Supersingular Isogeny Key Encapsulation (SIKE)

Reza Azarderakhsh Matthew Campagna Craig Costello
Luca De Feo Basil Hess David Jao Brian Koziel
Brian LaMacchia Patrick Longa Michael Naehrig
Joost Renes Vladimir Soukharev

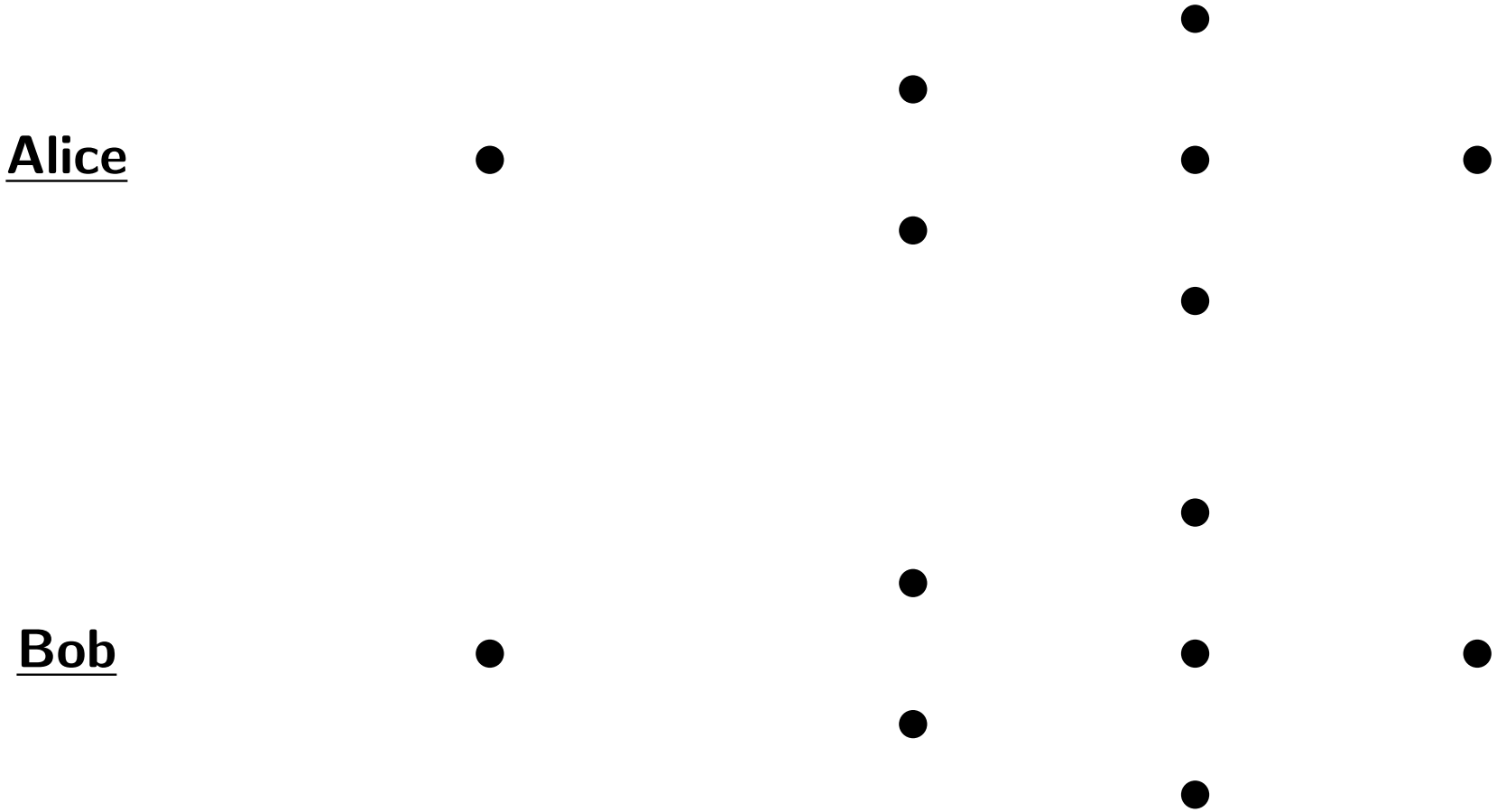
Digital Security Group, Radboud University, Nijmegen

1 February 2018

Introduction

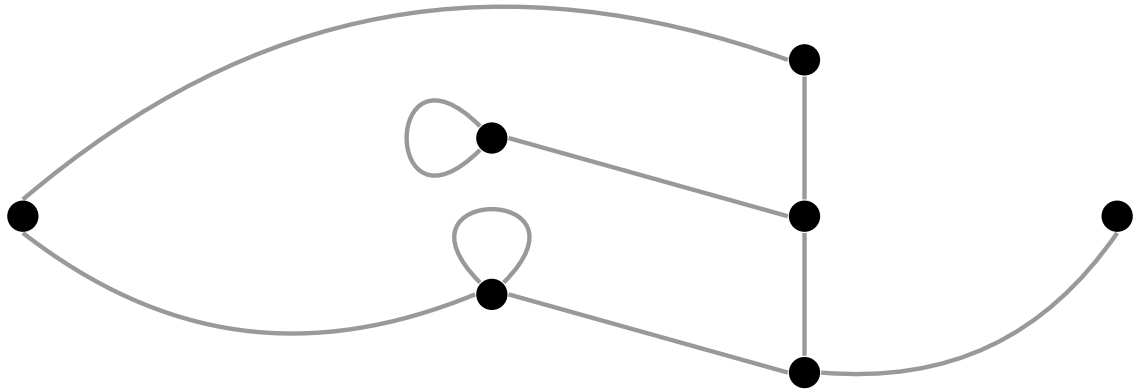
(generic intro...)

A graph-based protocol

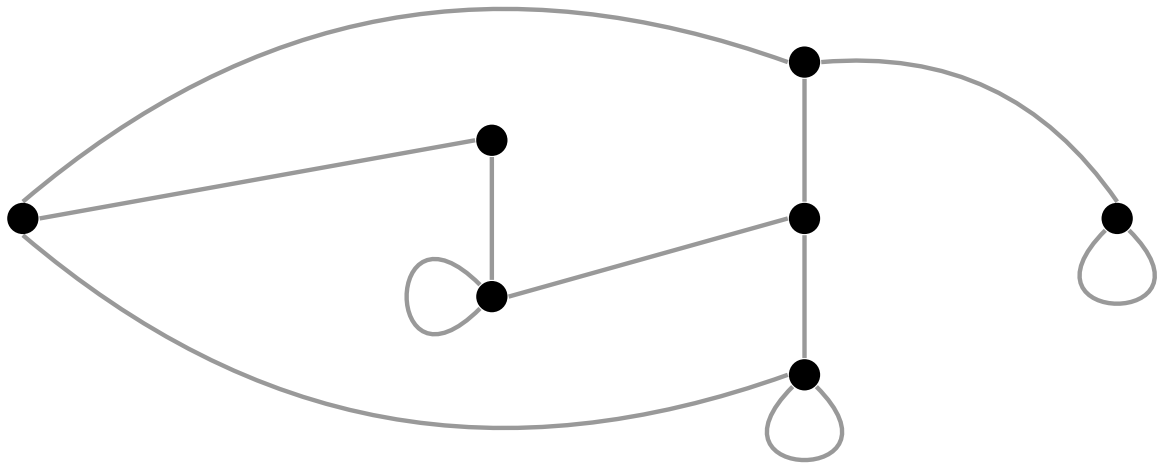


A graph-based protocol

Alice

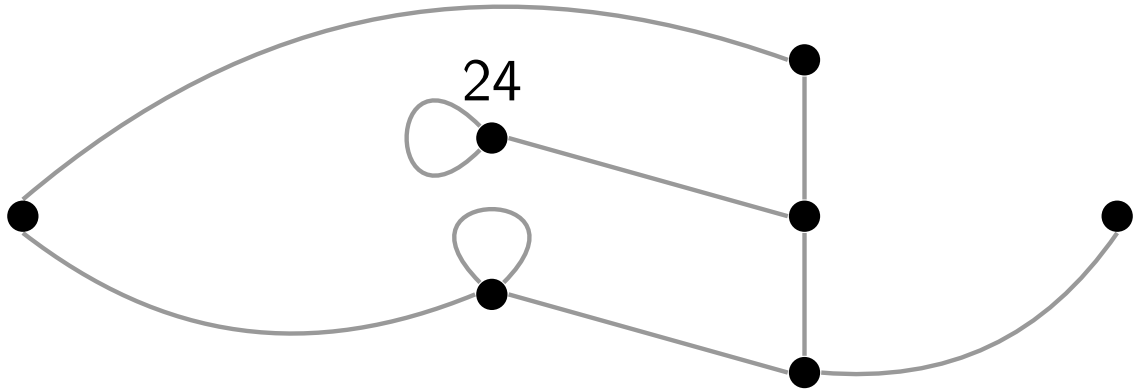


Bob

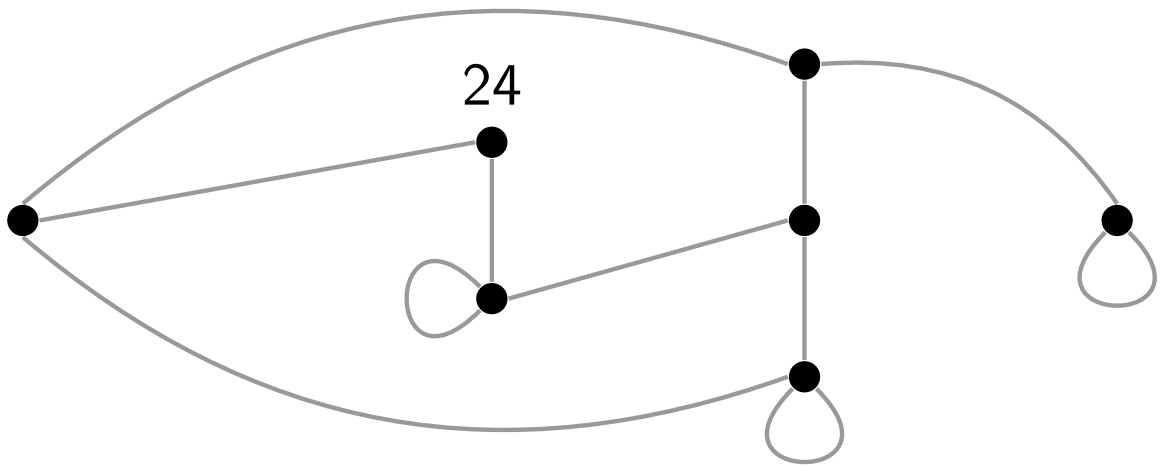


A graph-based protocol

Alice

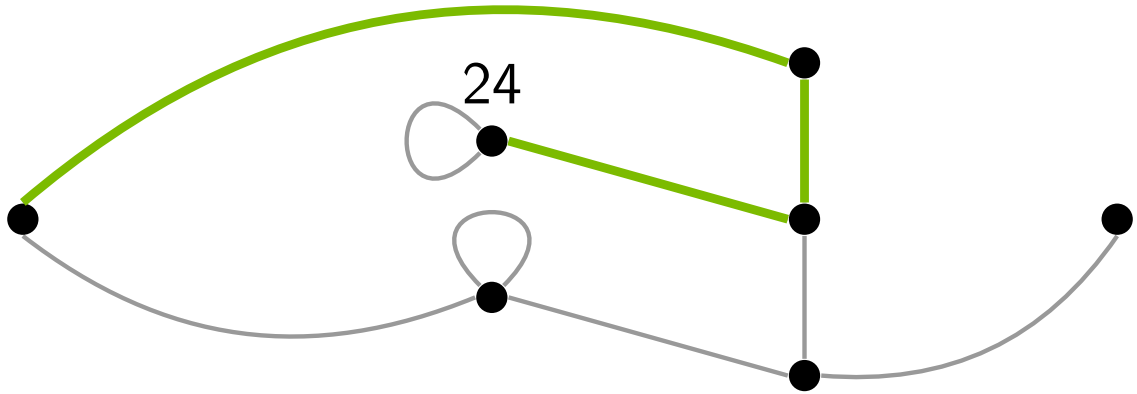


Bob

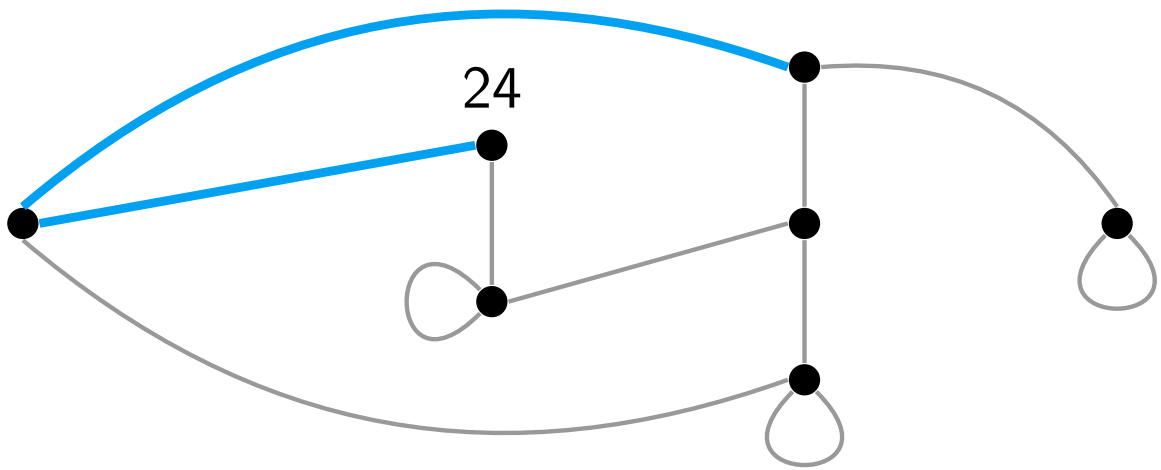


A graph-based protocol

Alice

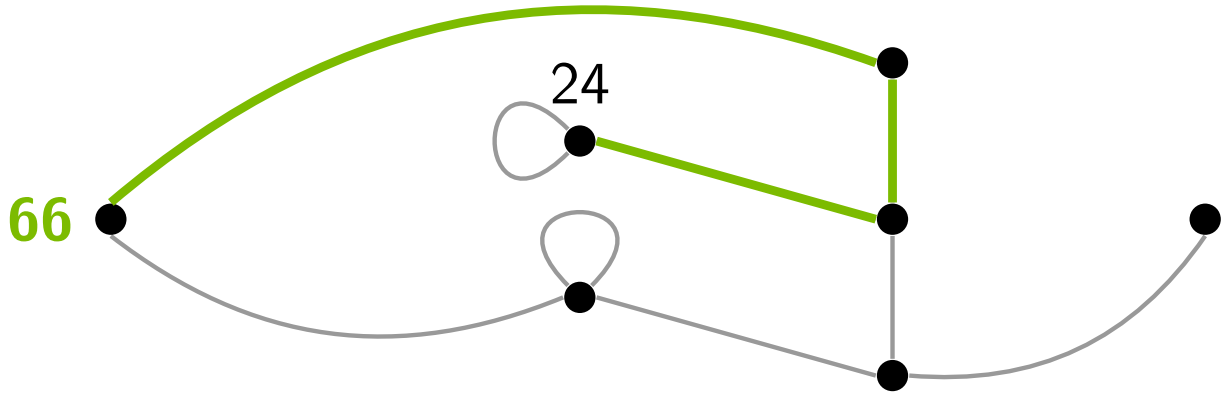


Bob

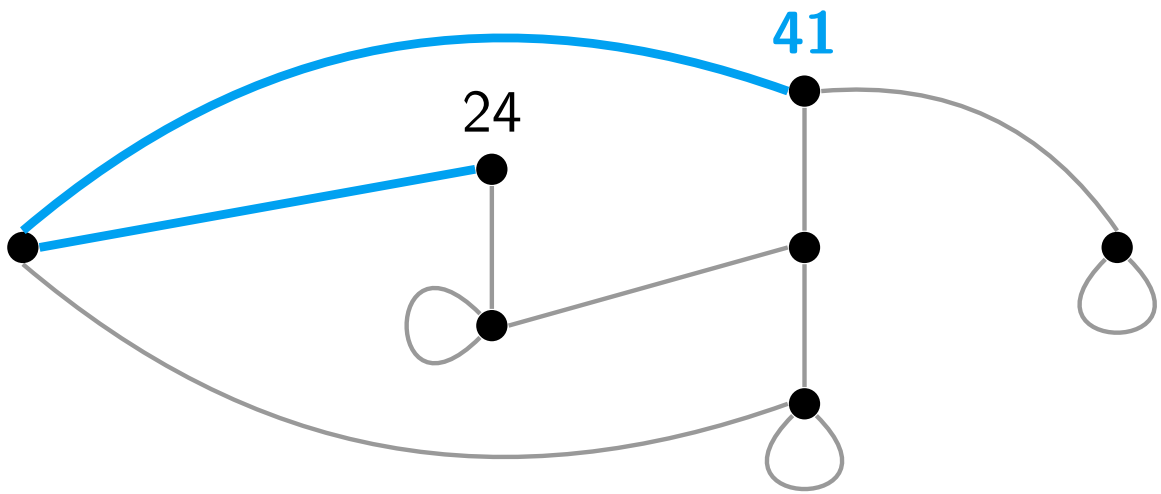


A graph-based protocol

Alice

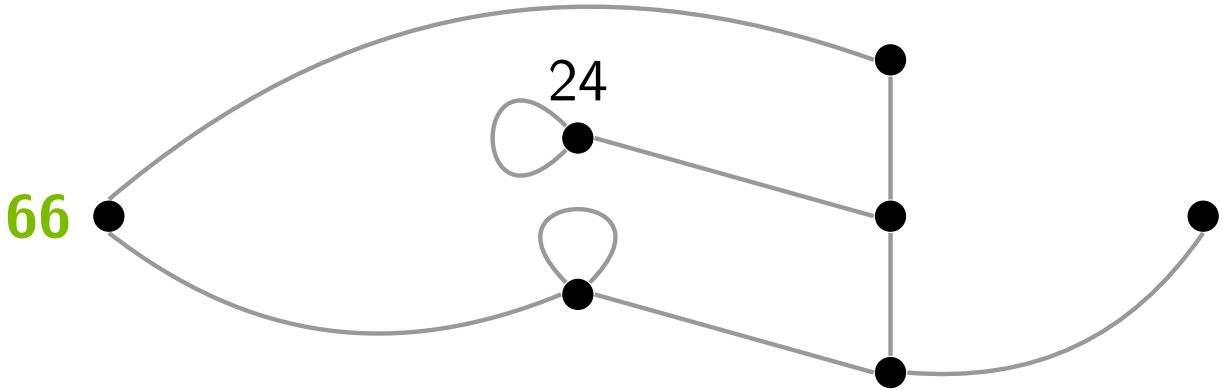


Bob

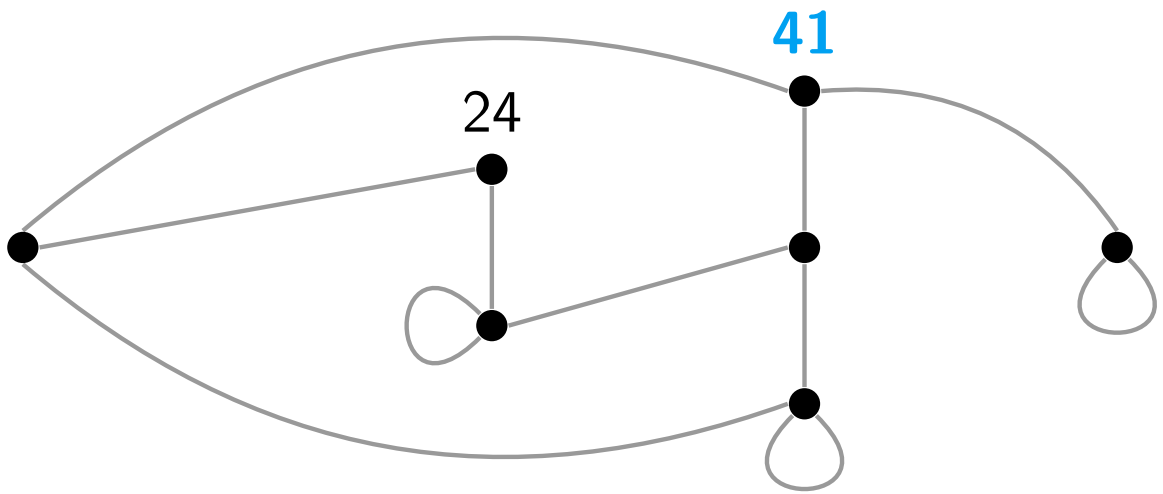


A graph-based protocol

Alice

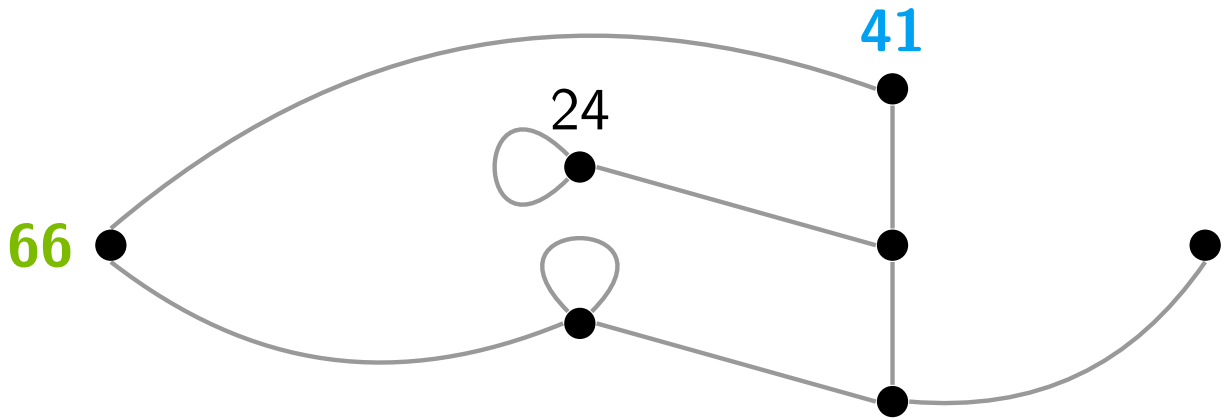


Bob

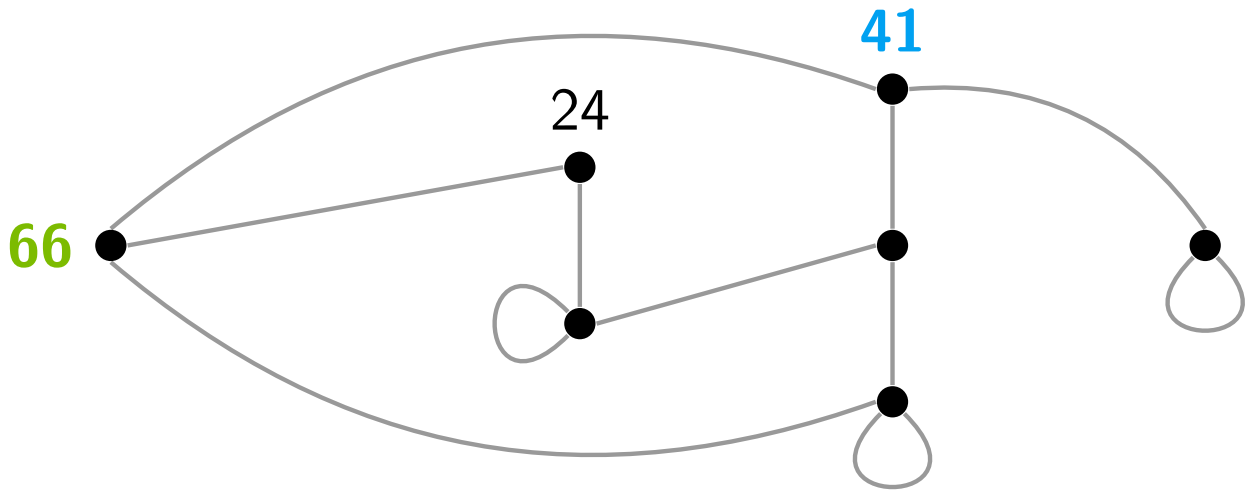


A graph-based protocol

Alice

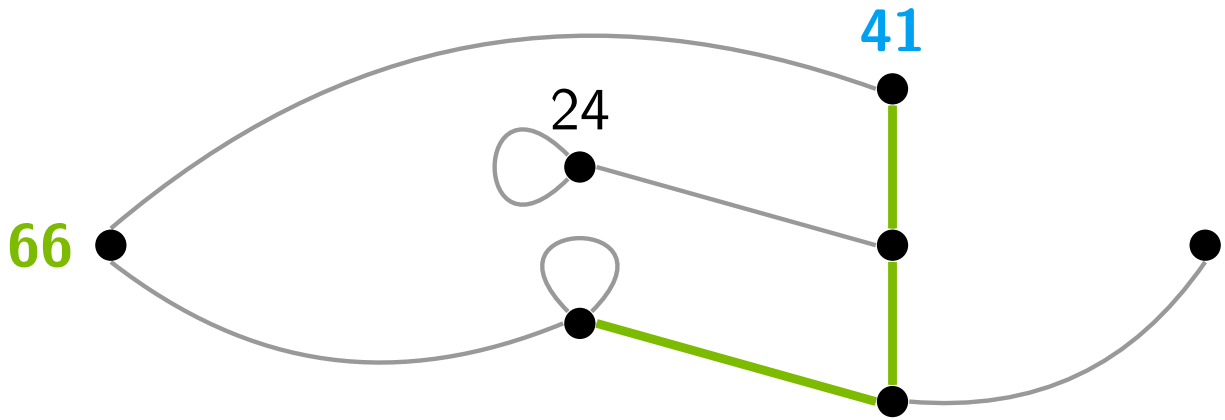


Bob

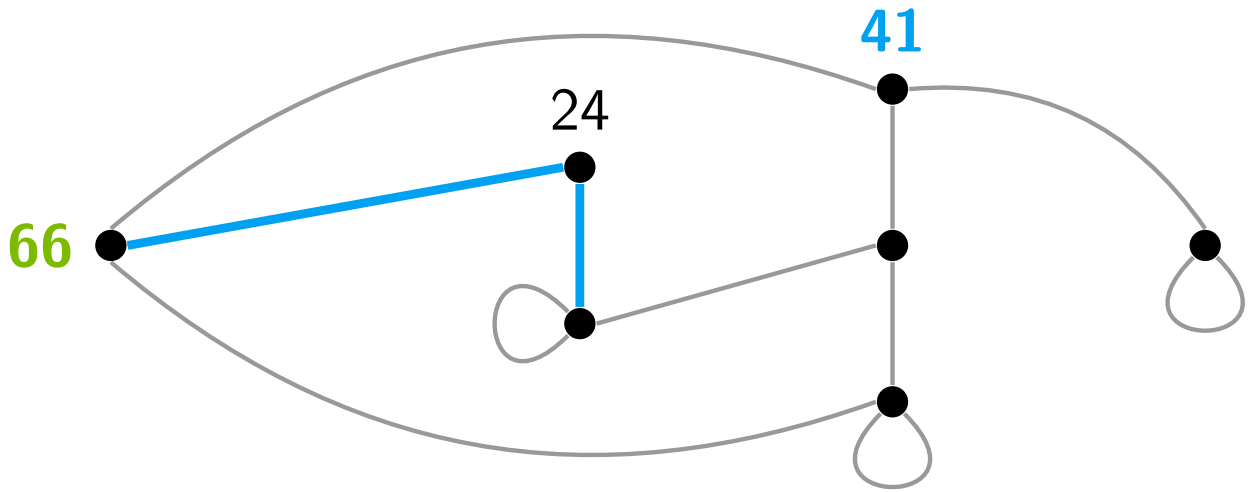


A graph-based protocol

Alice

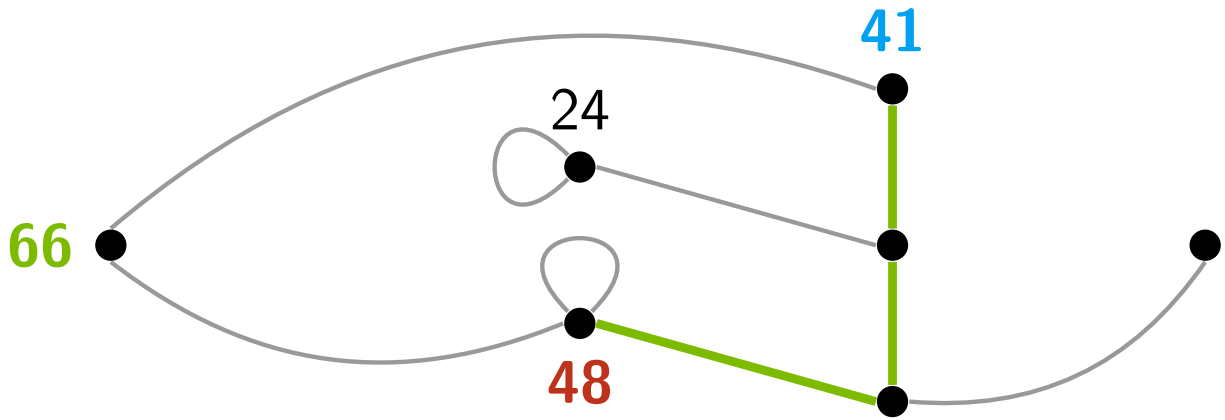


Bob

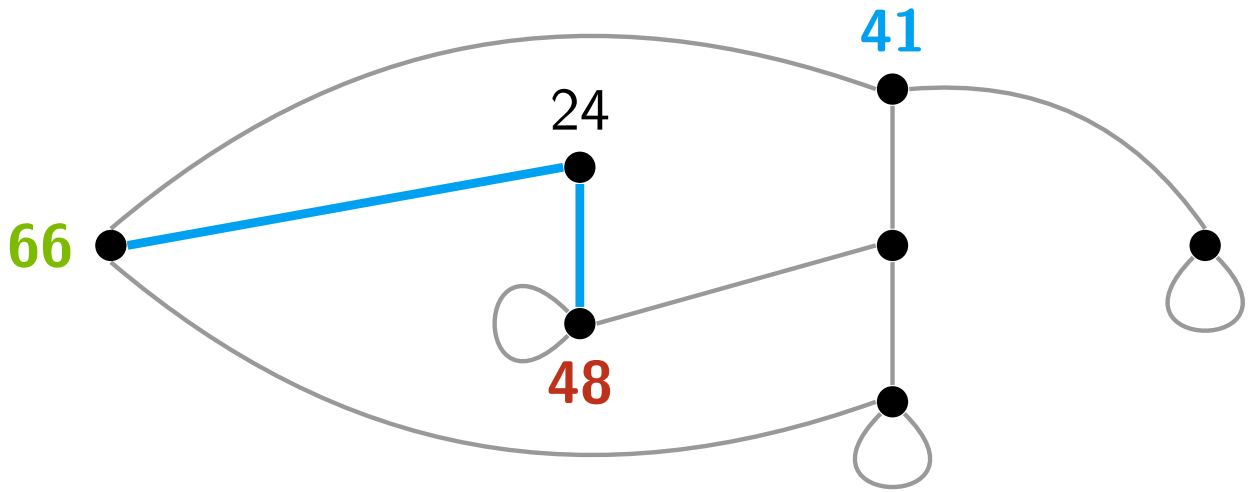


A graph-based protocol

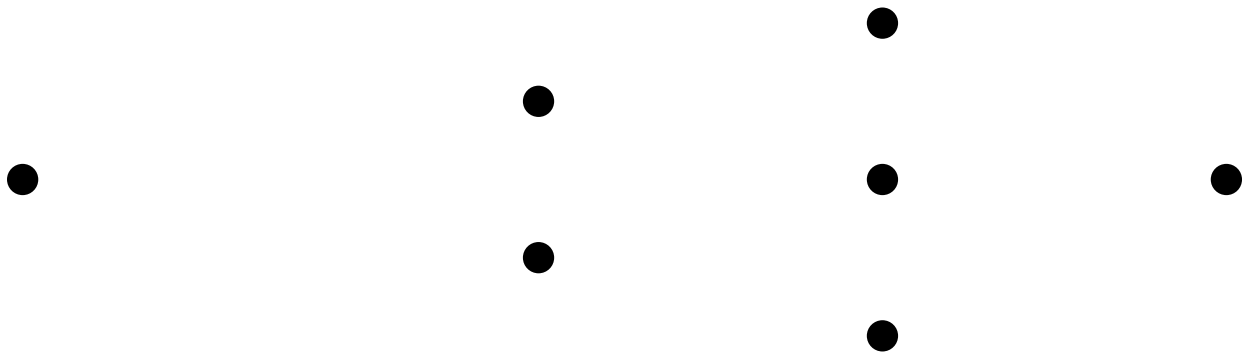
Alice



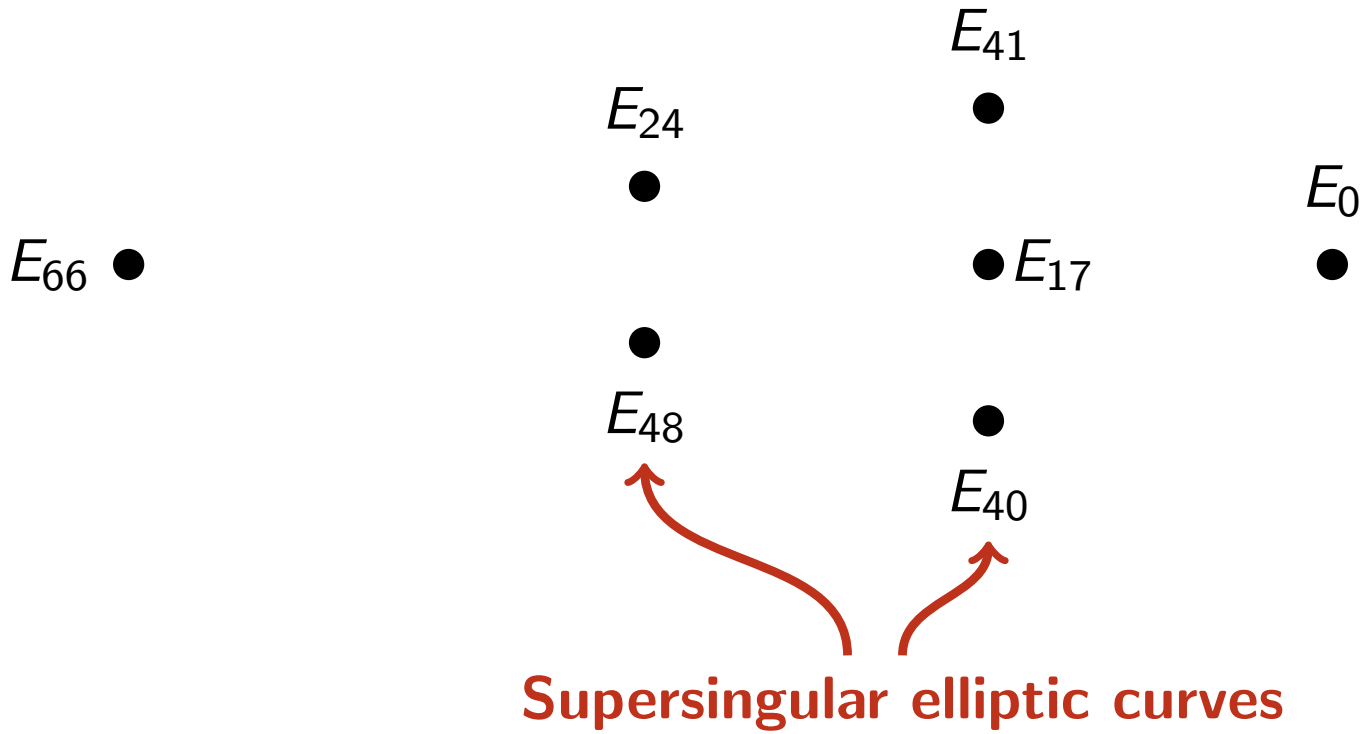
Bob



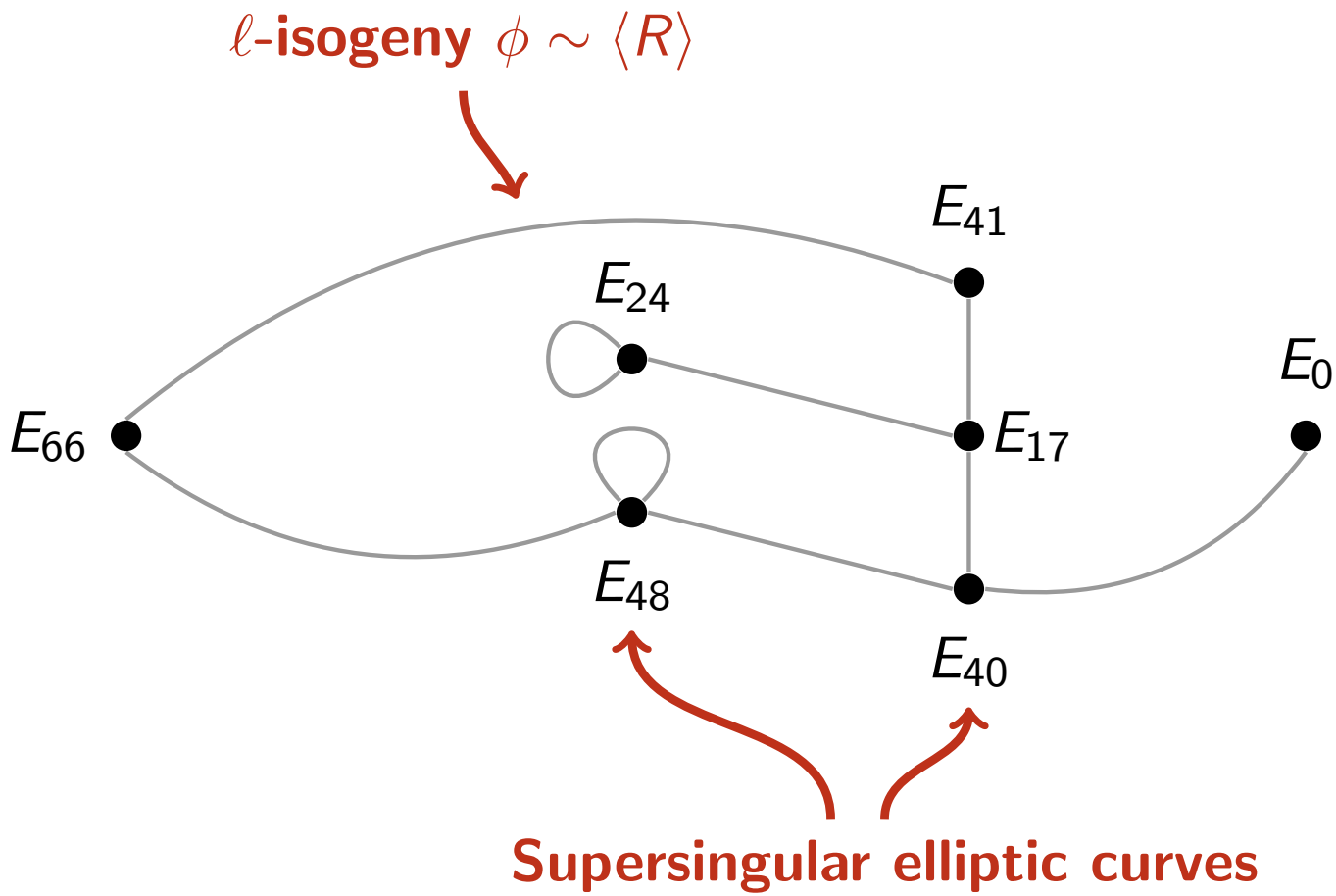
Constructing graphs and walks using isogenies



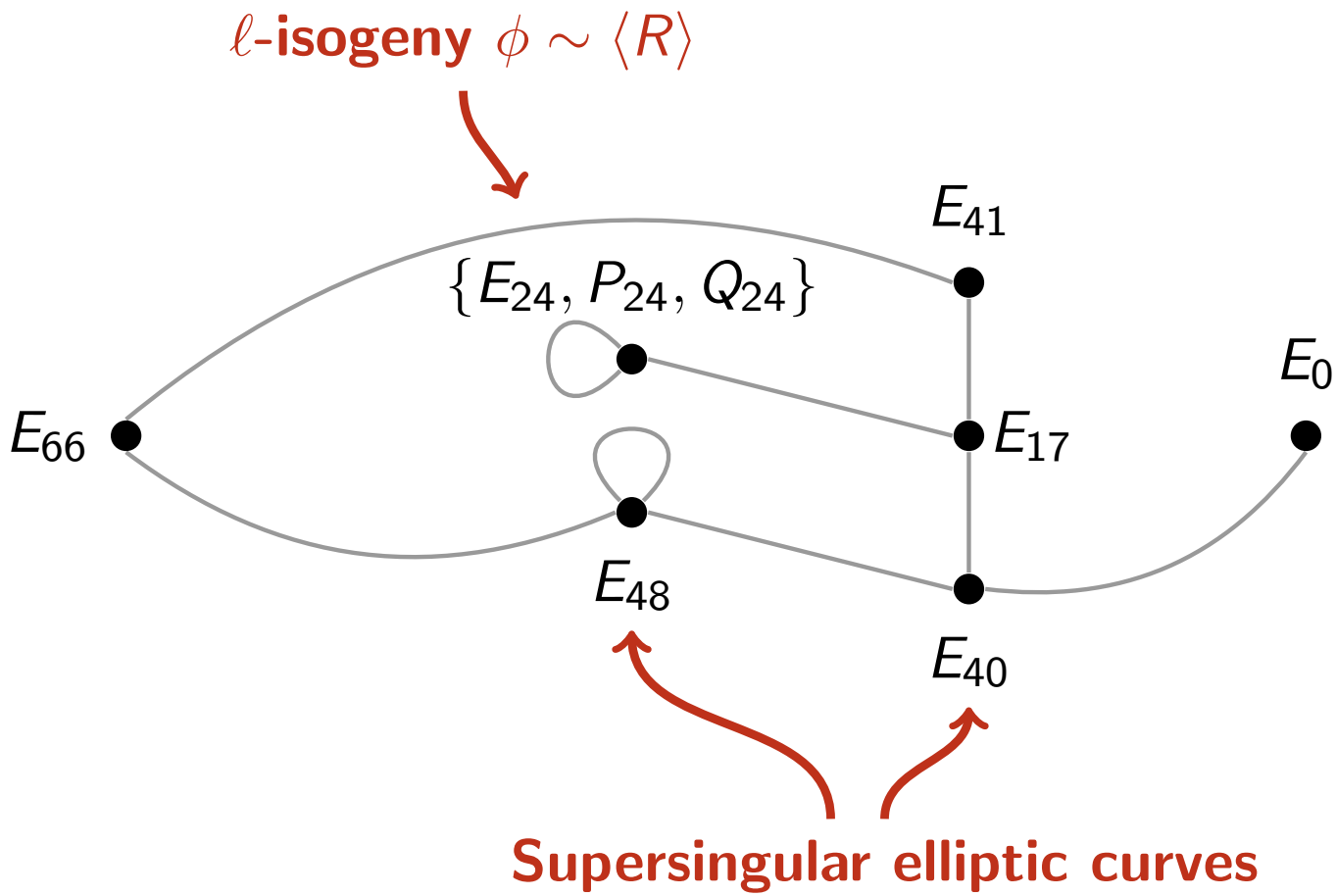
Constructing graphs and walks using isogenies



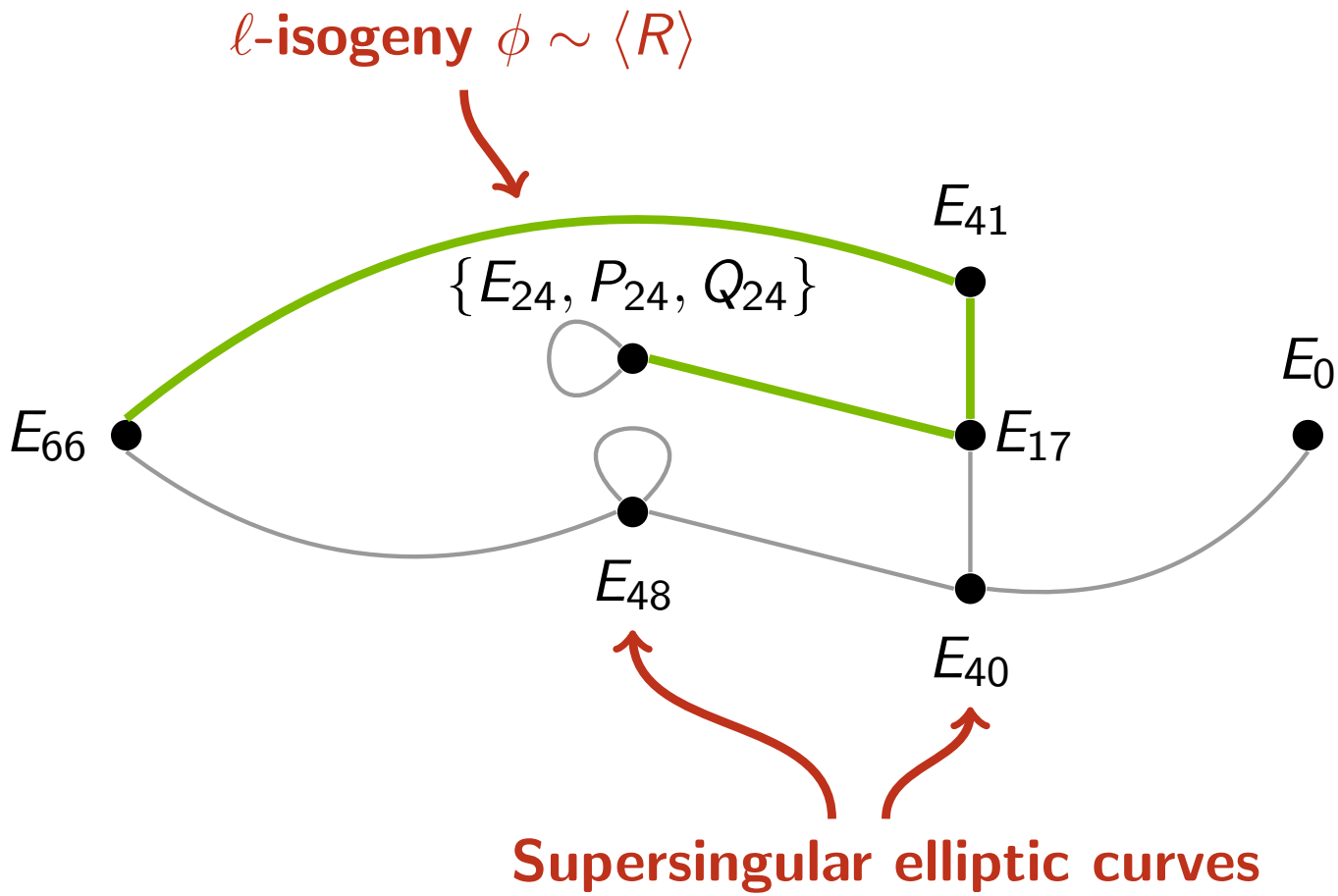
Constructing graphs and walks using isogenies



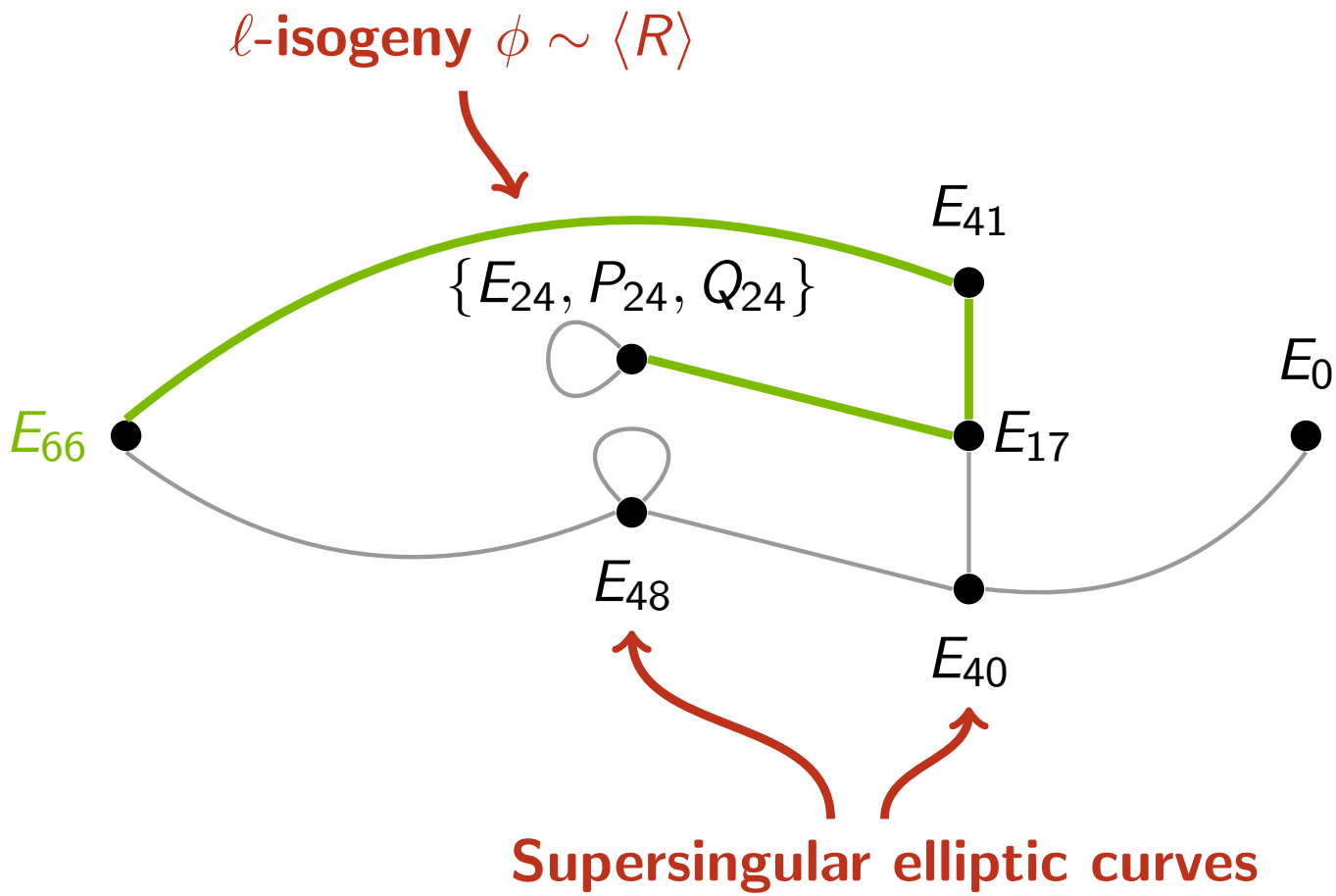
Constructing graphs and walks using isogenies



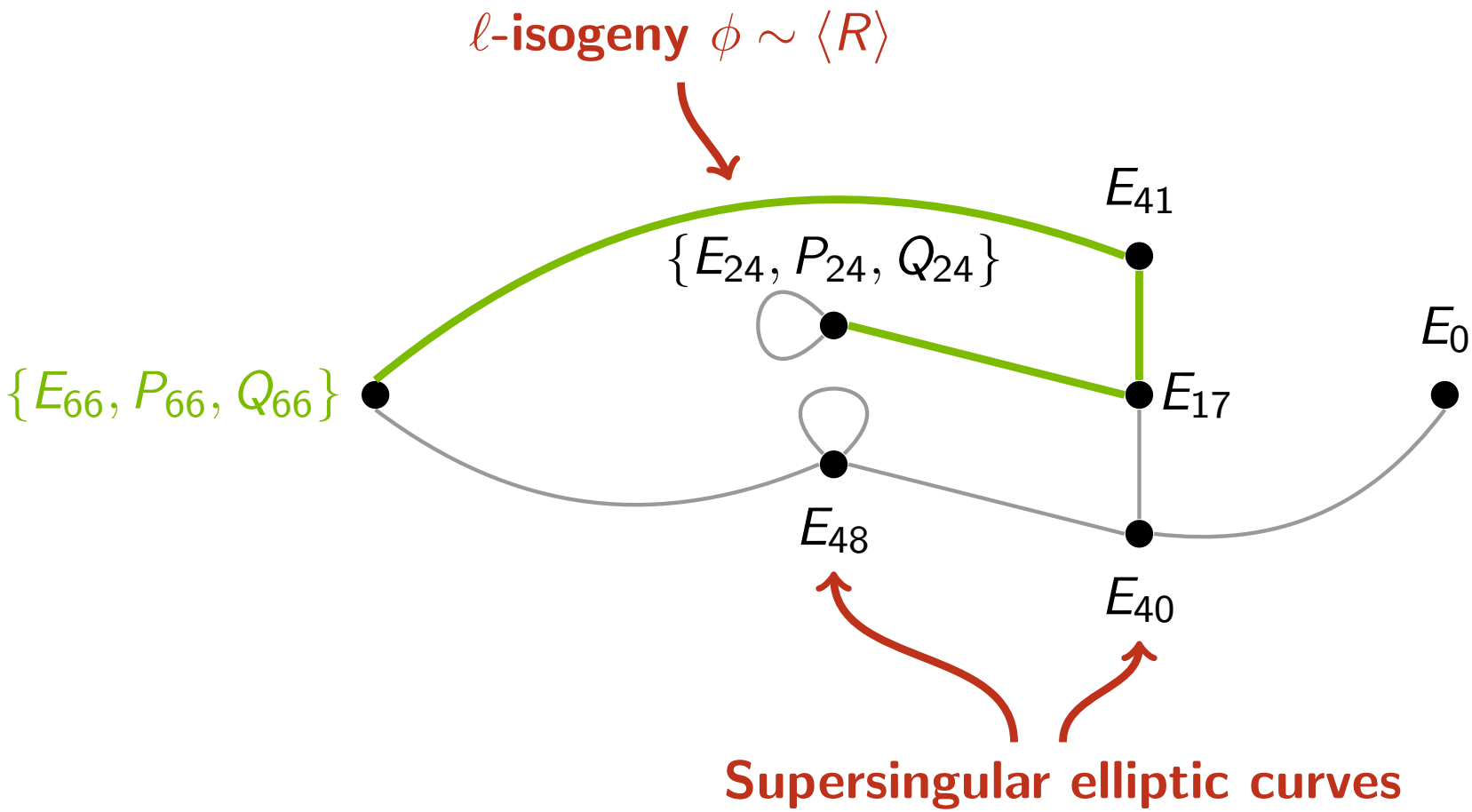
Constructing graphs and walks using isogenies



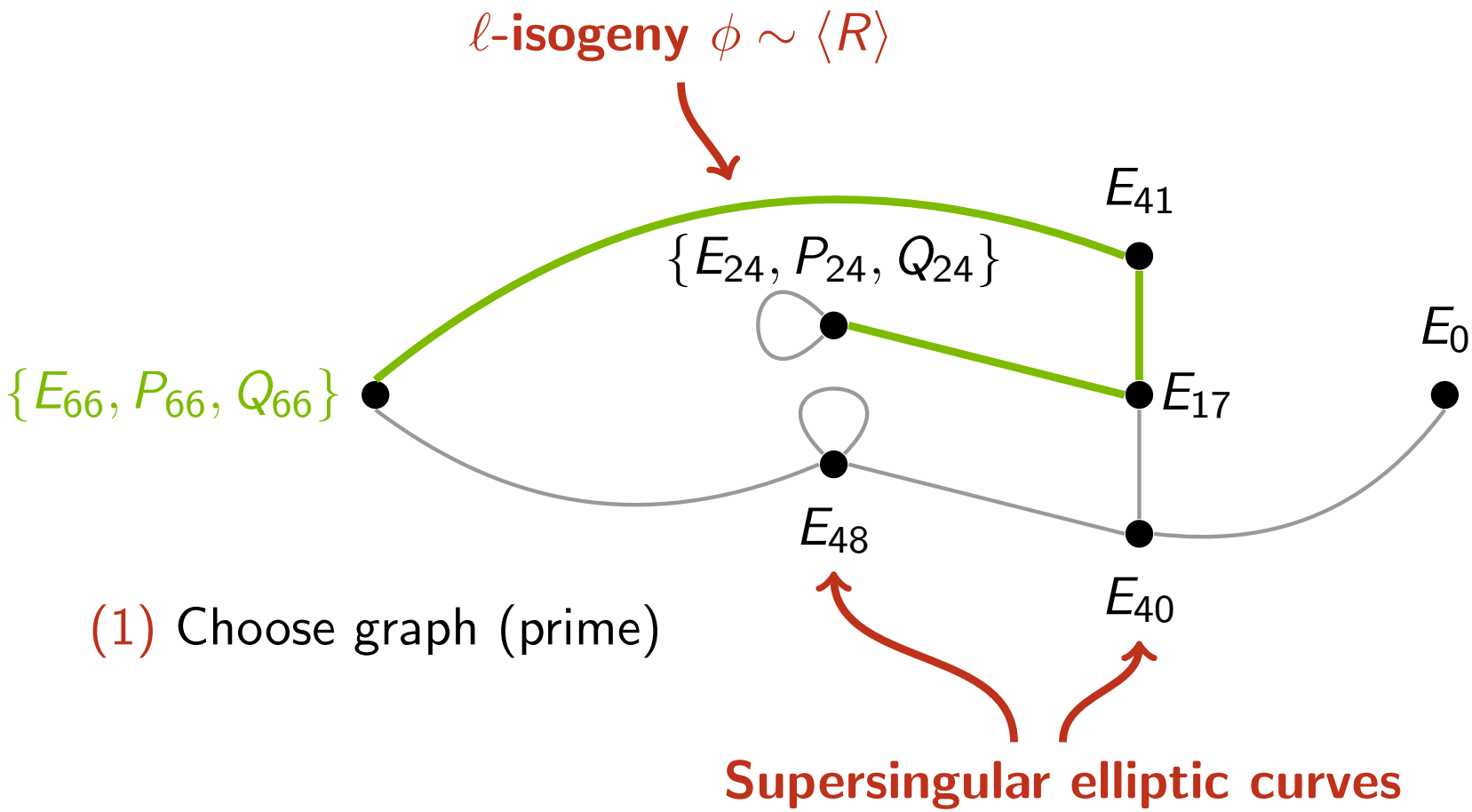
Constructing graphs and walks using isogenies



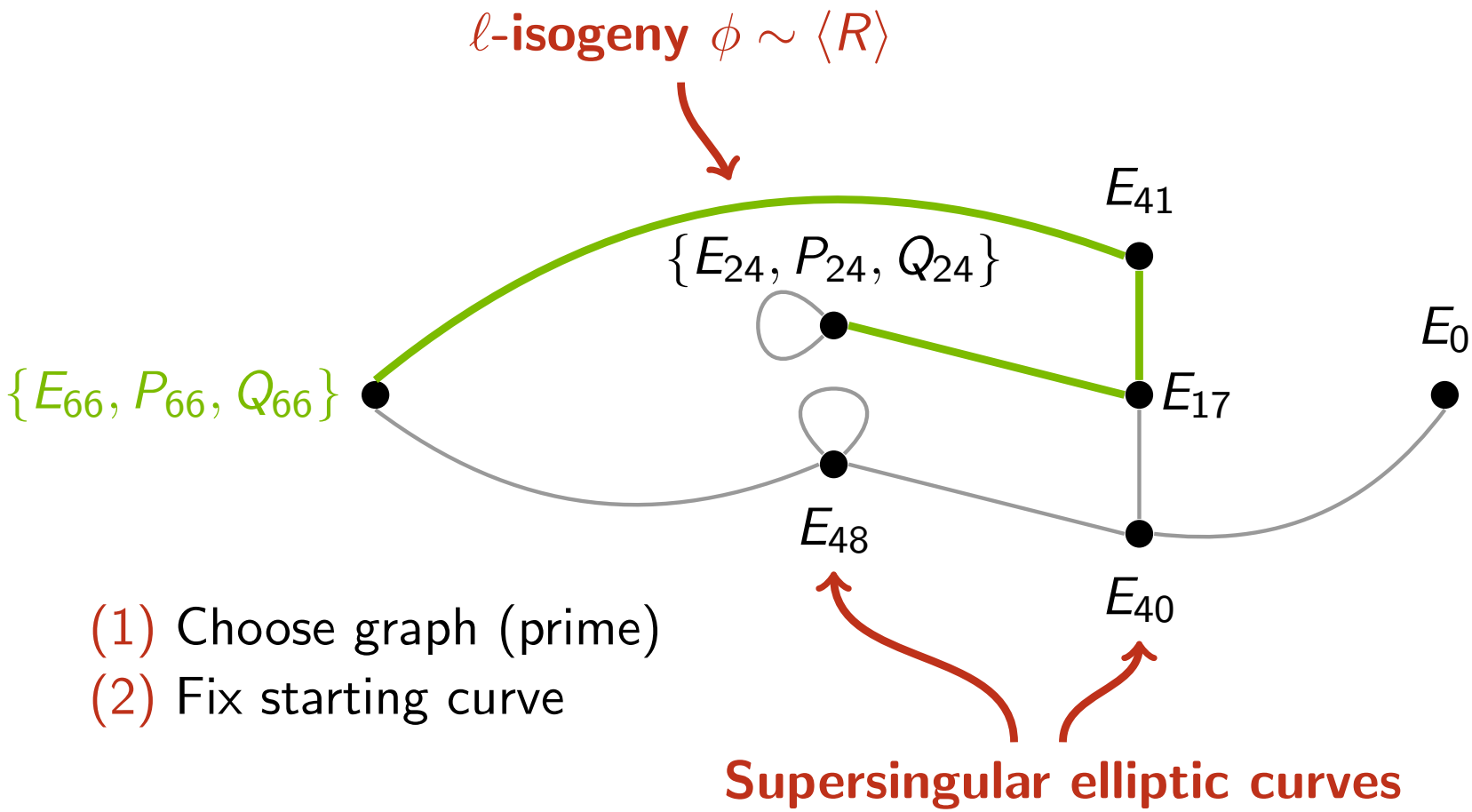
Constructing graphs and walks using isogenies



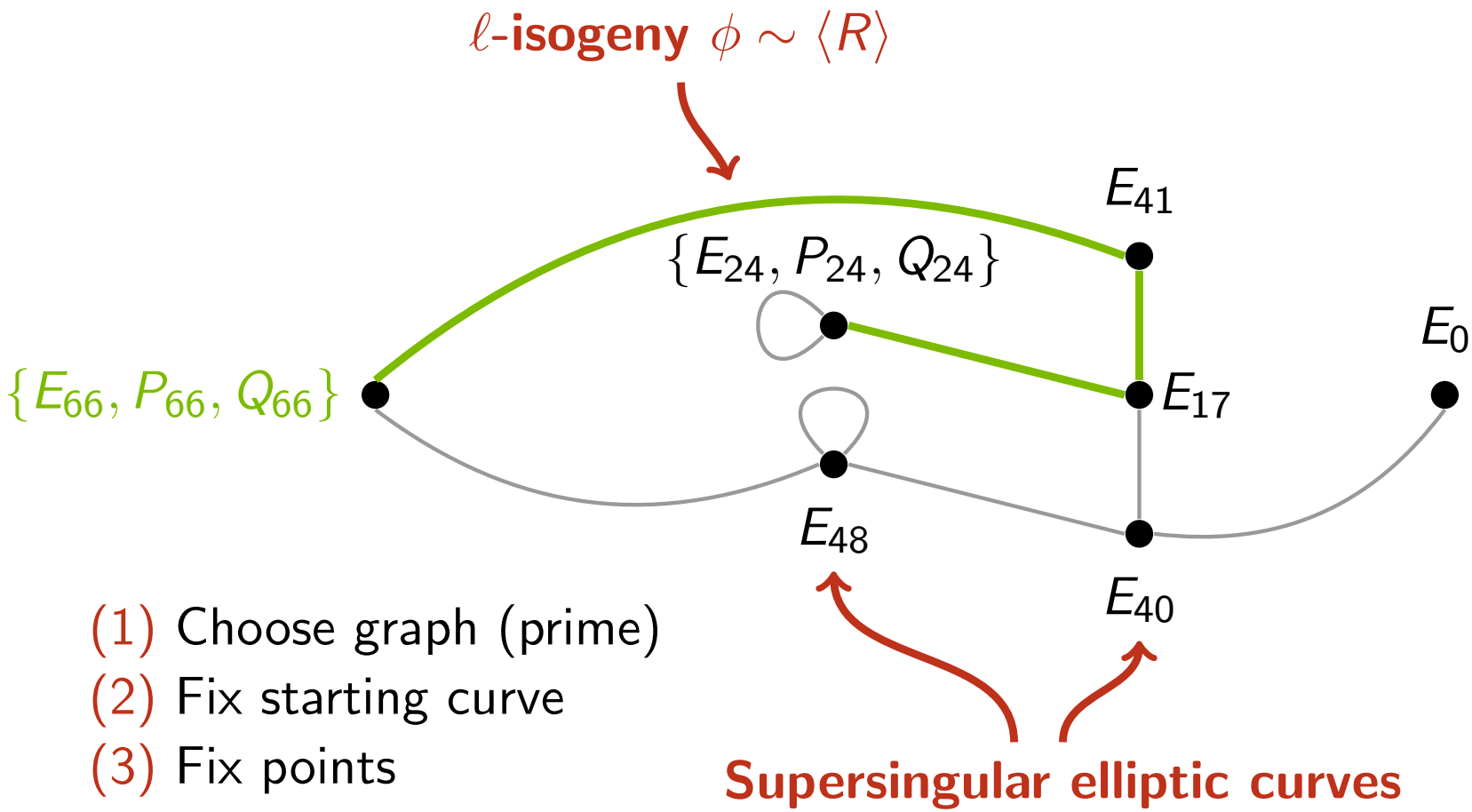
Constructing graphs and walks using isogenies



Constructing graphs and walks using isogenies



Constructing graphs and walks using isogenies



Choosing parameters

(1) Fix prime $p = 2^{e_2} \cdot 3^{e_3} - 1$

Choosing parameters

(1) Fix prime $p = 2^{e_2} \cdot 3^{e_3} - 1$

(2) Fix starting curve $E_0 : y^2 = x^3 + x$

Choosing parameters

(1) Fix prime $p = 2^{e_2} \cdot 3^{e_3} - 1$

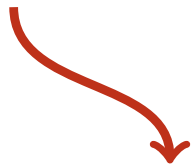
(2) Fix starting curve $E_0 : y^2 = x^3 + x$

(3) Choose "smallest" points such that

$$E_0[2^{e_2}] = \{P_2, Q_2\}, \quad E_0[3^{e_3}] = \{P_3, Q_3\}$$

Choosing parameters

Only choice to make! How large?



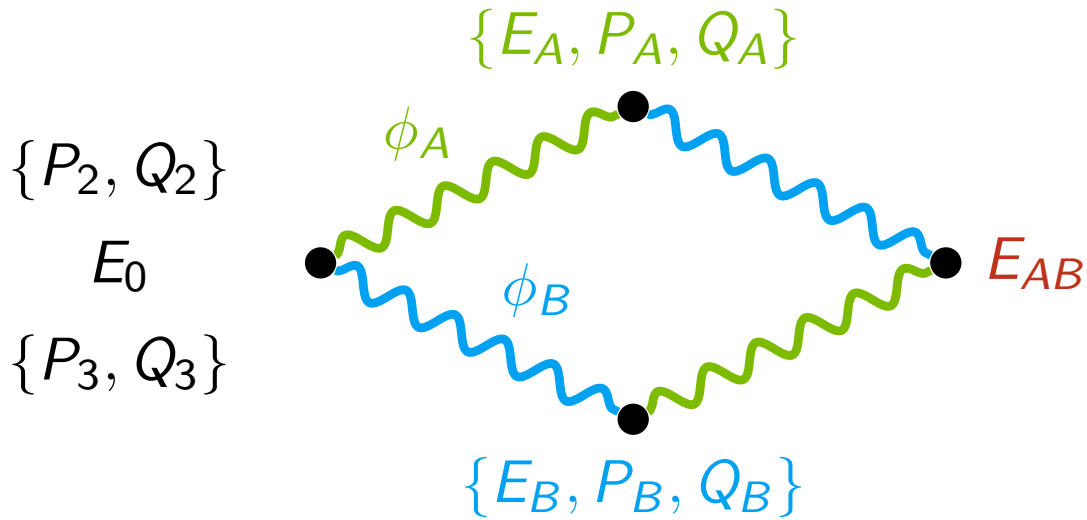
(1) Fix prime $p = 2^{e_2} \cdot 3^{e_3} - 1$

(2) Fix starting curve $E_0 : y^2 = x^3 + x$

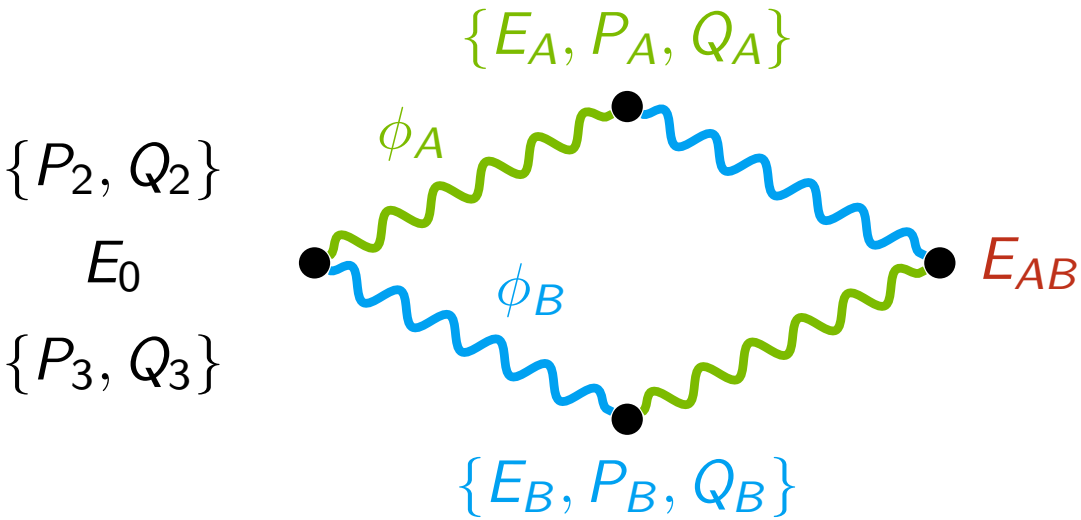
(3) Choose "smallest" points such that

$$E_0[2^{e_2}] = \{P_2, Q_2\}, \quad E_0[3^{e_3}] = \{P_3, Q_3\}$$

The SIDH problem

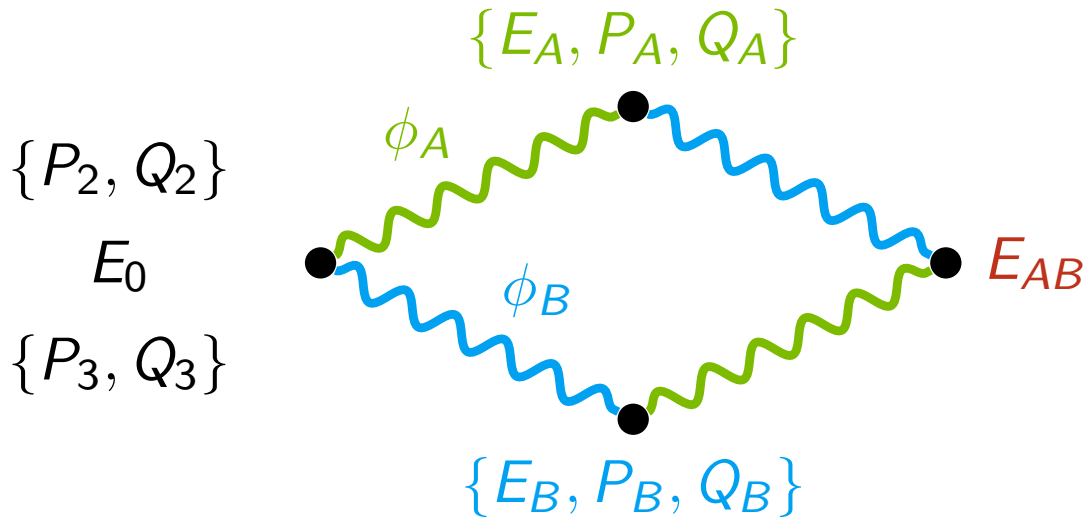


The SIDH problem



Prob. 1 (SIDH): Given $\{E_A, P_A, Q_A\}$ and $\{E_B, P_B, Q_B\}$, get E_{AB}

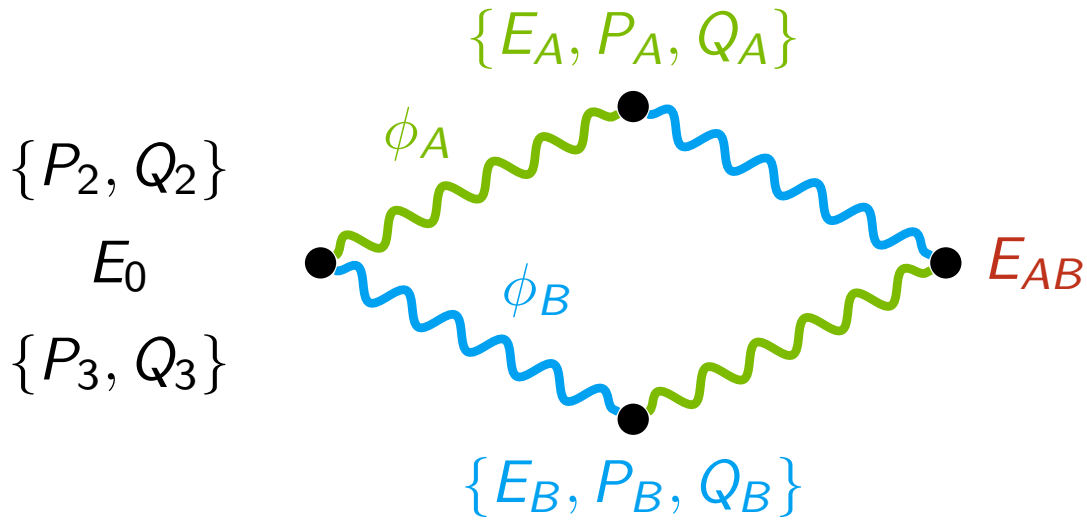
The SIDH problem



Prob. 1 (SIDH): Given $\{E_A, P_A, Q_A\}$ and $\{E_B, P_B, Q_B\}$, get E_{AB}

Prob. 2 (SSI*): Given $\{E_A, P_A, Q_A\}$, get ϕ_A

The SIDH problem

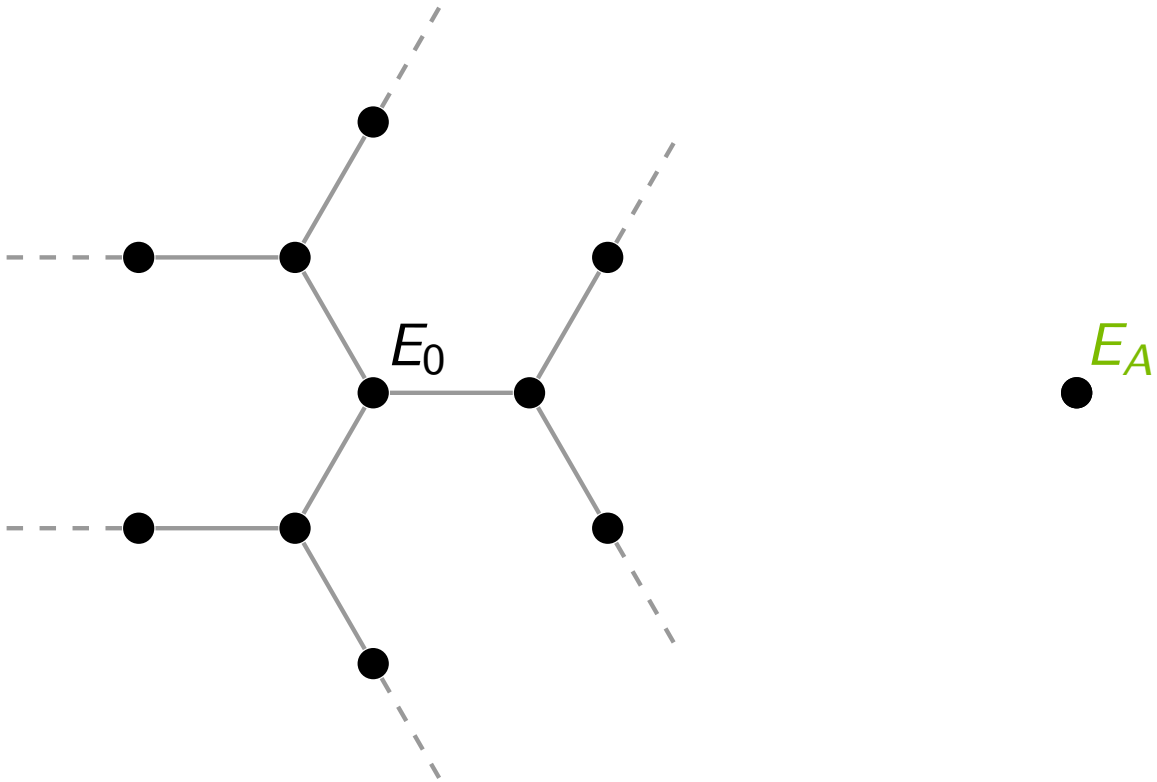


Prob. 1 (SIDH): Given $\{E_A, P_A, Q_A\}$ and $\{E_B, P_B, Q_B\}$, get E_{AB}

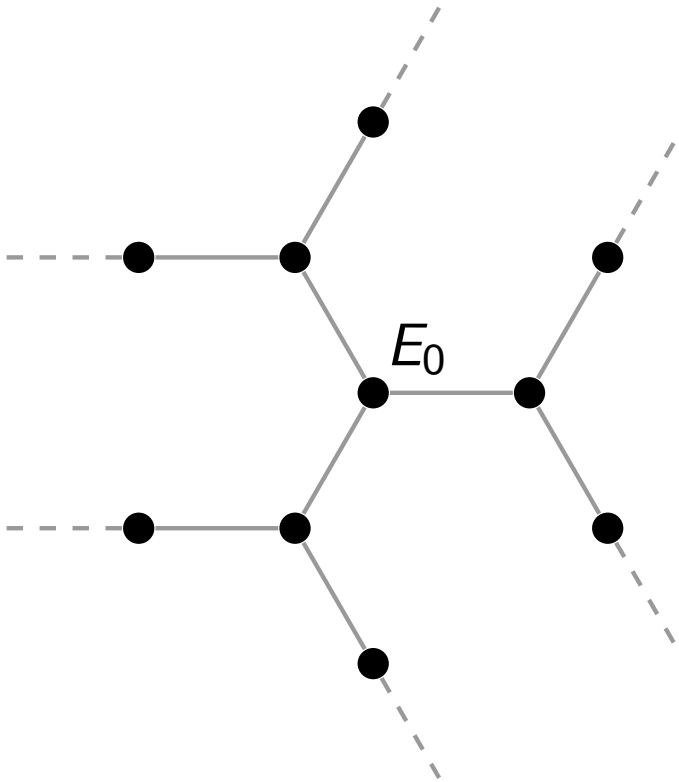
Prob. 2 (SSI*): Given $\{E_A, P_A, Q_A\}$, get ϕ_A

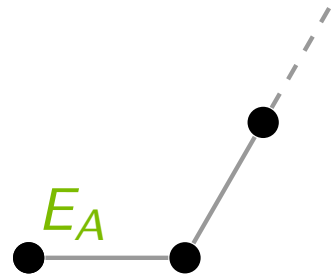
Prob. 3 (SSI): Given E_A, get ϕ_A

Solving SSI with claw finding algorithms

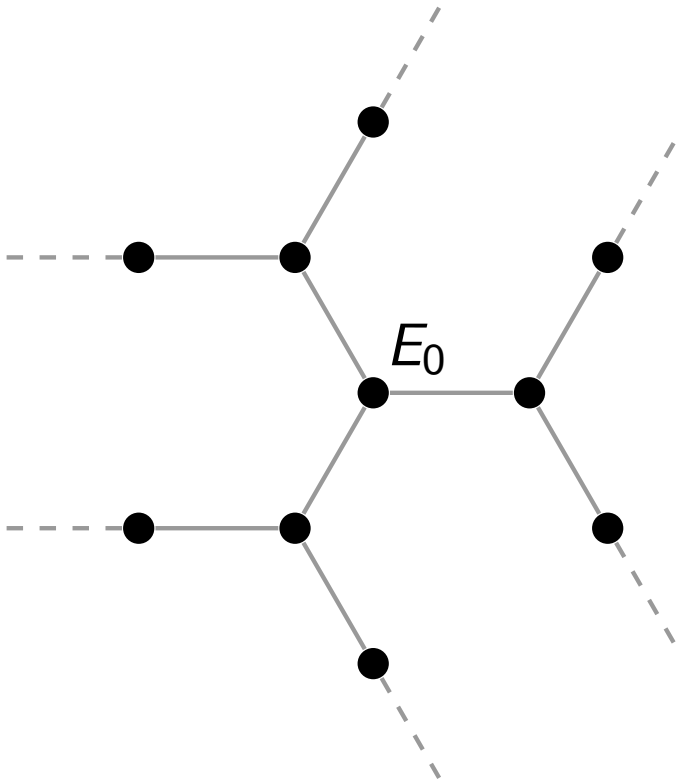


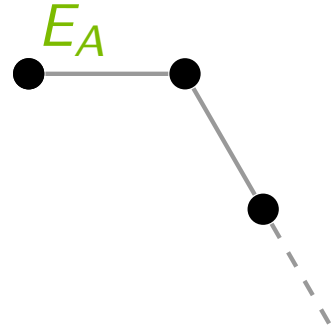
Solving SSI with claw finding algorithms



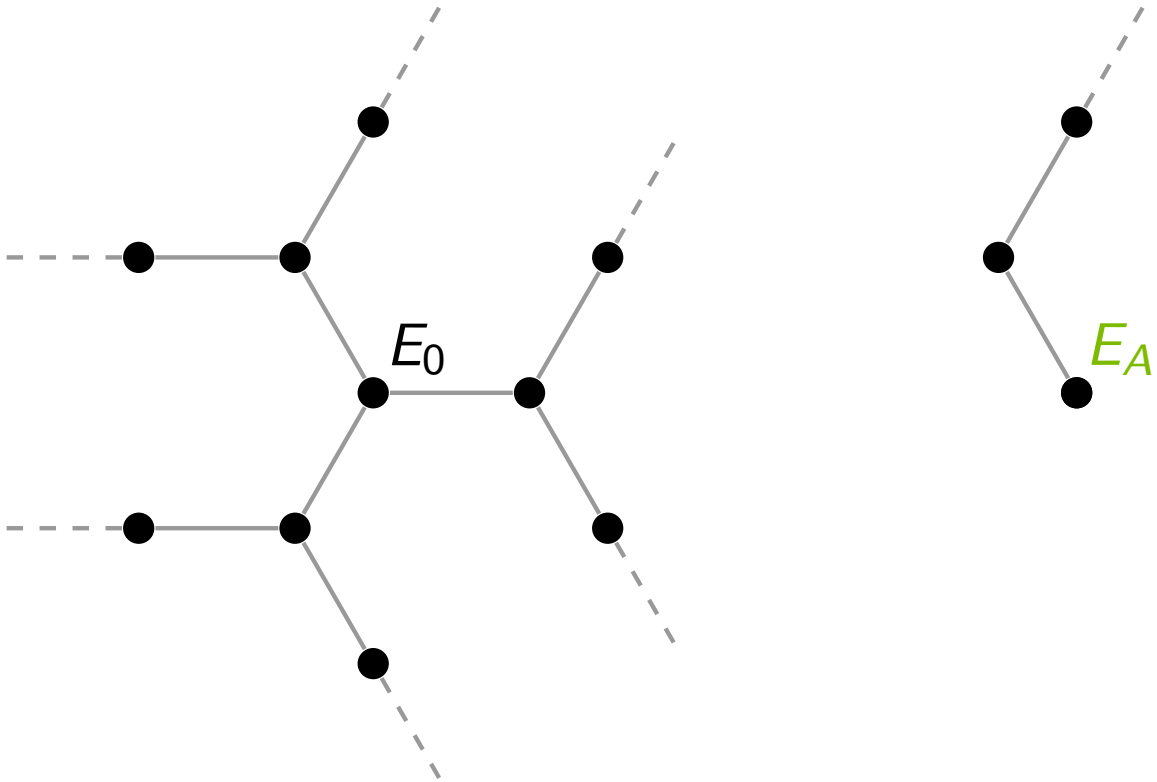


Solving SSI with claw finding algorithms

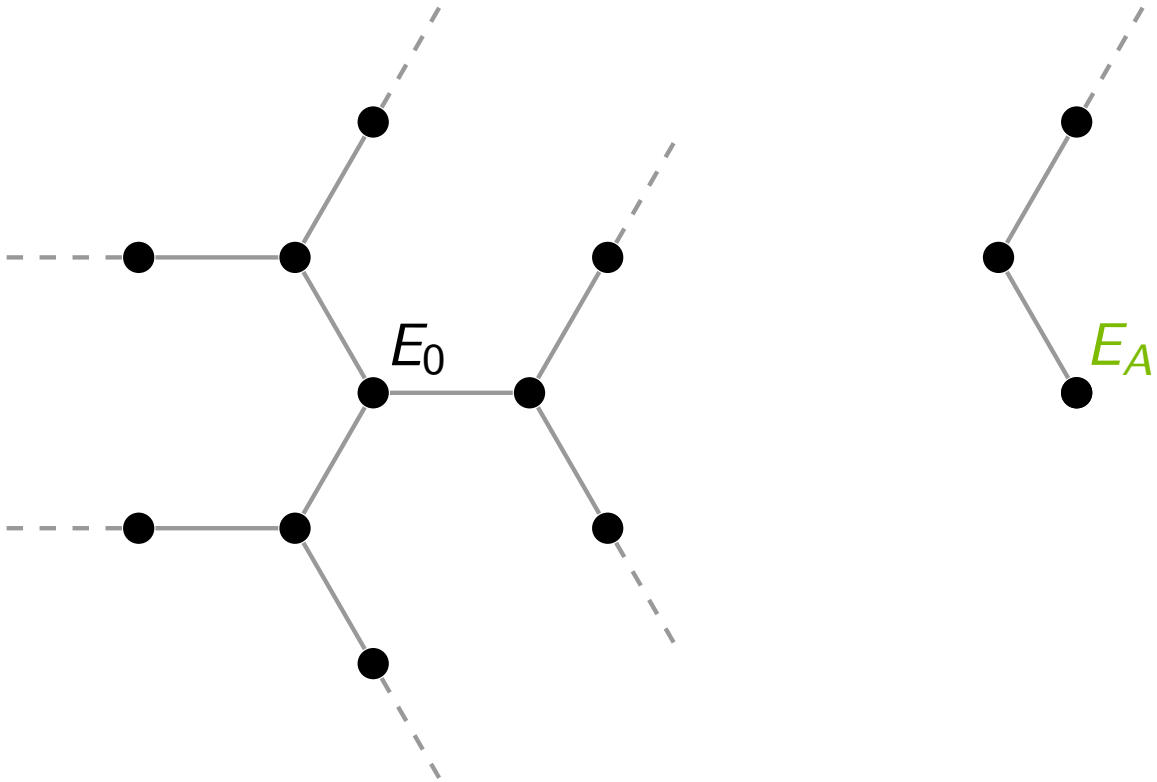




Solving SSI with claw finding algorithms



Solving SSI with claw finding algorithms



Complexity of $O(\sqrt{\deg \phi}) \sim O(\sqrt[4]{p})$ classical
$O(\sqrt[3]{\deg \phi}) \sim O(\sqrt[6]{p})$ quantum
oracle queries

Aligning security with the NIST requirements

"As secure as k-bit AES"

	Classical	Quantum
`AES128`	127	64

Aligning security with the NIST requirements

"As secure as k-bit AES"

	Classical	Quantum
`AES128`	127	64
`SIKEp503`	125	83

Aligning security with the NIST requirements

"As secure as k-bit AES"

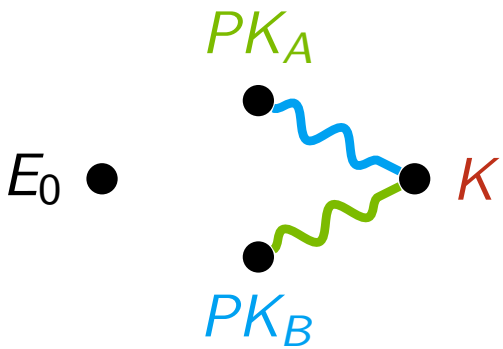
	Classical	Quantum
`AES128`	127	64
`SIKEp503`	125	83
`AES192`	191	96
`SIKEp751`	186	124

Aligning security with the NIST requirements

"As secure as k-bit AES"

	Classical	Quantum
AES128	127	64
SIKEp503	125	83
AES192	191	96
SIKEp751	186	124
AES256	255	128
SIKEp964	238	159

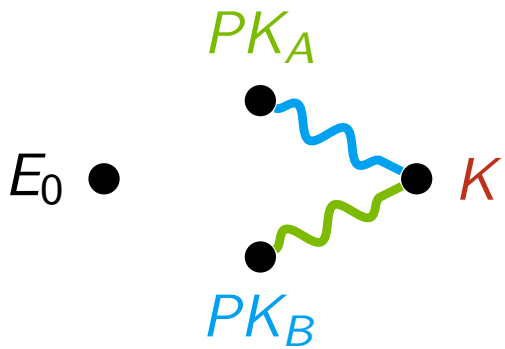
What is SIKE...



SIDH

Passively secure
under (SI)CDH

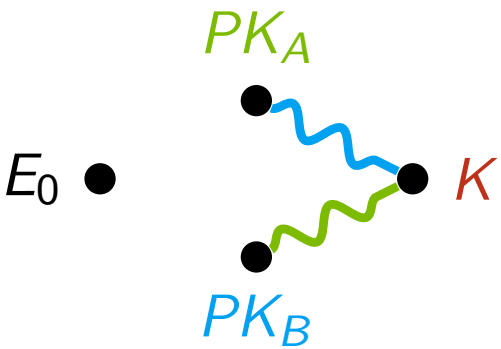
What is SIKE...

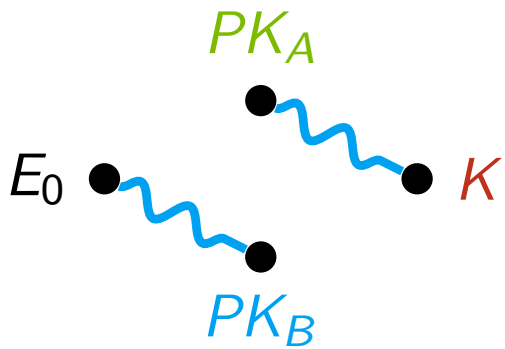


SIDH

Passively secure
under (SI)CDH

What is SIKE...

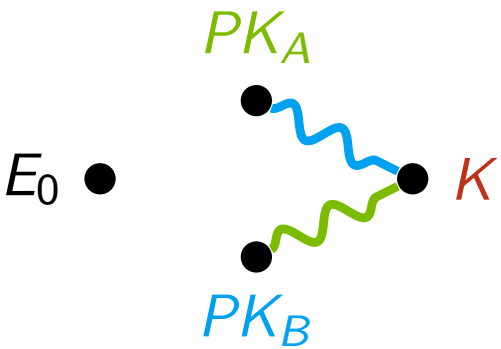


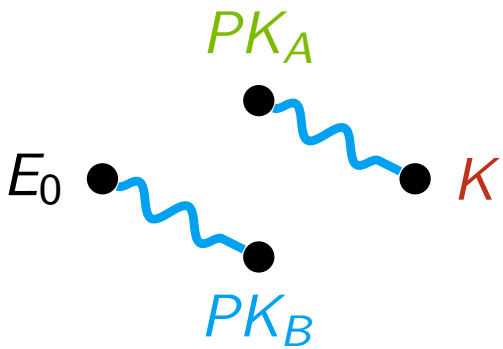


SIDH

Passively secure
under (SI)CDH

What is SIKE...





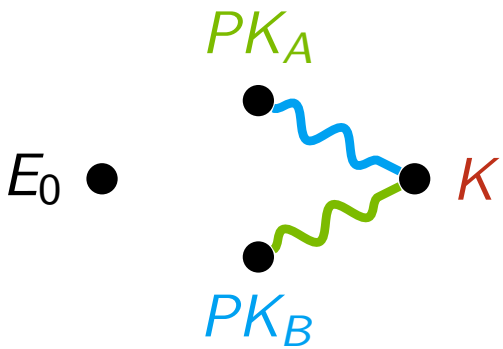
$C_0 = PK_B$

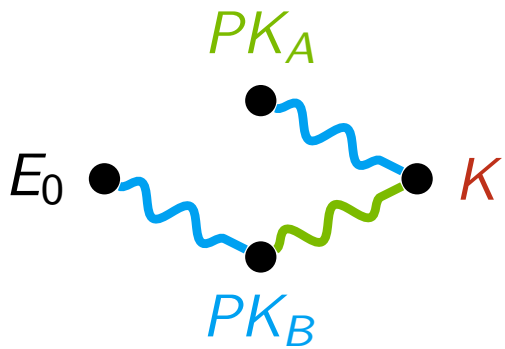
$C_1 = M \oplus F(K)$

SIDH

Passively secure
under (SI)CDH

What is SIKE...





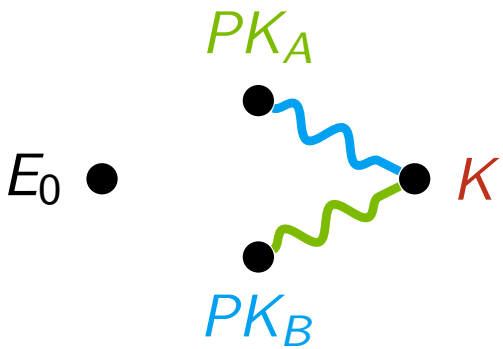
$C_0 = PK_B$

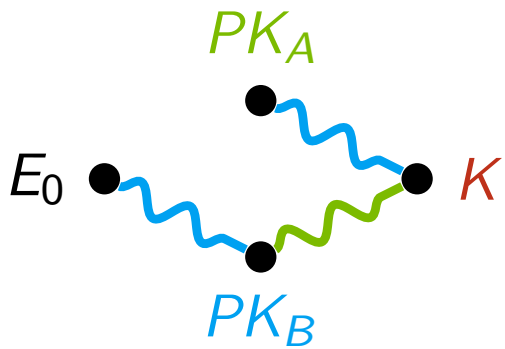
$C_1 = M \oplus F(K)$

SIDH

Passively secure
under (SI)CDH

What is SIKE...





$C_0 = PK_B$

$C_1 = M \oplus F(K)$

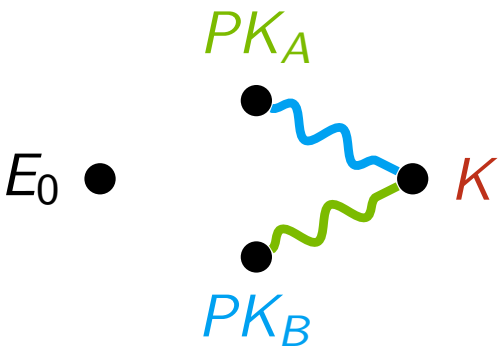
SIDH

Passively secure under (SI)CDH

ElGamal

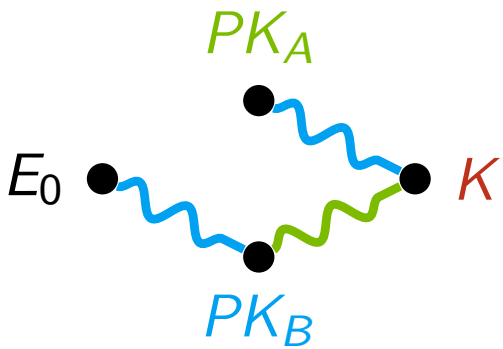
Passively secure under (SI)CDH in ROM

What is SIKE...



SIDH

Passively secure under (SI)CDH

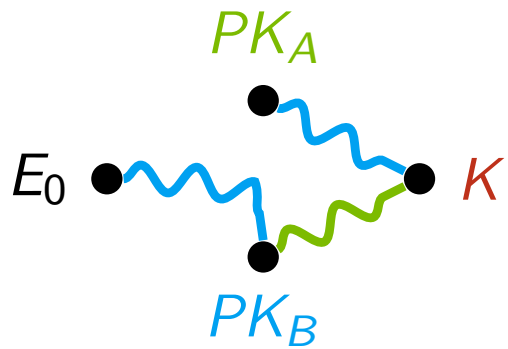


$C_0 = PK_B$

$C_1 = M \oplus F(K)$

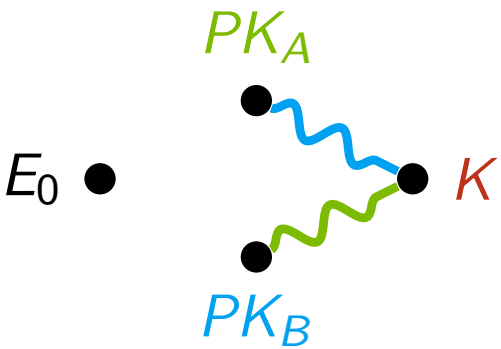
ElGamal

Passively secure under (SI)CDH in ROM



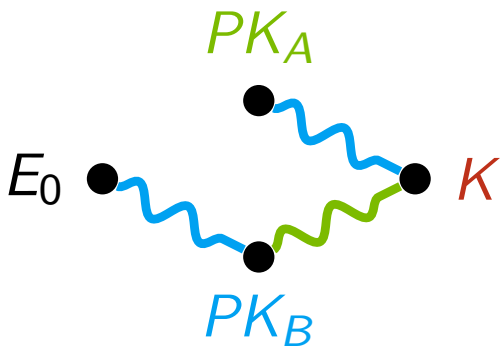
$S = H(M, C_0, C_1)$

What is SIKE...



SIDH

Passively secure under (SI)CDH

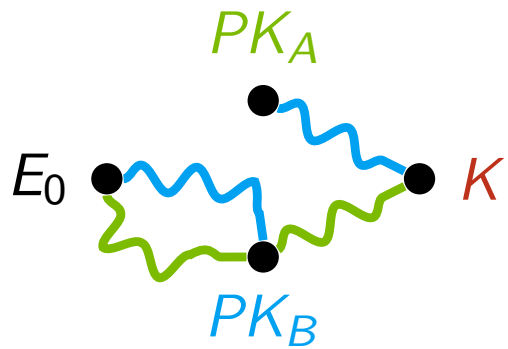


$C_0 = PK_B$

$C_1 = M \oplus F(K)$

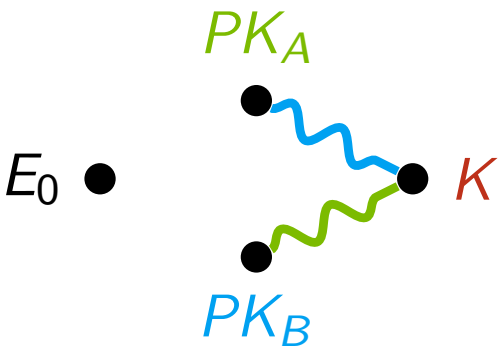
ElGamal

Passively secure under (SI)CDH in ROM



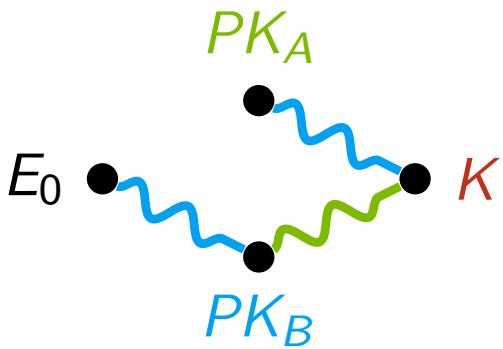
$S = H(M, C_0, C_1)$

What is SIKE...



SIDH

Passively secure under (SI)CDH

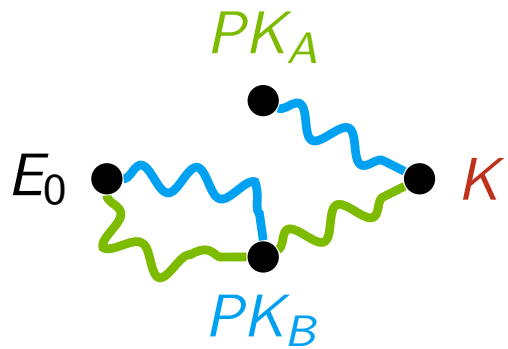


$C_0 = PK_B$

$C_1 = M \oplus F(K)$

ElGamal

Passively secure under (SI)CDH in ROM



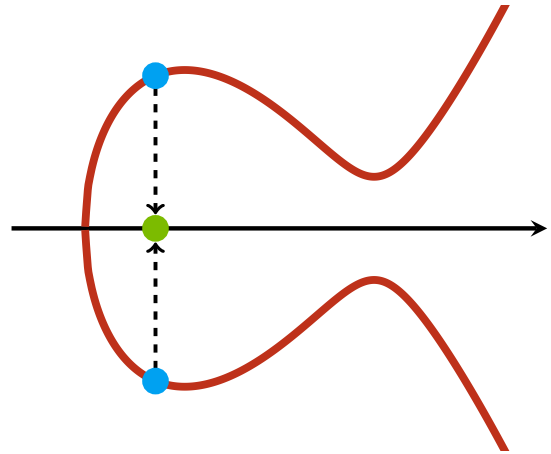
$S = H(M, C_0, C_1)$

SIKE

Actively secure under (SI)CDH in ROM

Implementation choices: curve model

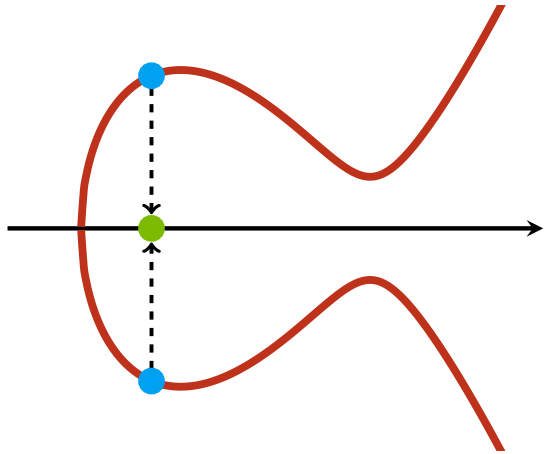
(1) Model choice: Montgomery



Implementation choices: curve model

(1) Model choice: Montgomery

(2) Only x-coordinates needed



$$E_0 \xrightarrow{\phi} E_1$$

$$(x, —) \longmapsto (f(x), —)$$

$$\deg(f) = \deg(\phi)$$

Computing isogenies

(3) Tree-based isogeny computation

$$(E_0, P_{00})$$

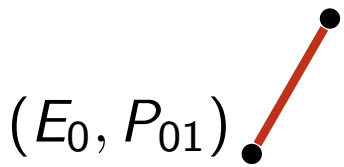
$$\bullet$$

Order of P_{00} is ℓ^e

$$\implies \deg(\phi_{00}) = \ell^e$$

Computing isogenies

(3) Tree-based isogeny computation



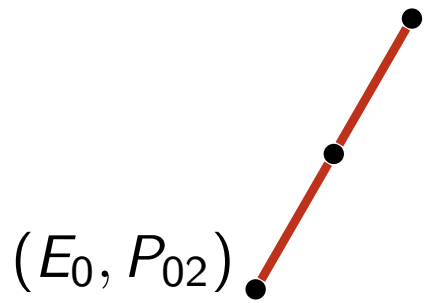
$P_{01} = [\ell]P_{00}$

Order of P_{01} is ℓ^{e-1}

$\implies \deg(\phi_{01}) = \ell^{e-1}$

Computing isogenies

(3) Tree-based isogeny computation



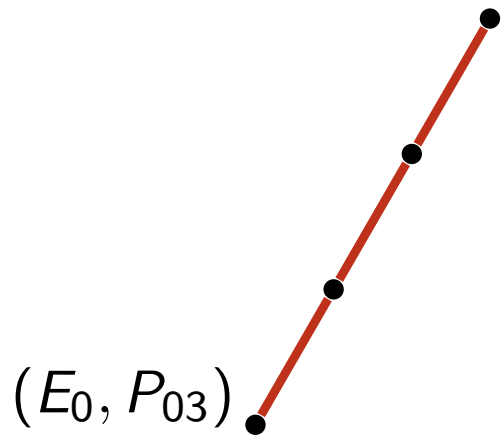
$P_{02} = [\ell^2]P_{00}$

Order of P_{02} is ℓ^{e-2}

$\implies \deg(\phi_{02}) = \ell^{e-2}$

Computing isogenies

(3) Tree-based isogeny computation



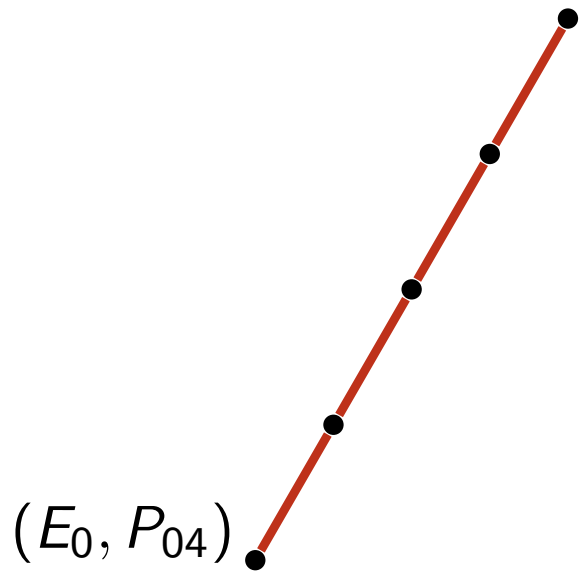
$P_{03} = [\ell^3]P_{00}$

Order of P_{03} is ℓ^{e-3}

$\implies \deg(\phi_{03}) = \ell^{e-3}$

Computing isogenies

(3) Tree-based isogeny computation



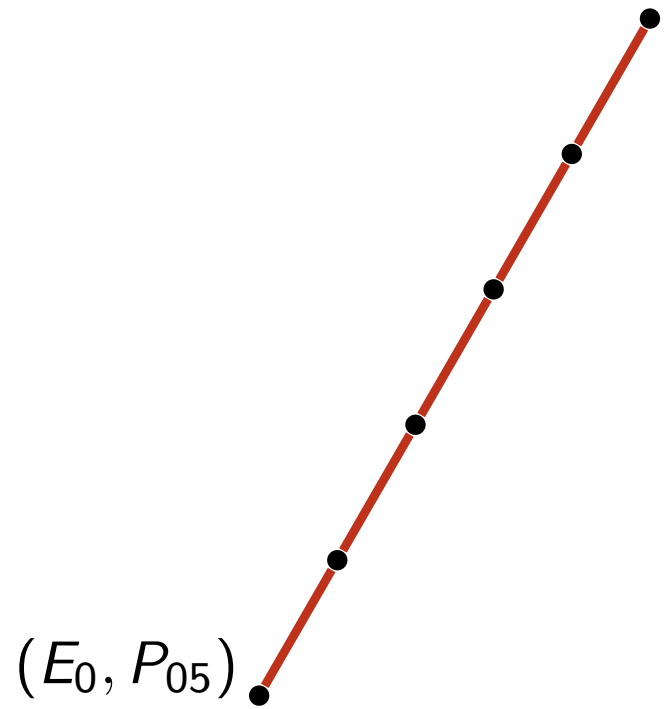
$P_{04} = [\ell^4]P_{00}$

Order of P_{04} is ℓ^{e-4}

$\implies \deg(\phi_{04}) = \ell^{e-4}$

Computing isogenies

(3) Tree-based isogeny computation



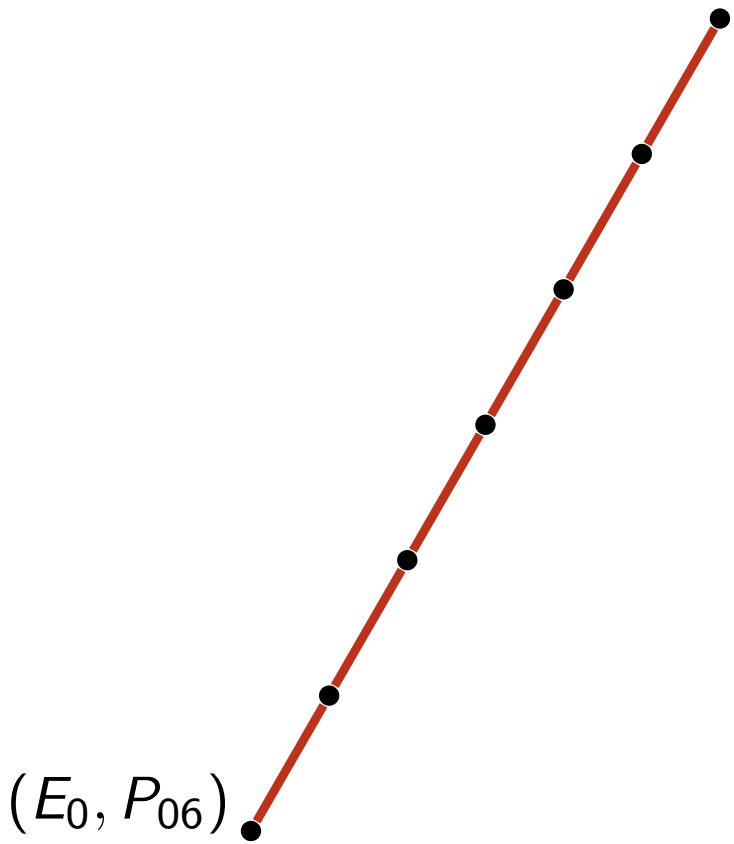
$P_{05} = [\ell^5]P_{00}$

Order of P_{05} is ℓ^{e-5}

$\implies \deg(\phi_{05}) = \ell^{e-5}$

Computing isogenies

(3) Tree-based isogeny computation



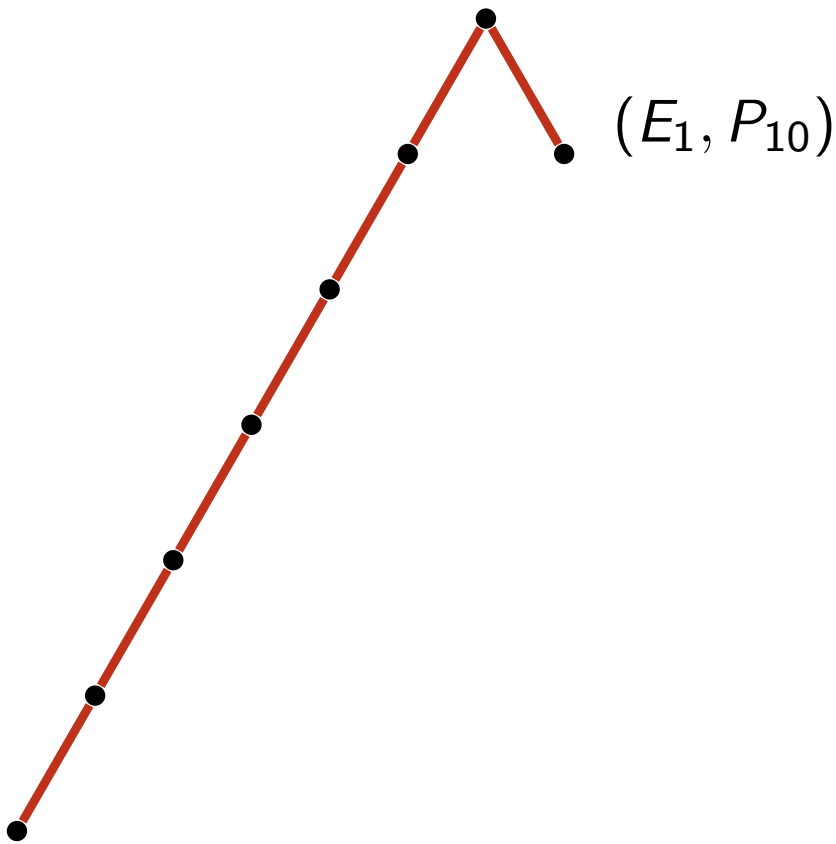
$P_{06} = [\ell^6]P_{00}$

Order of P_{06} is ℓ^{e-6}

$\implies \deg(\phi_{06}) = \ell^{e-6}$

Computing isogenies

(3) Tree-based isogeny computation



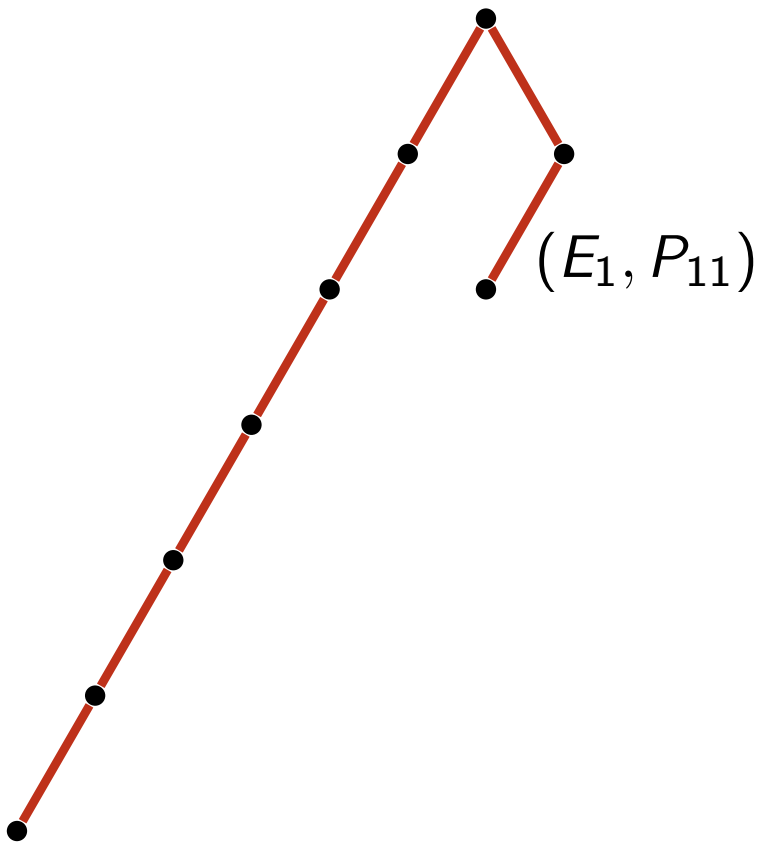
$P_{10} = \phi_{00}(P_{00})$

Order of P_{10} is ℓ^{e-1}

$\implies \deg(\phi_{10}) = \ell^{e-1}$

Computing isogenies

(3) Tree-based isogeny computation



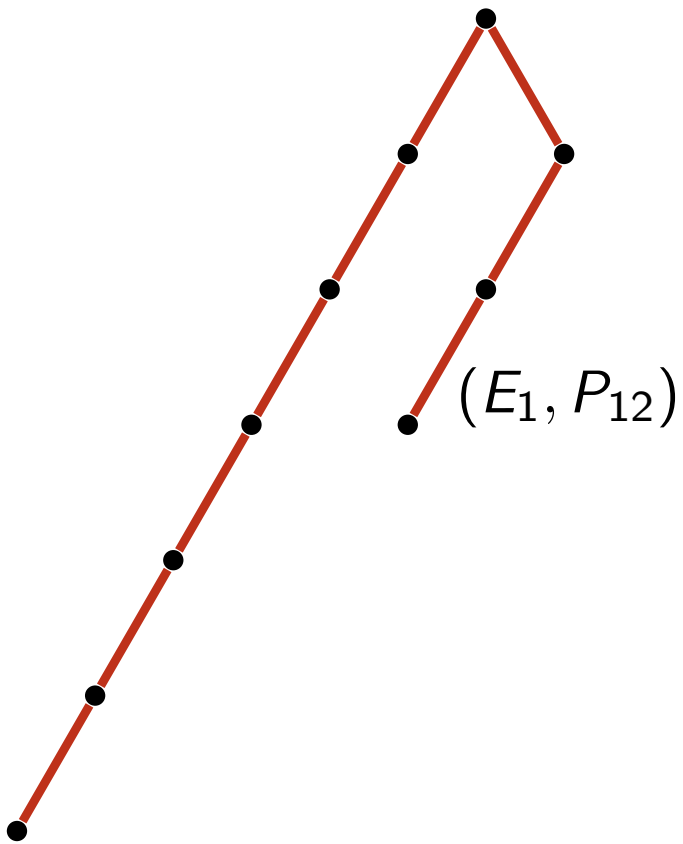
$P_{11} = [\ell]P_{10}$

Order of P_{11} is ℓ^{e-2}

$\implies \deg(\phi_{11}) = \ell^{e-2}$

Computing isogenies

(3) Tree-based isogeny computation



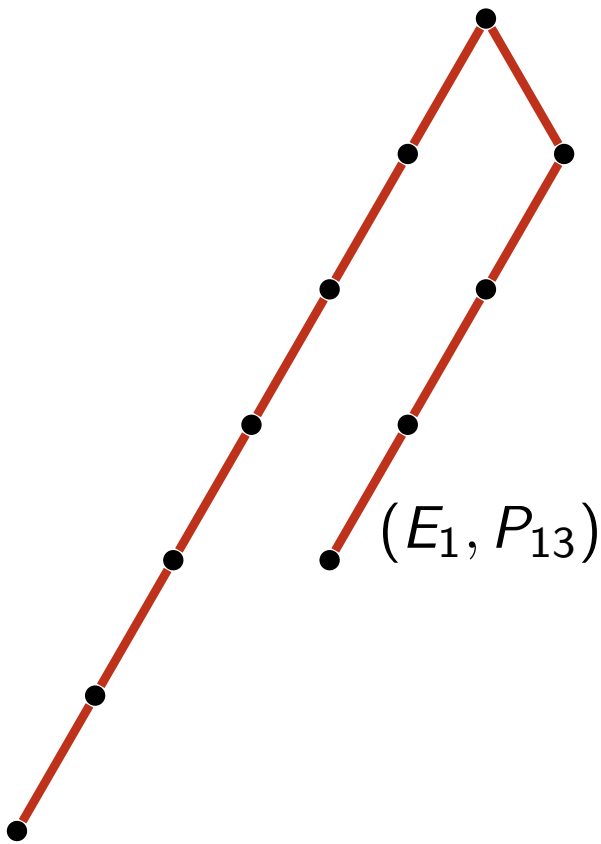
$P_{12} = [\ell^2]P_{10}$

Order of P_{12} is ℓ^{e-3}

$\implies \deg(\phi_{12}) = \ell^{e-3}$

Computing isogenies

(3) Tree-based isogeny computation



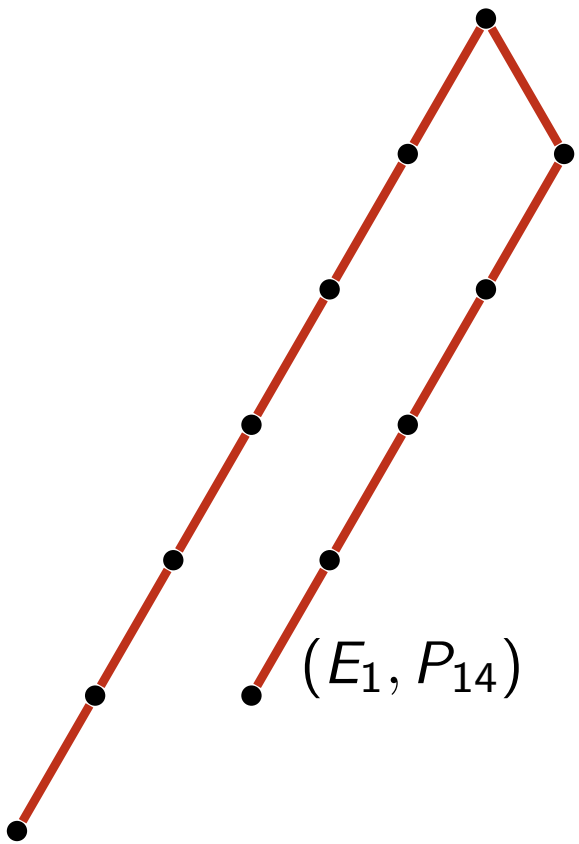
$P_{13} = [\ell^3]P_{10}$

Order of P_{13} is ℓ^{e-4}

$\implies \deg(\phi_{13}) = \ell^{e-4}$

Computing isogenies

(3) Tree-based isogeny computation



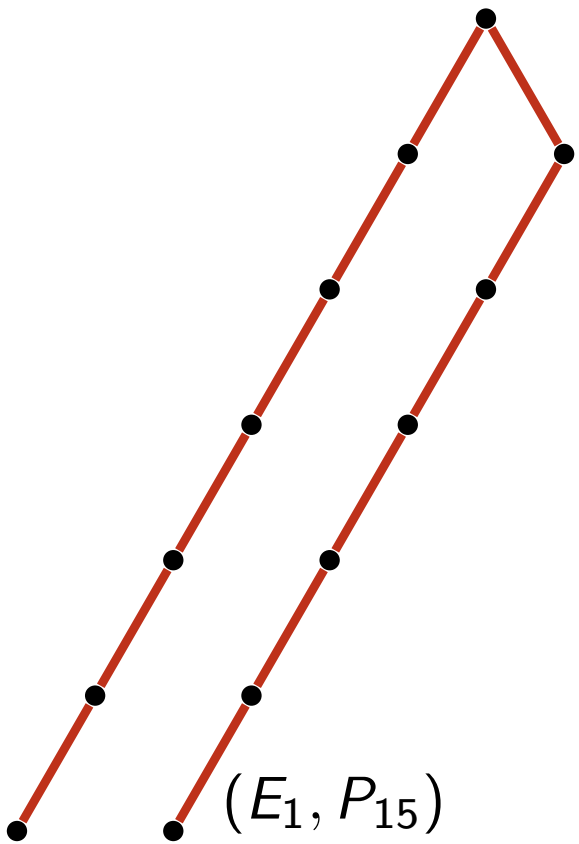
$P_{14} = [\ell^4]P_{10}$

Order of P_{14} is ℓ^{e-5}

$\implies \deg(\phi_{14}) = \ell^{e-5}$

Computing isogenies

(3) Tree-based isogeny computation



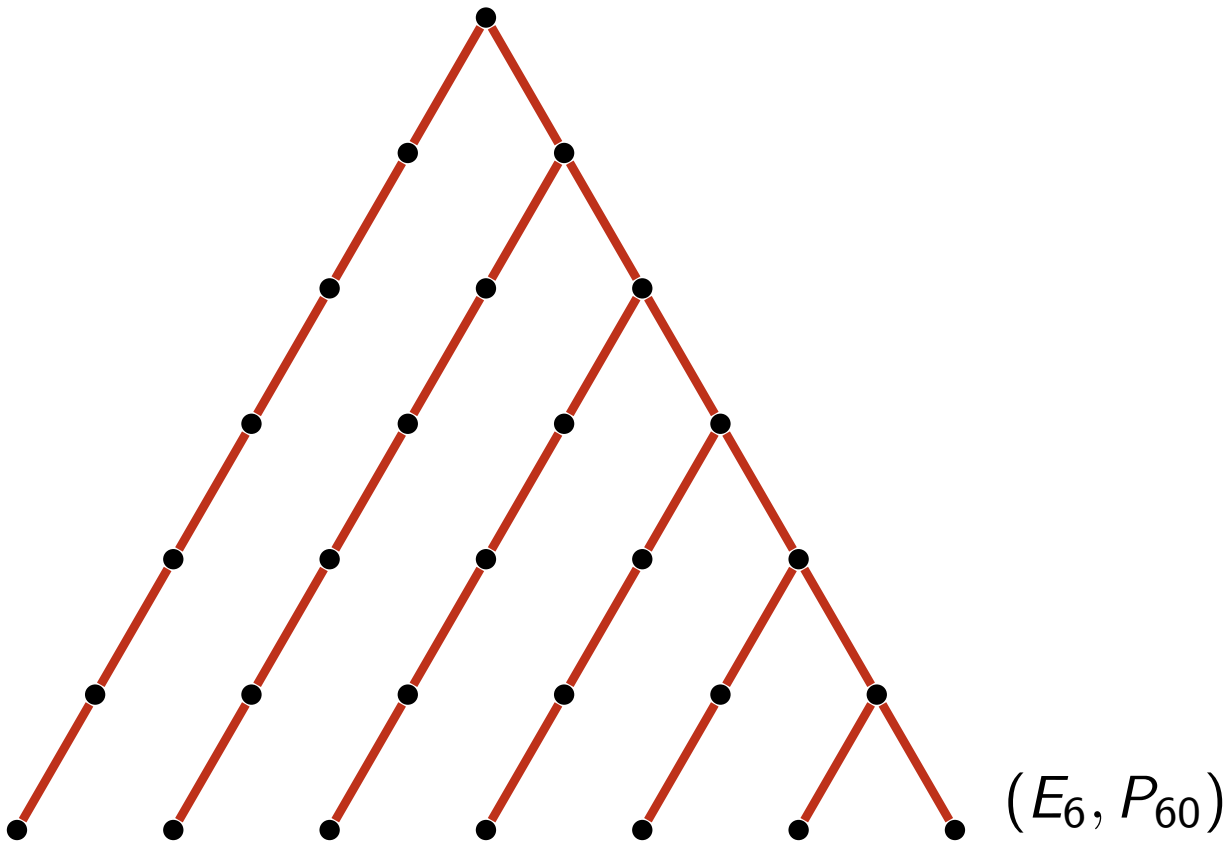
$P_{15} = [\ell^5]P_{10}$

Order of P_{15} is ℓ^{e-6}

$\implies \deg(\phi_{15}) = \ell^{e-6}$

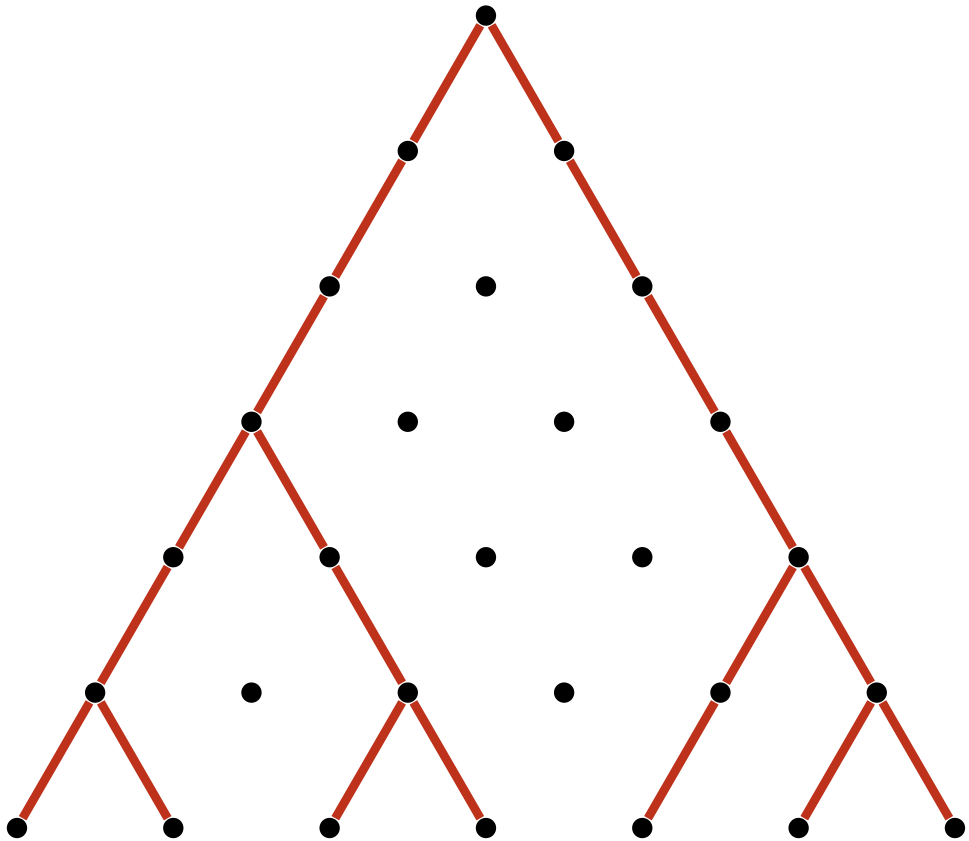
Computing isogenies

(3) Tree-based isogeny computation



Computing isogenies

(3) Tree-based isogeny computation



Where to begin

(4) Starting curve $E_0 : y^2 = x^3 + x$ with $j = 1728$

$\Longrightarrow$ Know things about $\mathrm{End}(E_0)$, could help attacks..[1]

$\Longrightarrow$ Defined over $\mathbb{F}_p \subset \mathbb{F}_{p^2}$

$\Longrightarrow$ Attack $O(\sqrt{p})$ (with low memory[2])

$\Longrightarrow$ No better way to obtain a random starting curve?

[1] Petit '17

[2] Delfs, Galbraith '13

Other implementation choices

(5) No public-key compression

Other implementation choices

(5) No public-key compression

(6) Sym. functions cSHAKE256

Final numbers

	Speed (ms)	PK (Kbytes)
RSA 3072	4.6	0.8
NIST P-256	1.4	0.1
Kyber	0.07	1.2
FrodoKEM	1.2–2.3	9.5 – 15.4
SIKEp503	10.1	0.4
SIKEp751	30.5	0.6
SIDHp503	10.3	0.4
SIDHp751	31.5	0.6

(Numbers from Patrick Longa's RWC'18 talk, measured on different platforms..)

Thanks

All details can be found at:
https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/SIKE.zip

All authors:
Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev