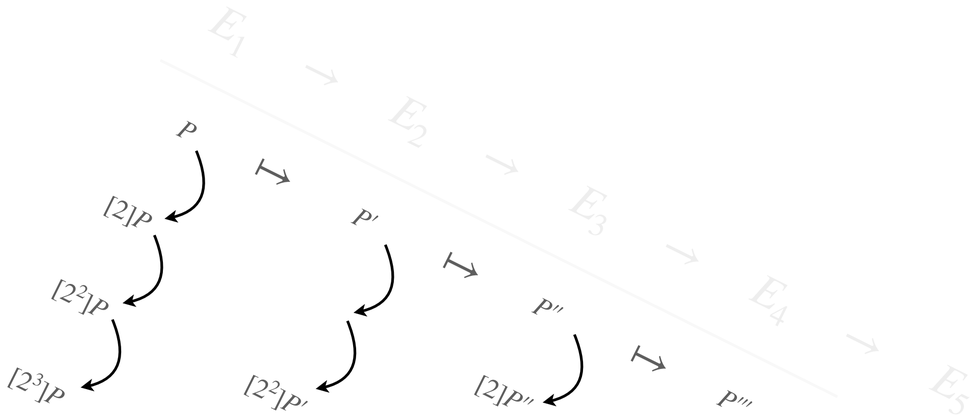
Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

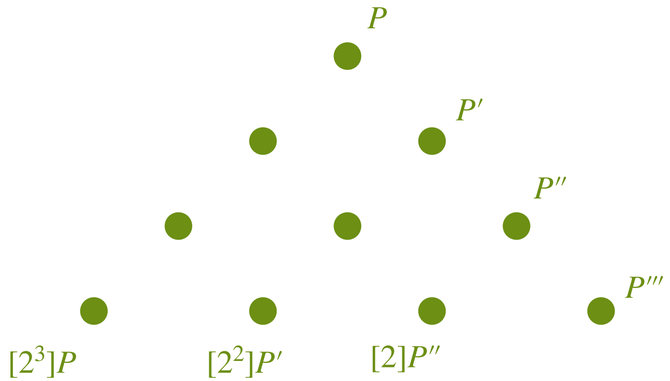
Can we do “better” strategies?



Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

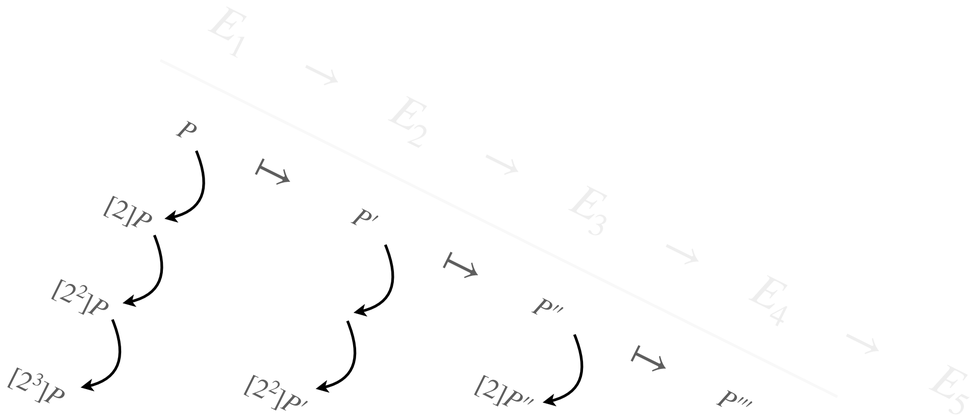
Can we do “better” strategies?

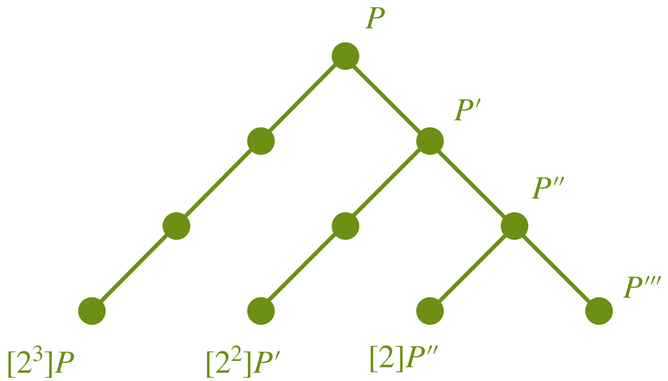




Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Can we do “better” strategies?

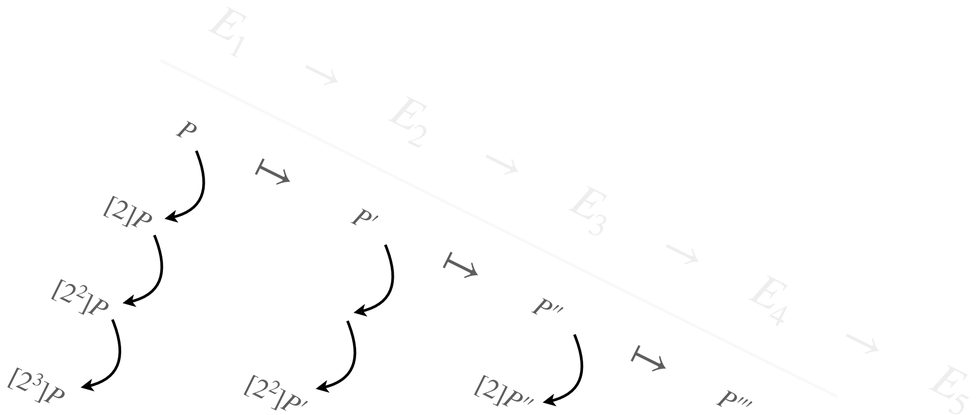


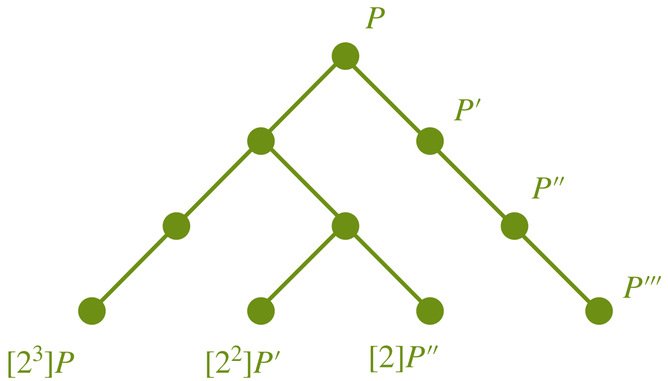


$\mathcal{O}(f^2)$

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

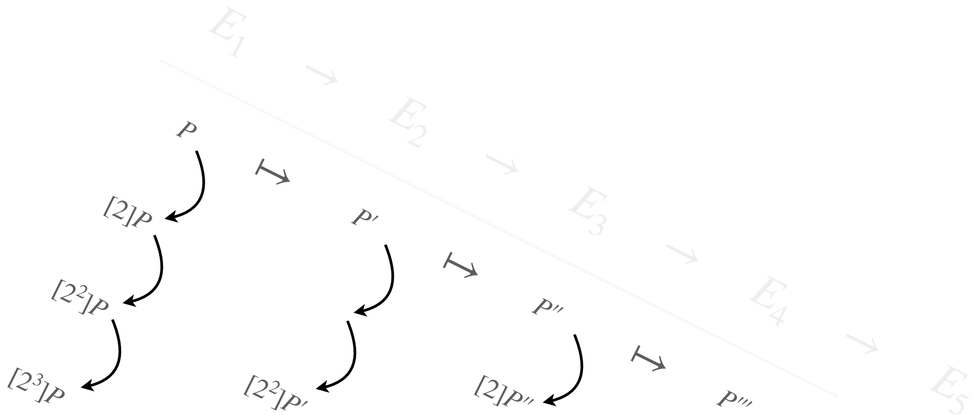
Can we do “better” strategies?

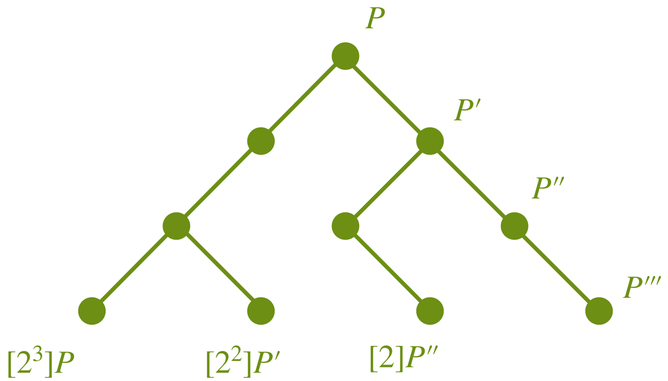




Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

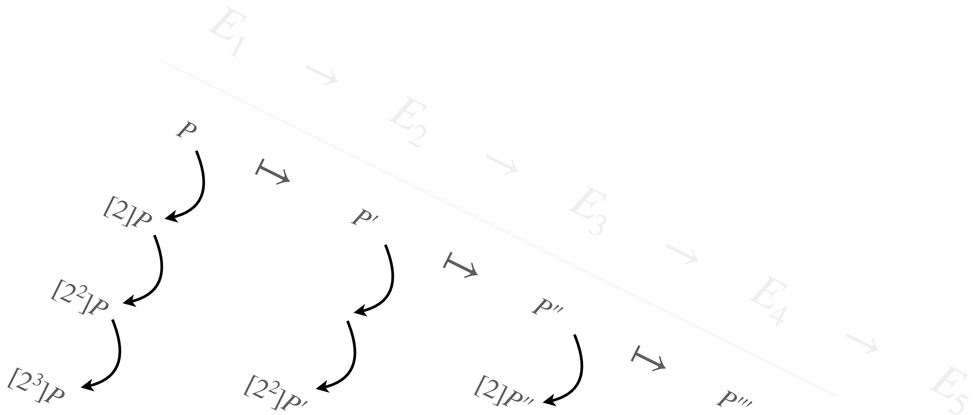
Can we do “better” strategies?

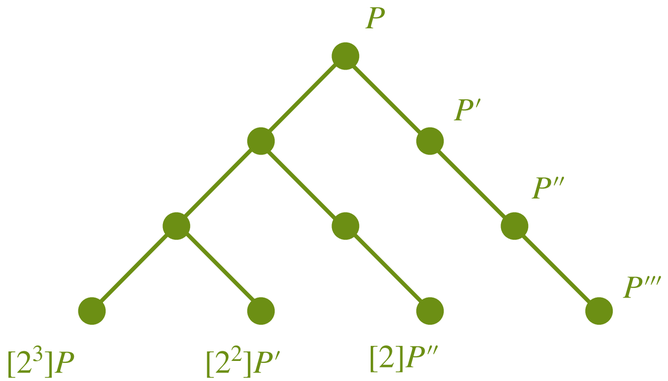




Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

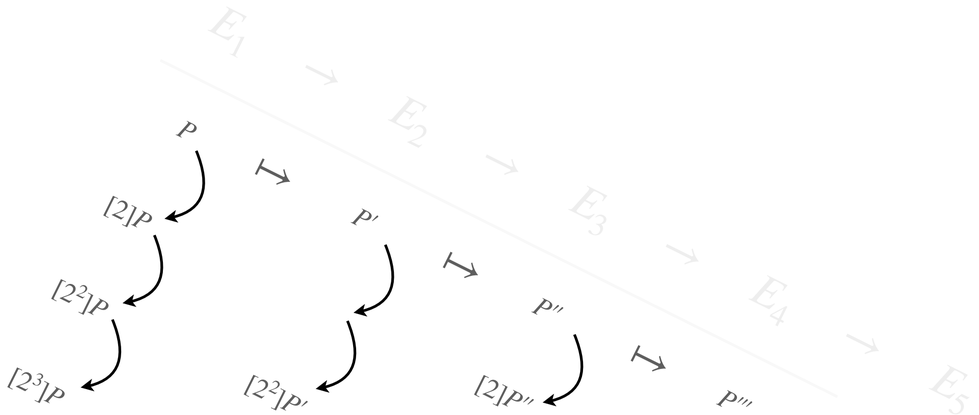
Can we do “better” strategies?

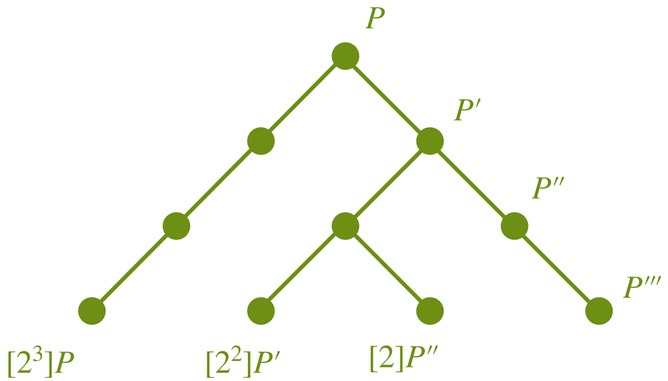




Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Can we do “better” strategies?



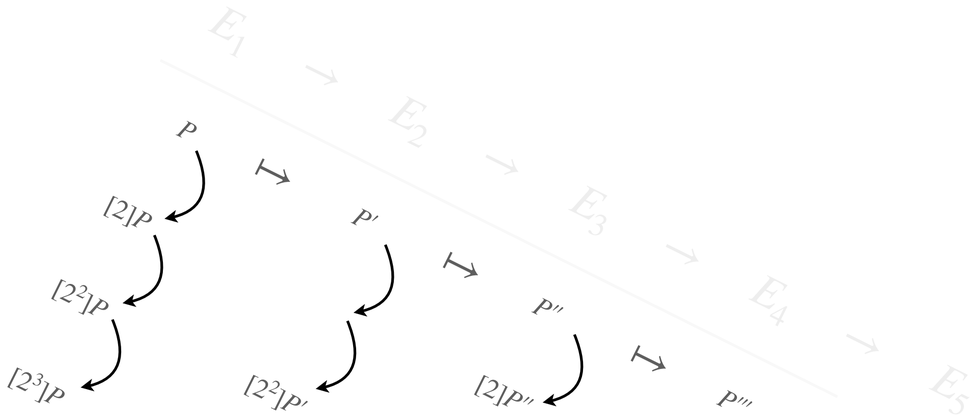


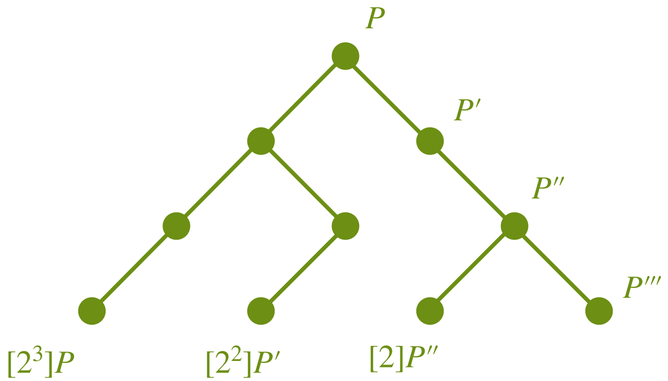
x

Subgoal: do an isogeny of degree 2^f

Subgoal: do eight blocks of such isogenies

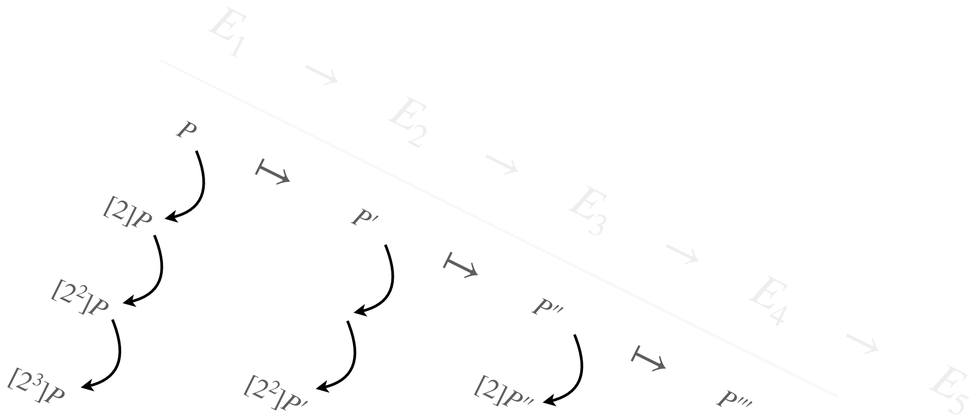
Can we do “better” strategies?

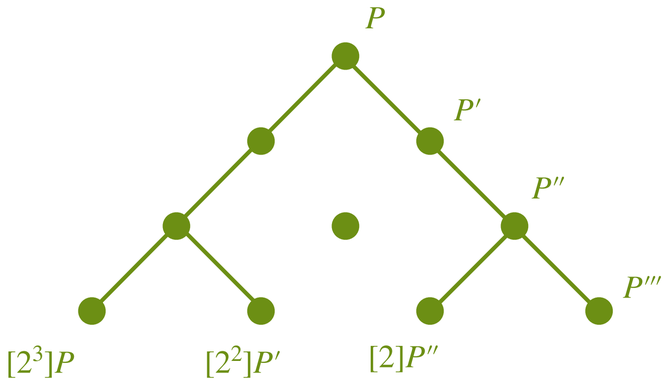




Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Can we do “better” strategies?



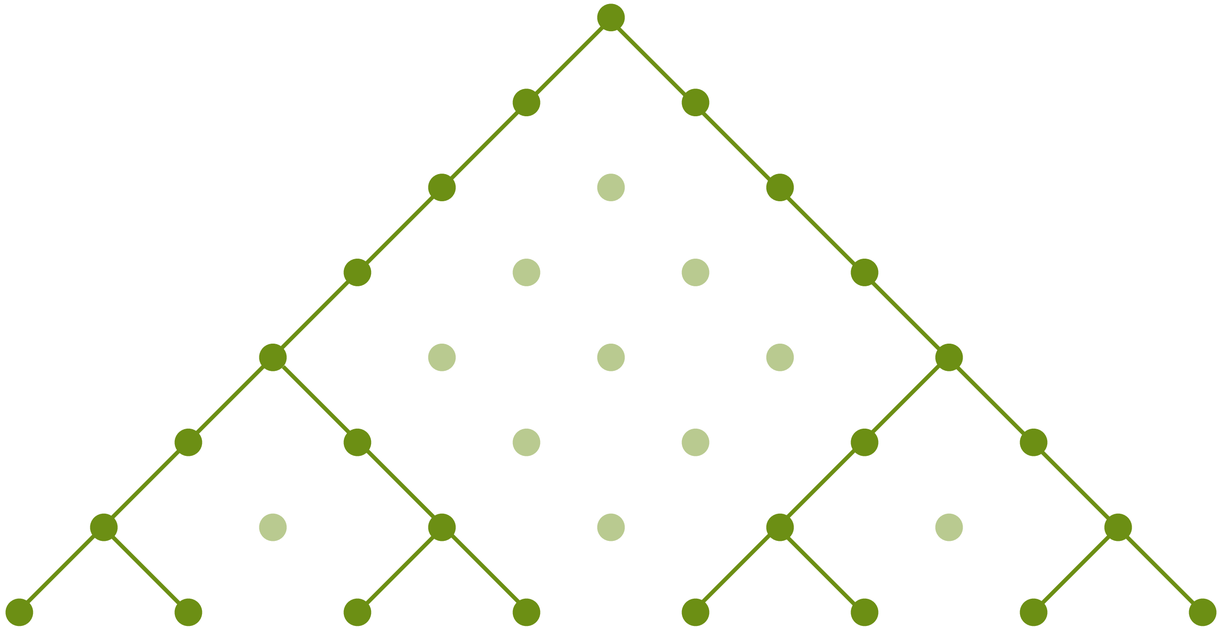


Goal: do an isogeny of degree 2^{1000}

Subgoal: do an isogeny of degree 2^f

Subgoal: do eight blocks of such isogenies

Balanced! 🧘🧘



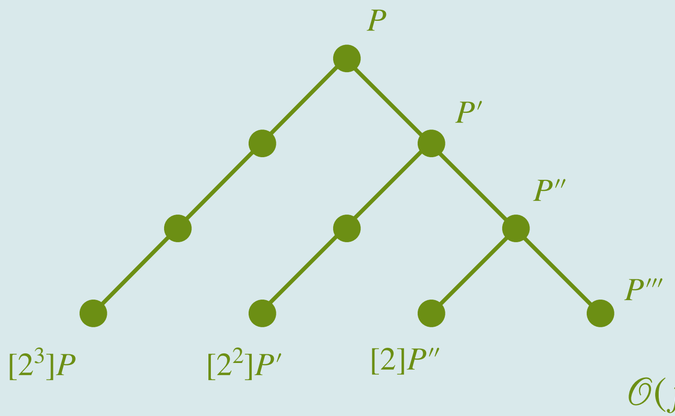
$\mathcal{O}(f \log f)$

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Strategy for your implementation

Strategy 1

Double all the way! Just a few pushes…
Easy & OK when DBL << PUSH



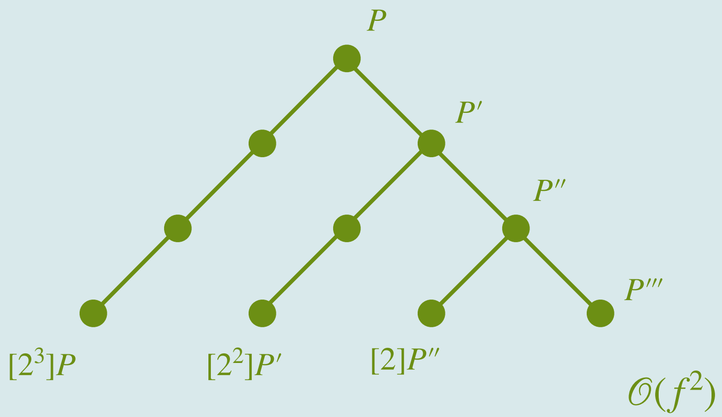
P'''

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Strategy for your implementation

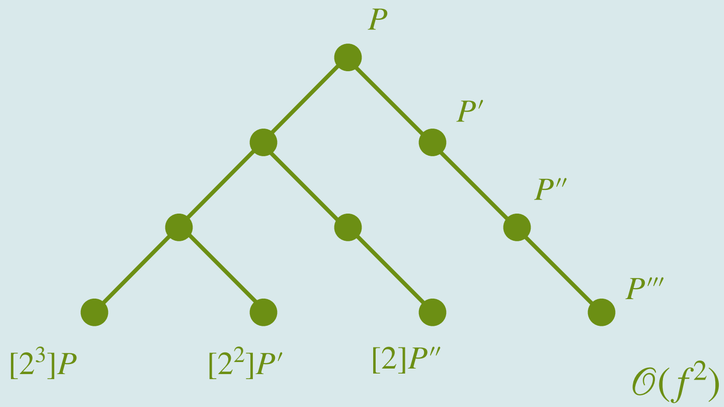
Strategy 1

Double all the way! Just a few pushes…
Easy & OK when DBL << PUSH



Strategy 2

Push push push, we hate doubling…
Easy & OK when PUSH << DBL



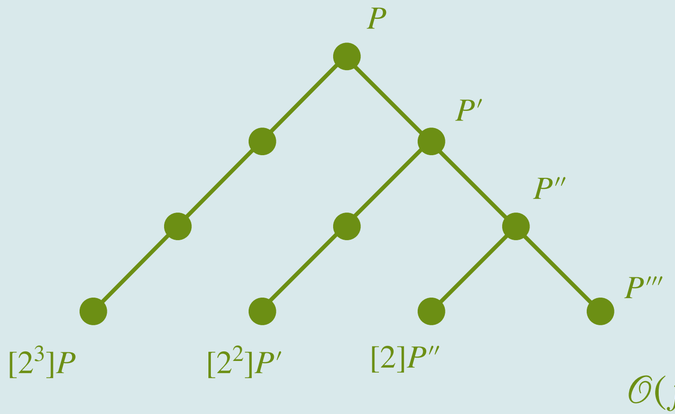
P'''

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Strategy for your implementation

Strategy 1

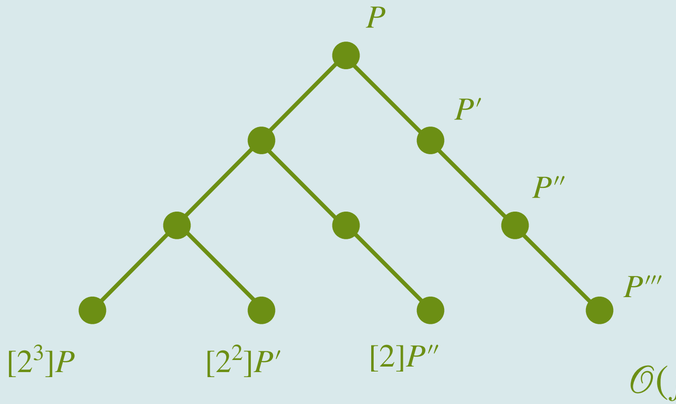
Double all the way! Just a few pushes...
Easy & OK when DBL << PUSH



$\mathcal{O}(f^2)$

Strategy 2

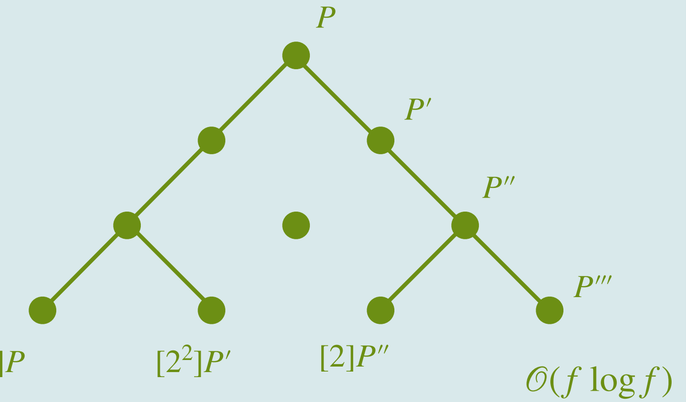
Push push push, we hate doubling...
Easy & OK when PUSH << DBL



$\mathcal{O}(f^2)$

Strategy 3

"Balanced" strategy, in general much better!
Always better than 1 or 2, medium difficulty



$\mathcal{O}(f \log f)$

note: one can compute "optimal" strategies given f, p, and the cost of DBL and PUSH

from 2^{128} to 2^{1000}

Goal: do an isogeny of degree 2^{1000}

Subgoal: do an isogeny of degree 2^f

Subgoal: do eight blocks of such isogenies

$$E_A \xrightarrow{\varphi} E_{A'}$$

$$E_A \xrightarrow{\varphi_1} E^{(1)} \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_7} E^{(7)} \xrightarrow{\varphi_8} E_{A'}$$

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Recipe for a 2^{1000}-isogeny

- start with a nice Montgomery curve E_A
- describe the first block by some point $K_1 \in E_A[2^f]$
- compute $E_A \to E^{(1)}$ as composition of f isogenies of degree 2
- describe the second block by some point $K_2 \in E_1[2^f]$
- compute $E^{(1)} \to E^{(2)}$ as composition of f isogenies of degree 2
- ....
- ....
- ....
- compute $E^{(7)} \to E_{A'}$ as composition of f isogenies of degree 2
- TADAA!

Goal: do an isogeny of degree 2^{1000} ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies

Recipe for a 2^{1000}-isogeny

- start with a nice Montgomery curve E_A
- describe the first block by some point $K_1 \in E_A[2^f]$
- compute $E_A \to E^{(1)}$ as composition of f isogenies of degree 2
- describe the second block by some point $K_2 \in E_1[2^f]$
- compute $E^{(1)} \to E^{(2)}$ as composition of f isogenies of degree 2
- ....
- ....
- ....
- compute $E^{(7)} \to E_{A'}$ as composition of f isogenies of degree 2
- TADAA!

▶

Ingredients for a 2^{1000}-isogeny

- the Montgomery coefficient $A \in \mathbb{F}_{p^2}$ of E_A
- the kernel points $K_1, K_2, \ldots, K_7$
- but really only the x-coordinate of these K_i
- so $x_{K_i} \in \mathbb{F}_{p^2}$

Goal: do an isogeny of degree 2^{1000}

Subgoal: do an isogeny of degree 2^f

Subgoal: do eight blocks of such isogenies

Recipe for a 2^{1000}-isogeny

- start with a nice Montgomery curve E_A
- describe the first block by some point $K_1 \in E_A[2^f]$
- compute $E_A \to E^{(1)}$ as composition of f isogenies of degree 2
- describe the second block by some point $K_2 \in E_1[2^f]$
- compute $E^{(1)} \to E^{(2)}$ as composition of f isogenies of degree 2
- ....
- ....
- ....
- compute $E^{(7)} \to E_{A'}$ as composition of f isogenies of degree 2
- TADAA!

Ingredients for a 2^{1000}-isogeny

- the Montgomery coefficient $A \in \mathbb{F}_{p^2}$ of E_A
- the kernel points $K_1, K_2, \ldots, K_7$
- but really only the x-coordinate of these K_i
- so $x_{K_i} \in \mathbb{F}_{p^2}$

Uncompressed SQIsign response isogeny!

$$A, x_{K_1}, x_{K_2}, \ldots, x_{K_7}$$

Goal: do an isogeny of degree 2^{1000}

Subgoal: do an isogeny of degree 2^f

Subgoal: do eight blocks of such isogenies

Recipe for a 2^{1000}-isogeny

- start with a nice Montgomery curve E_A
- describe the first block by some point $K_1 \in E_A[2^f]$
- compute $E_A \to E^{(1)}$ as composition of f isogenies of degree 2
- describe the second block by some point $K_2 \in E_1[2^f]$
- compute $E^{(1)} \to E^{(2)}$ as composition of f isogenies of degree 2
- ....
- ....
- ....
- compute $E^{(7)} \to E_{A'}$ as composition of f isogenies of degree 2
- TADAA!

Ingredients for a 2^{1000}-isogeny

- the Montgomery coefficient $A \in \mathbb{F}_{p^2}$ of E_A
- the kernel points $K_1, K_2, \ldots, K_7$
- but really only the x-coordinate of these K_i
- so $x_{K_i} \in \mathbb{F}_{p^2}$

Uncompressed SQIsign response isogeny!

$$A, x_{K_1}, x_{K_2}, \ldots, x_{K_7}$$

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

$2 \log p$ bits ≈ 64 bytes

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ ▶ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

$2 \log p$ bits ≈ 64 bytes

▶

f bits ≈ 16 bytes

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

1

we have $K \in E[2^f]$
given by
$x_K = a + bi \in \mathbb{F}_q$

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

1

we have $K \in E[2^f]$
given by
$x_K = a + bi \in \mathbb{F}_q$

▶

2

FACT:
we have
$E[2^f] \cong \mathbb{Z}/f \times \mathbb{Z}/f$

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

1

we have $K \in E[2^f]$
given by
$x_K = a + bi \in \mathbb{F}_q$

▶

2

FACT:
we have
$E[2^f] \cong \mathbb{Z}/f \times \mathbb{Z}/f$

▶

3

Corollary
we can find basis
P, Q for $E[2^f]$

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

1

we have $K \in E[2^f]$
given by
$x_K = a + bi \in \mathbb{F}_q$

2

FACT:
we have
$E[2^f] \cong \mathbb{Z}/f \times \mathbb{Z}/f$

3

Corollary
we can find basis
P, Q for $E[2^f]$

4

Compression
write $K = P + sQ$
for some $s \in [0..2^f]$

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

3

Corollary
we can find basis
P, Q for $E[2^f]$

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

3

Corollary
we can find basis
P, Q for $E[2^f]$

Potential problem!
If I find different basis P, Q,
I get different point $K = P + sQ$

How to compress an isogeny

3

Corollary
we can find basis P, Q for $E[2^f]$

Potential problem!
If I find different basis P, Q,
I get different point $K = P + sQ$

deterministic basis

How do ensure everyone finds the same basis P, Q for a given E?

1. check $x = 1 + i,\ 1 + 2 \cdot i,\ 1 + 3 \cdot i,\ \ldots$ until $P = (x, -)$ is on the curve E
2. set $P \leftarrow \left[\frac{p+1}{2^f}\right] P$ and then check if $P_2 := [2^{f-1}]P \neq \mathcal{O}$, else back to 1
3. continue with increasing x until $Q = (x, -)$ is on the curve E
4. set $Q \leftarrow \left[\frac{p+1}{2^f}\right] Q$ and then check if $Q_2 := [2^{f-1}]Q \neq \mathcal{O}$, else back to 3
5. check if $P_2 \neq Q_2$ to ensure its a basis, else back to 3
6. return P and Q

How to compress an isogeny

(with a little bit of magic)

4

Compression

write $K = P + sQ$

for some $s \in [0..2^f]$

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

(with a little bit of magic)

4

Compression
write $K = P + sQ$
for some $s \in [0..2^f]$

For technical reasons, we sometimes need to swap around these point P, Q.

Therefore, in (y)our implementation, we provide an additional bit `swap` that tells you wether or not you need to swap P and Q.

You can then use a magic function `get_kernel_point(P, Q, s)` to get this K.

How to compress an isogeny

(with a little bit of magic)

4

Compression
write $K = P + sQ$
for some $s \in [0..2^f]$

For technical reasons, we sometimes need to swap around these point P, Q.

Therefore, in (y)our implementation, we provide an additional bit `swap` that tells you wether or not you need to swap P and Q.

You can then use a magic function `get_kernel_point(P, Q, s)` to get this K.

if you are a real nerd, you can check what's in this magic function and try to understand Kummer arithmetic more deeply

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

✓

Uncompressed long isogeny

$$A, x_{K_1}, x_{K_2}, \ldots, x_{K_7}$$

- easy!
- fast!
- big-ish

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

✓ **Uncompressed long isogeny**

$$A, x_{K_1}, x_{K_2}, \ldots, x_{K_7}$$

- easy!
- fast!
- big-ish

▶

Compression (only by signer)

$$x_{K_i} \to s_i$$

1. for each K_i on $E^{(i)}$
2. finds basis P, Q for $E[2^f]$
3. writes $K_i = P + s_i Q$
4. replaces x_{K_i} by s_i

Goal: do an isogeny of degree 2^{1000} ✓ ▶ Subgoal: do an isogeny of degree 2^f ✓ Subgoal: do eight blocks of such isogenies ✓

How to compress an isogeny

✓

Uncompressed long isogeny

$$A, x_{K_1}, x_{K_2}, \ldots, x_{K_7}$$

- easy!
- fast!
- big-ish

▶

Compression (only by signer)

$$x_{K_i} \to s_i$$

1. for each K_i on $E^{(i)}$
2. finds basis P, Q for $E[2^f]$
3. writes $K_i = P + s_i Q$
4. replaces x_{K_i} by s_i

▶

✓

Compressed long isogeny!

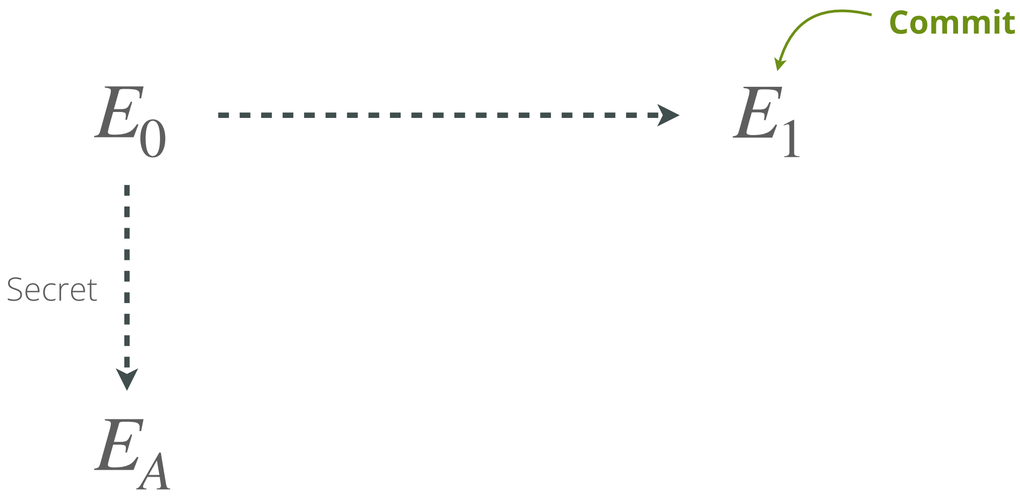
$$A, s_1, s_2, \ldots, s_7$$

- bit more thinking
- bit more computing
- very very small

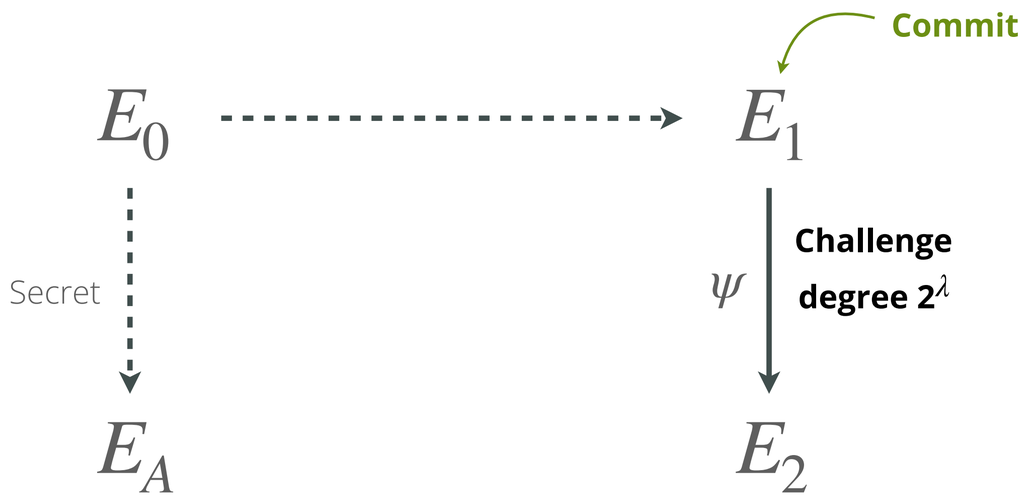
from 2^{1000} to SQIsign verification

Recall: How does SQIsign work

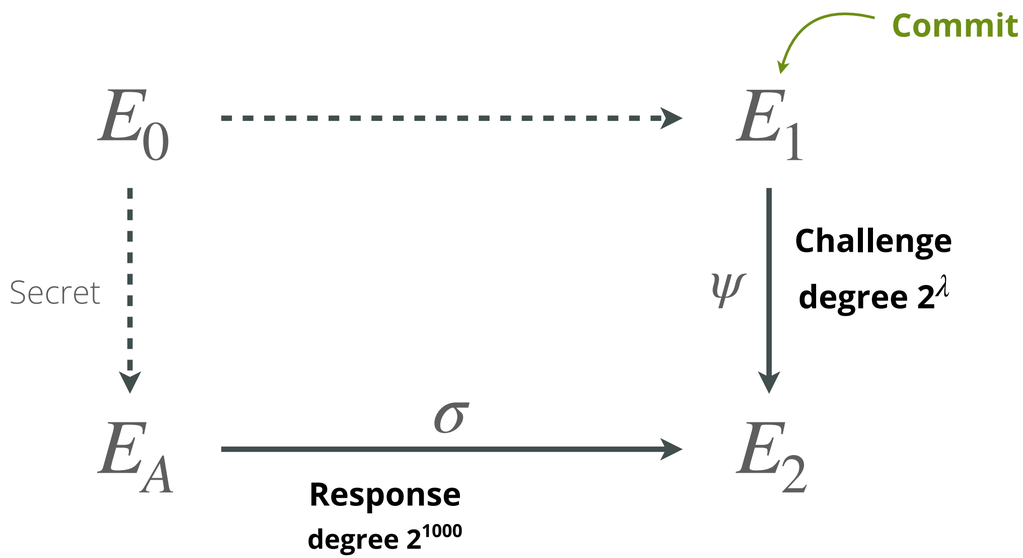
Recall: How does SQIsign work



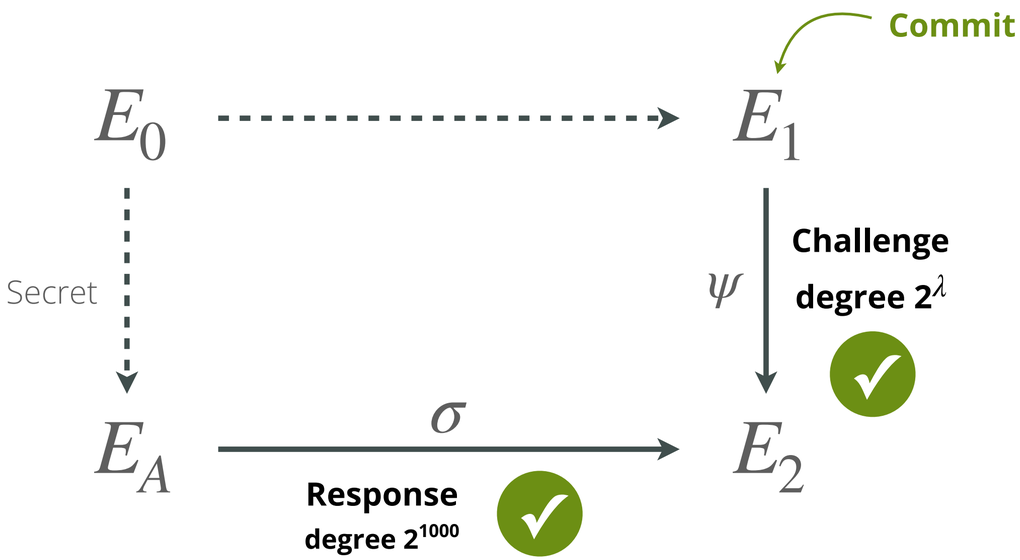
Recall: How does SQIsign work



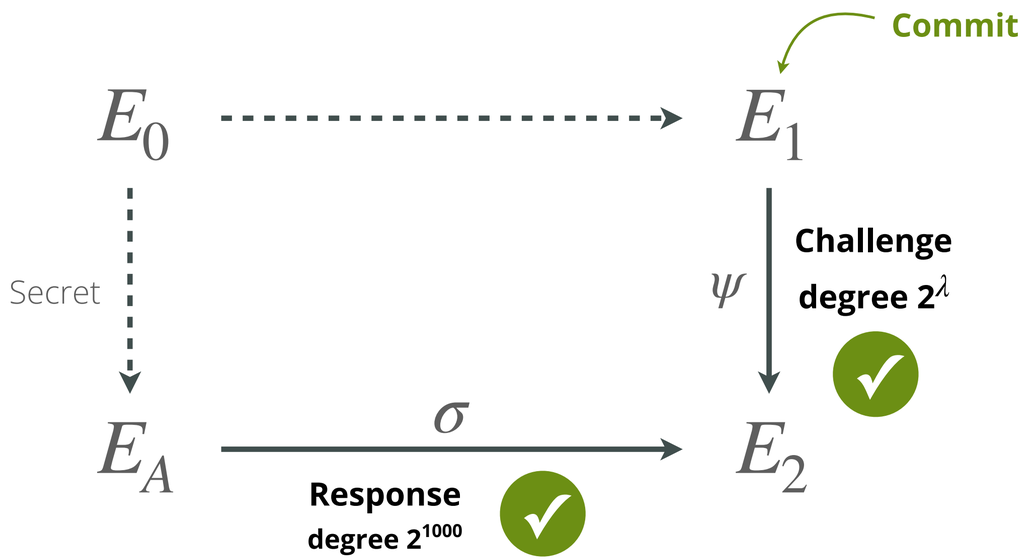
Recall: How does SQIsign work



Recall: How does SQIsign work



Recall: How does SQIsign work



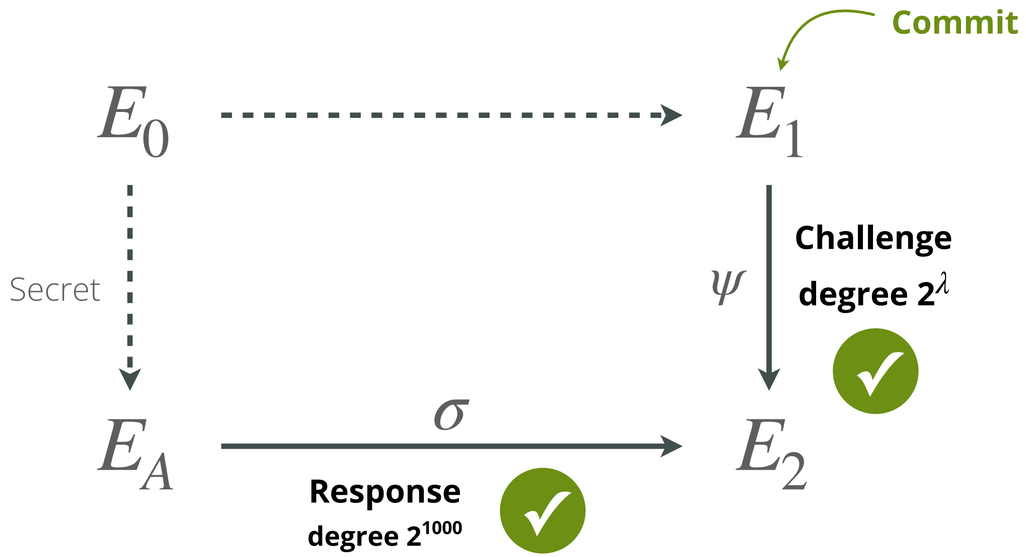
before Fiat-Shamir

1. we essentially want a **"random" isogeny** ψ of degree 2^λ

2. this is given by a **"random" point** K of order 2^λ

3. find basis P, Q for $E_1[2^\lambda]$, set $K = P + sQ$ for **random** $s \xleftarrow{\$} [1..2^\lambda]$

Recall: How does SQIsign work



before Fiat-Shamir

1. we essentially want a **"random" isogeny** ψ of degree 2^λ

2. this is given by a **"random" point** K of order 2^λ

3. find basis P, Q for $E_1[2^\lambda]$, set $K = P + sQ$ for **random** $s \xleftarrow{\$} [1..2^\lambda]$

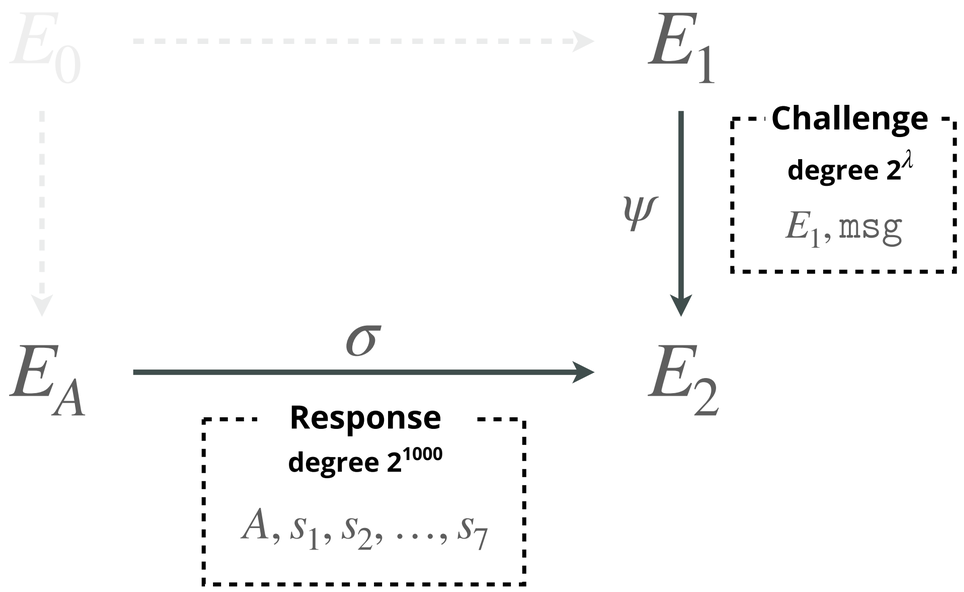
after Fiat-Shamir

1. we **hash** the message $\texttt{msg} \mapsto s \in [1..2^\lambda]$

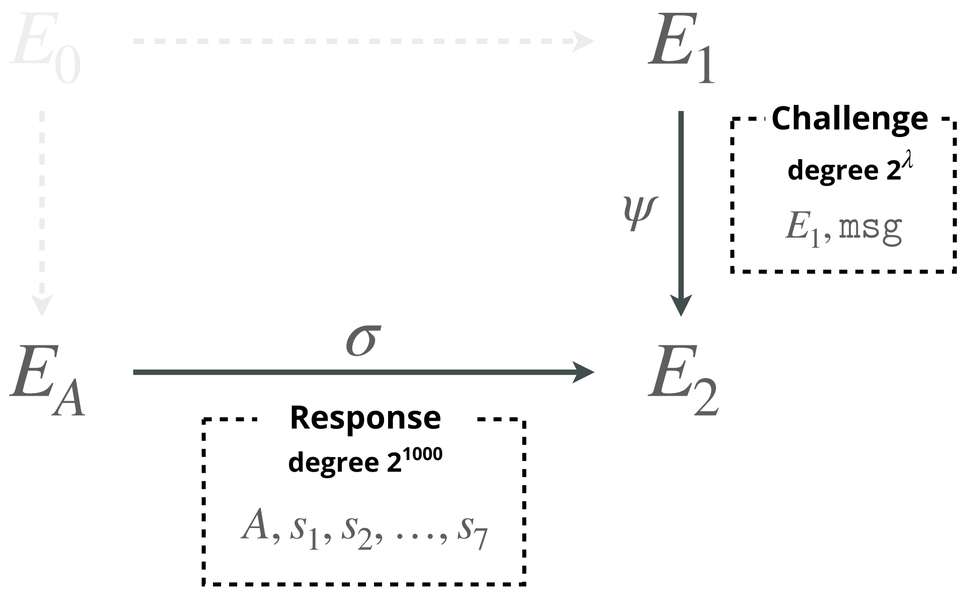
2. we set $K = P + sQ$ to get a **"hashed" point** of order 2^λ

3. we get a **"hashed" isogeny** ψ of order 2^λ from kernel K

Recall: How does SQIsign work



Recall: How does SQIsign work



SQIsign verification

Assume we have a public key E_A and a message $\mathtt{msg}$.
The signature σ is given by $(s_1, s_2, \ldots, s_7, E_1)$.
To verify σ

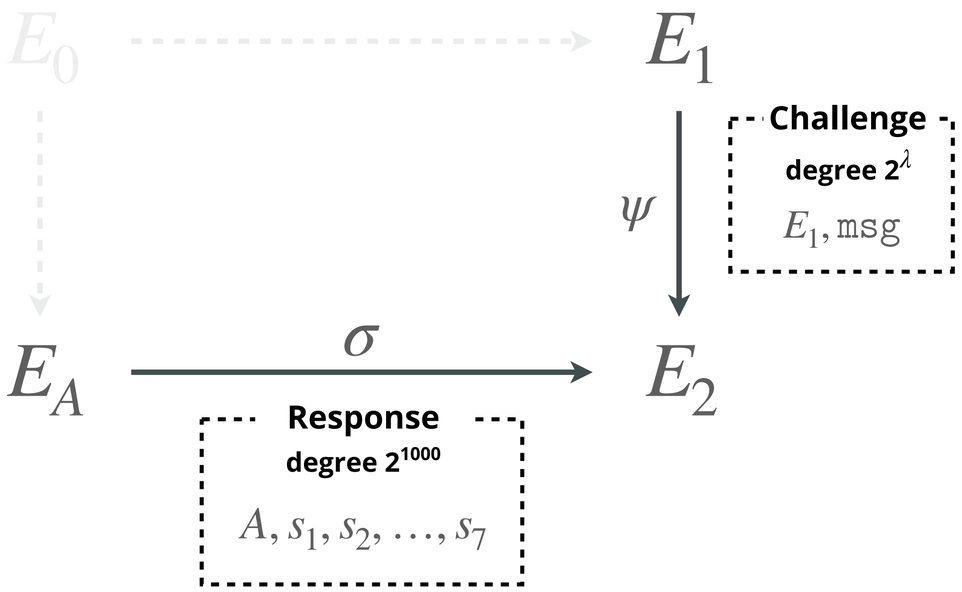
Repeat Challenge

1. On E_1 get basis P, Q for $E_1[2^\lambda]$
2. Hash $\mathtt{msg}$ to some value $s \in [1..2^\lambda]$
3. Compute $K = P + sQ$ and the isogeny $\psi : E_1 \to E_2$

Verify Response

1. On E_A get basis P, Q for $E_A[2^f]$
2. Compute $K_1 = P + s_1 Q$ and $\varphi_1 : E_A \to E^{(1)}$
3. Repeat for all other $s_2, \ldots, s_7$
4. This gives $\sigma = \varphi_7 \circ \varphi_6 \circ \ldots \circ \varphi_1$ by $E_A \to E_2$
5. Verify this is the same as in **challenge**

Recall: How does SQIsign work



SQIsign verification

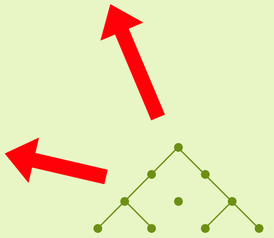
Assume we have a public key E_A and a message `msg`.
The signature σ is given by $(s_1, s_2, \ldots, s_7, E_1)$.
To verify σ

Repeat Challenge

1. On E_1 get basis P, Q for $E_1[2^\lambda]$
2. Hash `msg` to some value $s \in [1..2^\lambda]$
3. Compute $K = P + sQ$ and the isogeny $\psi : E_1 \to E_2$

Verify Response

1. On E_A get basis P, Q for $E_A[2^f]$
2. Compute $K_1 = P + s_1 Q$ and $\varphi_1 : E_A \to E^{(1)}$
3. Repeat for all other $s_2, \ldots, s_7$
4. This gives $\sigma = \varphi_7 \circ \varphi_6 \circ \ldots \circ \varphi_1$ by $E_A \to E_2$
5. Verify this is the same as in **challenge**



Your work in block 4

1. Compute 2^f-isogeny using “**naive**” strategy (either strat. 1 or 2)

2. Verify **uncompressed** SQIsign signature using **naive** strategy

Your work in block 4