Computing Isogenies between Montgomery Curves Using the Action of $(0, 0)$

Joost Renes

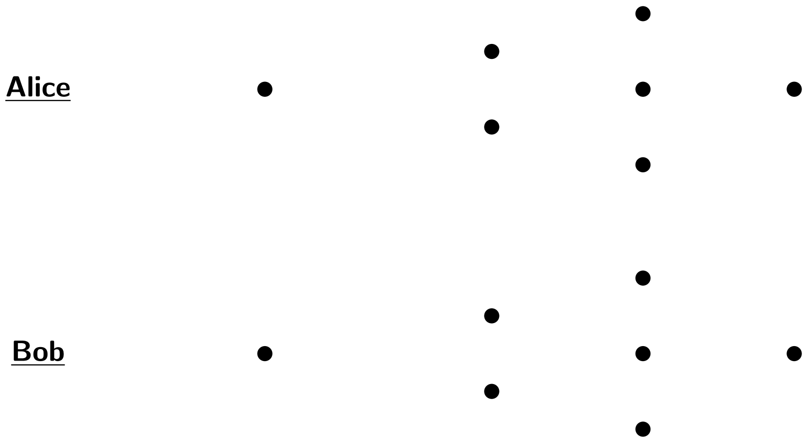
Radboud University, The Netherlands

9 April 2018

Supersingular isogeny-based cryptography

- Proposed by Jao & De Feo [JF11]
- Submitted to NIST competition [Aza+17] (*on Wednesday*)
  - SIDH (passive security)
  - SIKE (active security)
- This talk: *computing isogenies on curves with extra structure*

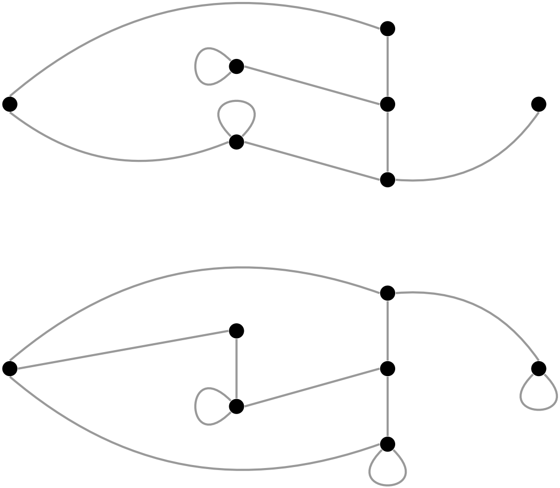
A graph-based protocol



A graph-based protocol

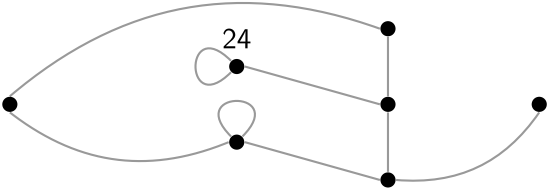
Alice

Bob

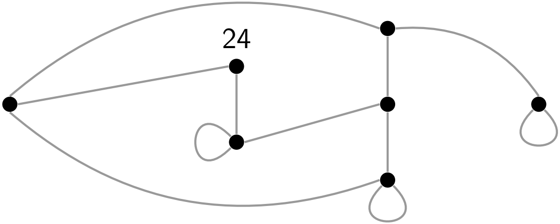


A graph-based protocol

Alice

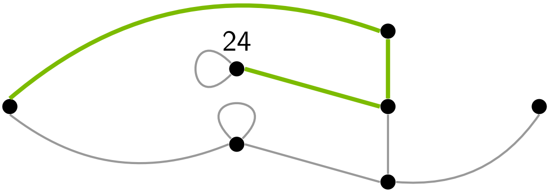


Bob

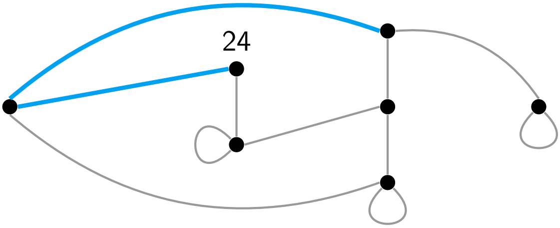


A graph-based protocol

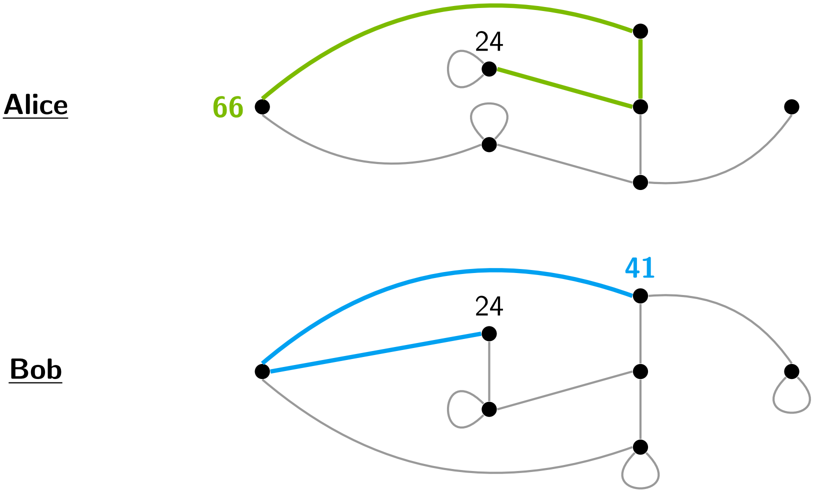
Alice



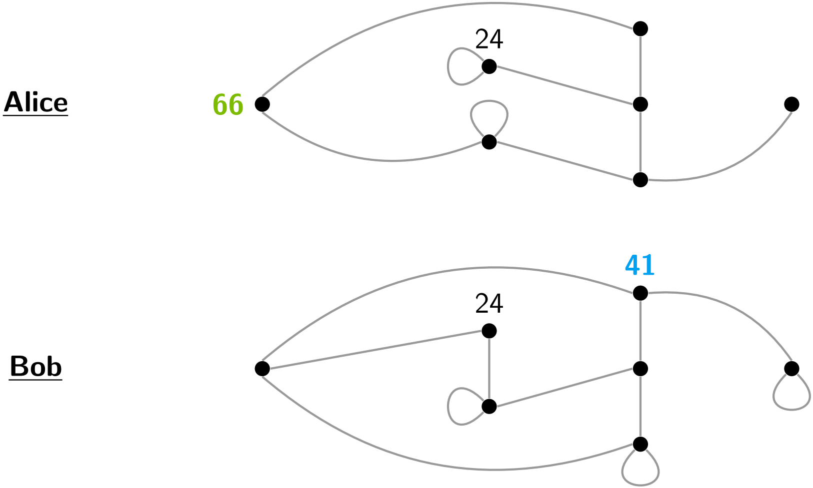
Bob



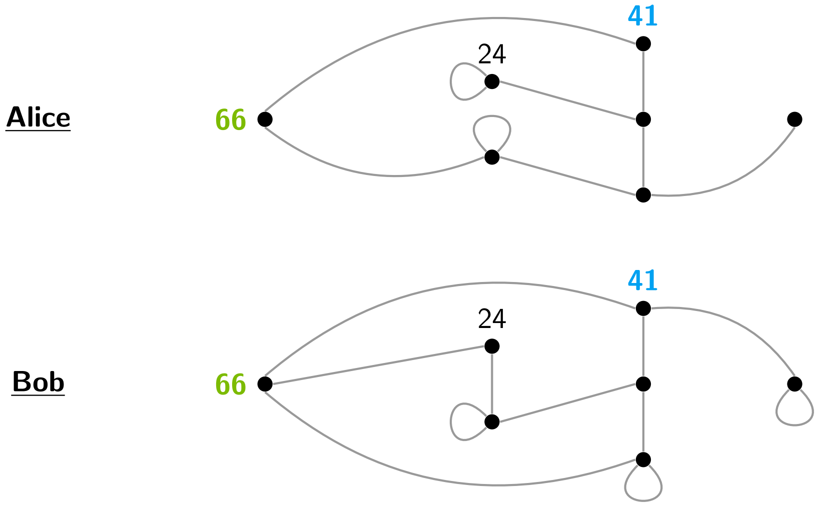
A graph-based protocol



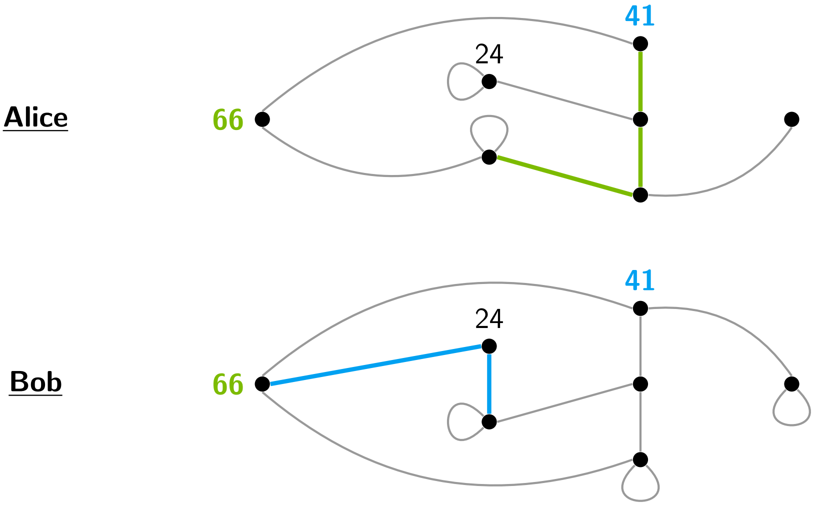
A graph-based protocol



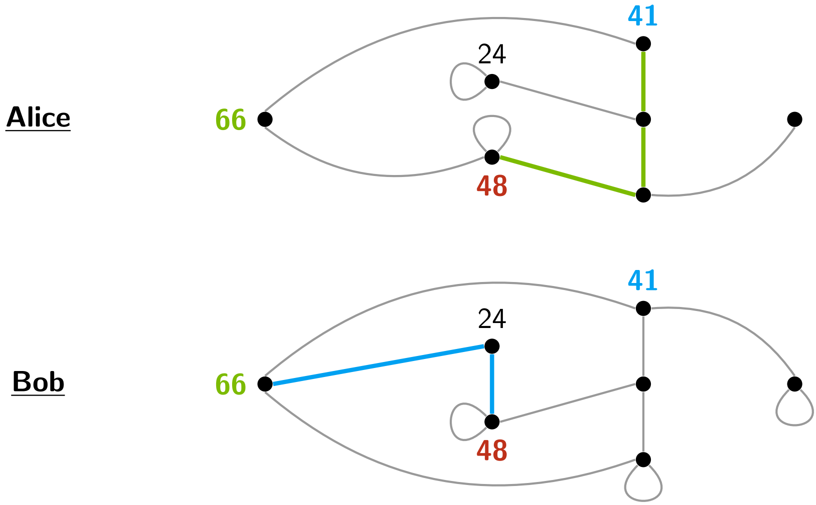
A graph-based protocol



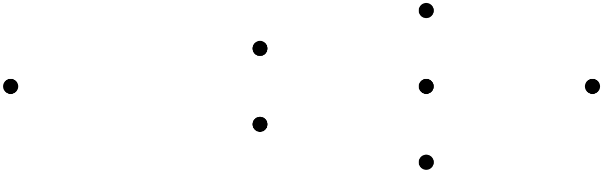
A graph-based protocol



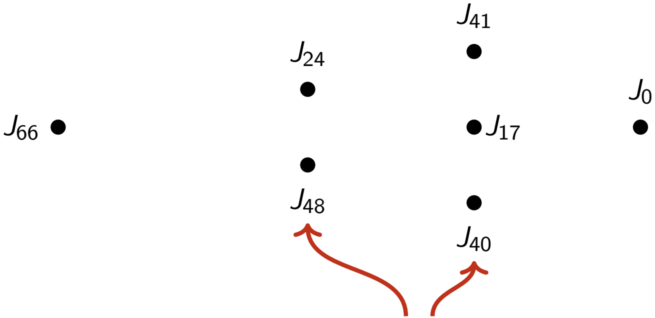
A graph-based protocol



Constructing graphs and walks using isogenies

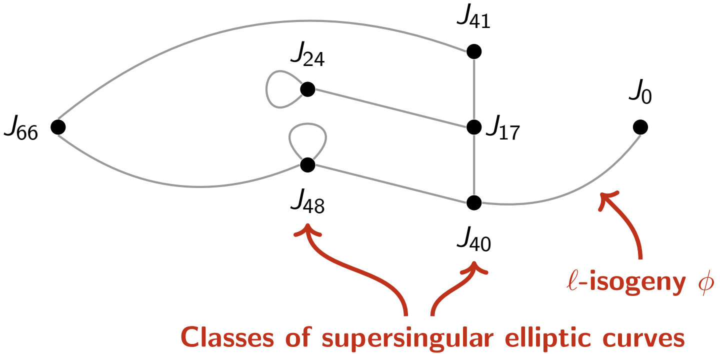


Constructing graphs and walks using isogenies

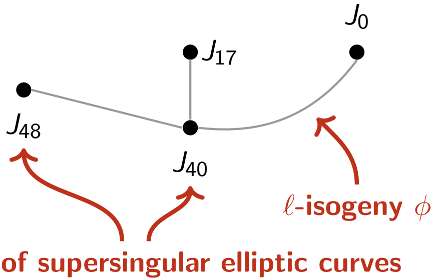


Classes of supersingular elliptic curves

Constructing graphs and walks using isogenies

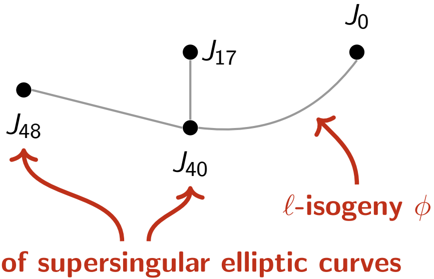


Constructing graphs and walks using isogenies



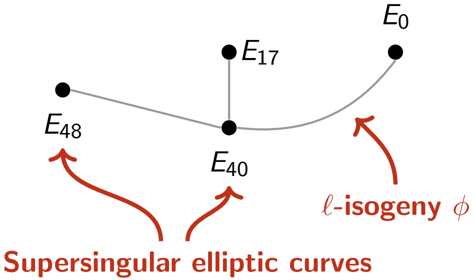
Constructing graphs and walks using isogenies

$$(1) \quad \Phi_\ell(X, Y) = X^{\ell+1} + Y^{\ell+1} + \cdots$$



Constructing graphs and walks using isogenies

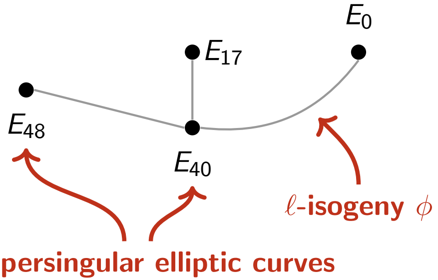
$$\cancel{\Phi_\ell(X, Y) = X^{\ell+1} + Y^{\ell+1} + \cdots} \tag{1}$$



Constructing graphs and walks using isogenies

(1) $\cancel{\Phi_\ell(X,Y) = X^{\ell+1} + Y^{\ell+1} + \cdots}$

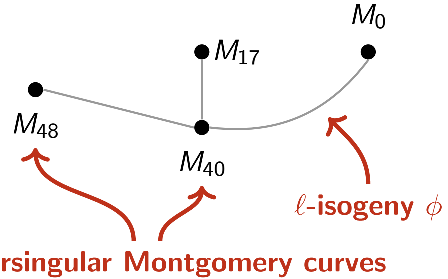
(2) $\ell + 1$ subgroups of order ℓ (Vélu's formulas)



Constructing graphs and walks using isogenies

~~(1) $\Phi_\ell(X, Y) = X^{\ell+1} + Y^{\ell+1} + \cdots$~~

~~(2) $\ell + 1$ subgroups of order ℓ (Vélu's formulas)~~

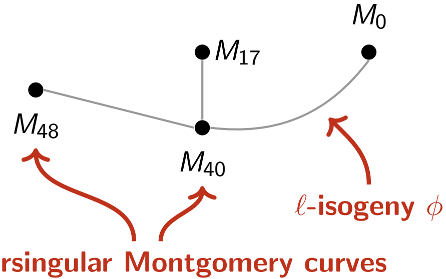


Constructing graphs and walks using isogenies

~~(1) $\Phi_\ell(X, Y) = X^{\ell+1} + Y^{\ell+1} + \cdots$~~

~~(2) $\ell + 1$ subgroups of order ℓ (Vélu's formulas)~~

(3) Costello–Hisil [CH17] for $\ell \geq 3$



Constructing graphs and walks using isogenies

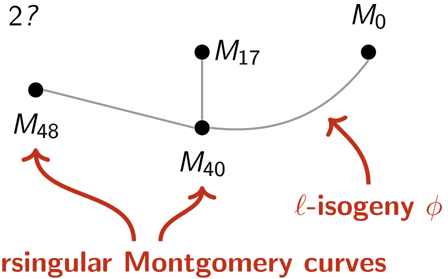
~~(1) $\Phi_\ell(X, Y) = X^{\ell+1} + Y^{\ell+1} + \cdots$~~

~~(2) $\ell + 1$ subgroups of order ℓ (Vélu's formulas)~~

(3) Costello–Hisil [CH17] for $\ell \geq 3$

(Q1) *Where do these formulas come from?*

(Q2) *What about $\ell = 2$?*



What is an isogeny..

(1) A *morphism* of curves

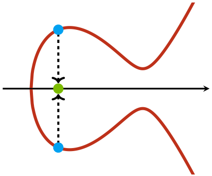
$$M_A(x,y) = 0 \xrightarrow{\quad\quad\phi\quad\quad} M_{A'}(x,y) = 0$$

What is an isogeny..

(1) A *morphism* of curves

$$M_A(x, y) = 0 \xrightarrow{\phi = \left(\frac{f(x)}{g(x)}, \text{—}\right)} M_{A'}(x, y) = 0$$

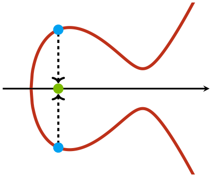
What is an isogeny..



(1) A *morphism* of curves

$$M_A(x,y)=0 \xrightarrow{\phi=\left(\frac{f(x)}{g(x)},\,\text{---}\right)} M_{A'}(x,y)=0$$

What is an isogeny..



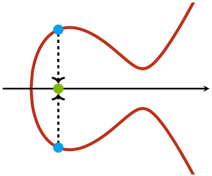
(1) A *morphism* of curves

$$M_A(x,y)=0 \xrightarrow{\phi=\left(\frac{f(x)}{g(x)},—\right)} M_{A'}(x,y)=0$$

(2) A *homomorphism* of groups

$$\begin{array}{ccccc} (x_0,—) & \oplus & (x_1,—) & = & (x_2,—) \\ \big\downarrow & & & & \\ \left(\frac{f(x_0)}{g(x_0)},—\right) & & & & \end{array}$$

What is an isogeny..



(1) A *morphism* of curves

$$M_A(x,y) = 0 \xrightarrow{\phi = \left(\frac{f(x)}{g(x)}, \text{---}\right)} M_{A'}(x,y) = 0$$

(2) A *homomorphism* of groups

$$\begin{array}{ccccc} (x_0, \text{---}) & \oplus & (x_1, \text{---}) & = & (x_2, \text{---}) \\ \downarrow & & \downarrow & & \downarrow \\ \left(\frac{f(x_0)}{g(x_0)}, \text{---}\right) & \oplus & \left(\frac{f(x_1)}{g(x_1)}, \text{---}\right) & = & \left(\frac{f(x_2)}{g(x_2)}, \text{---}\right) \end{array}$$

Describing f and g

Given an isogeny $\phi(x) = \left(\frac{f(x)}{g(x)}, \text{---} \right)$

(1) A point ∞ such that $\phi : \infty \mapsto \infty$. Also

Describing f and g

Given an isogeny $\phi(x) = \left(\frac{f(x)}{g(x)}, — \right)$

(1) A point ∞ such that $\phi : \infty \mapsto \infty$. Also

$$(x_T, —) \mapsto \infty \iff g(x_T) = 0$$

Describing f and g

Given an isogeny $\phi(x) = \left(\frac{f(x)}{g(x)}, \text{—} \right)$

(1) A point ∞ such that $\phi : \infty \mapsto \infty$. Also

$$(x_T, \text{—}) \mapsto \infty \iff g(x_T) = 0$$

$$\implies g(x) \approx \prod_{T \in \ker \phi} (x - x_T)$$

Describing f and g

Given an isogeny $\phi(x) = \left(\frac{f(x)}{g(x)}, — \right)$

(1) A point ∞ such that $\phi : \infty \mapsto \infty$. Also

$$(x_T, —) \mapsto \infty \iff g(x_T) = 0$$

$$\implies g(x) \approx \prod_{T \in \ker \phi} (x - x_T)$$

(2) A point $Q \in M_A$ such that $f(x_Q) = 0$

Describing f and g

Given an isogeny $\phi(x) = \left(\frac{f(x)}{g(x)}, — \right)$

(1) A point ∞ such that $\phi : \infty \mapsto \infty$. Also

$$(x_T, —) \mapsto \infty \iff g(x_T) = 0$$

$$\implies g(x) \approx \prod_{T \in \ker \phi} (x - x_T)$$

(2) A point $Q \in M_A$ such that $f(x_Q) = 0$

$$\implies f(x_{T+Q}) = 0 \text{ for all } T \in \ker \phi$$

Describing f and g

Given an isogeny $\phi(x) = \left(\frac{f(x)}{g(x)}, — \right)$

(1) A point ∞ such that $\phi : \infty \mapsto \infty$. Also

$$(x_T, —) \mapsto \infty \iff g(x_T) = 0$$

$$\implies g(x) \approx \prod_{T \in \ker \phi} (x - x_T)$$

(2) A point $Q \in M_A$ such that $f(x_Q) = 0$

$$\implies f(x_{T+Q}) = 0 \text{ for all } T \in \ker \phi$$

$$\implies f(x) \approx \prod_{T \in \ker \phi} (x - x_{T+Q})$$

Isogeny structure

Theorem (sketch)

Let $G \subset M(\bar{K})$ be a subgroup, $Q \notin G$ and

$$\phi = \left(\frac{f(x)}{g(x)}, - \right)$$

a separable isogeny such that $\ker \phi = G$ *and* $f(x_Q) = 0$. *Then*

$$f(x) = c_f \cdot \prod_{T \in G} (x - x_{T+Q}), \quad g(x) = \prod_{T \in G \setminus \infty} (x - x_T).$$

Isogeny structure

Theorem (sketch)

Let $G \subset M(\bar{K})$ be a subgroup, $Q \notin G$ and

$$\phi = \left(\frac{f(x)}{g(x)}, \text{---} \right)$$

a separable isogeny such that $\ker \phi = G$ *and* $f(x_Q) = 0$. *Then*

$$f(x) = c_f \cdot \prod_{T \in G} (x - x_{T+Q}), \quad g(x) = \prod_{T \in G \setminus \infty} (x - x_T).$$

- Generalizes when Q does not map to $(0, \text{---})$

Isogeny structure

Theorem (sketch)

Let $G \subset M(\bar{K})$ be a subgroup, $Q \notin G$ and

$$\phi = \left(\frac{f(x)}{g(x)}, -\right)$$

a separable isogeny such that $\ker\phi = G$ and $f(x_Q) = 0$. Then

$$f(x) = c_f \cdot \prod_{T \in G} (x - x_{T+Q}), \quad g(x) = \prod_{T \in G \setminus \infty} (x - x_T).$$

- Generalizes when Q does not map to $(0, -)$
- Close connection between action of Q and isogeny!

Application to Montgomery curves

This works perfectly for Montgomery curves!

(1) A distinguished point $Q = (0, 0)$ of order two

(2) A very simple action $(x_T, —) + Q = \left(\frac{1}{x_T}, —\right)$

Application to Montgomery curves

This works perfectly for Montgomery curves!

(1) A distinguished point $Q = (0, 0)$ of order two

(2) A very simple action $(x_T, —) + Q = \left(\frac{1}{x_T}, —\right)$

$$\implies \phi(x) = \left(x \prod_{T \in G \setminus \infty} \frac{x \cdot x_T - 1}{x - x_T}, — \right)$$

Application to Montgomery curves

This works perfectly for Montgomery curves!

(1) A distinguished point $Q = (0, 0)$ of order two

(2) A very simple action $(x_T, —) + Q = \left(\frac{1}{x_T}, —\right)$

$$\implies \phi(x) = \left(x \prod_{T \in G \setminus \infty} \frac{x \cdot x_T - 1}{x - x_T}, — \right)$$

and $A' = \pi(A - 3\sigma)$, where

$$\pi = \prod_{T \in G \setminus \infty} x_T \,, \quad \sigma = \prod_{T \in G \setminus \infty} x_T - \frac{1}{x_T}$$

Application to Montgomery curves

This works perfectly for Montgomery curves!

(1) A distinguished point $Q = (0,0)$ of order two

(2) A very simple action $(x_T, —) + Q = \left(\frac{1}{x_T}, —\right)$

$$\implies \phi(x) = \left(x \prod_{T \in G \setminus \infty} \frac{x \cdot x_T - 1}{x - x_T}, — \right)$$

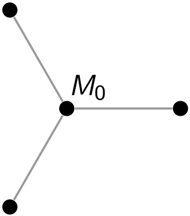
and $A' = \pi(A - 3\sigma)$, where

$$\pi = \prod_{T \in G \setminus \infty} x_T \,, \quad \sigma = \prod_{T \in G \setminus \infty} x_T - \frac{1}{x_T}$$

for *any subgroup* not containing $(0,0)$, generalizing [CH17]

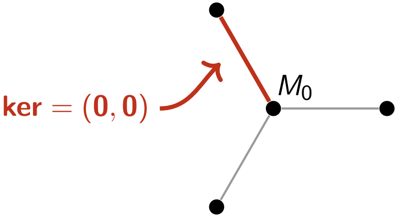
Isogenies of degree two..

A curve has three points of order two, one of which is $(0, 0)$



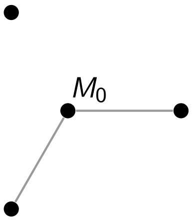
Isogenies of degree two..

A curve has three points of order two, one of which is $(0, 0)$



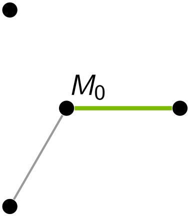
Isogenies of degree two..

A curve has three points of order two, one of which is $(0, 0)$



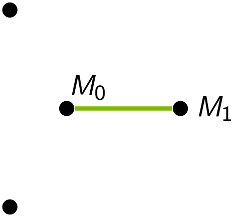
Isogenies of degree two..

A curve has three points of order two, one of which is $(0,0)$



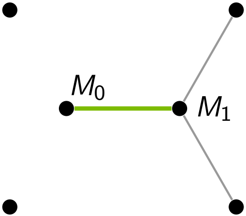
Isogenies of degree two..

A curve has three points of order two, one of which is $(0,0)$



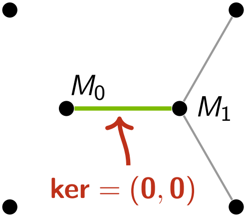
Isogenies of degree two..

A curve has three points of order two, one of which is $(0,0)$



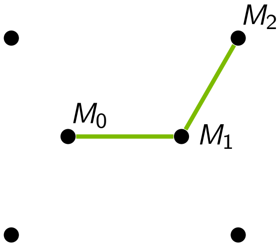
Isogenies of degree two..

A curve has three points of order two, one of which is $(0, 0)$



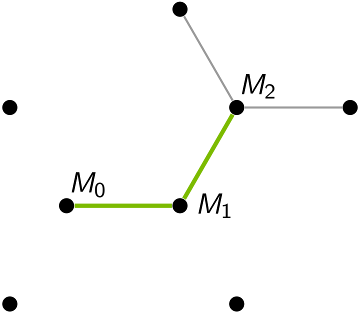
Isogenies of degree two..

A curve has three points of order two, one of which is $(0, 0)$



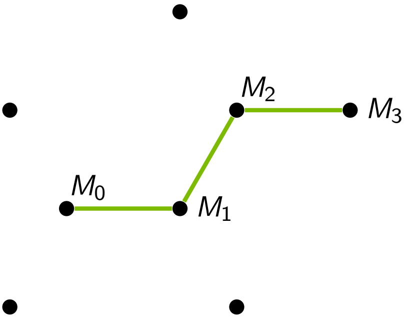
Isogenies of degree two..

A curve has three points of order two, one of which is $(0, 0)$



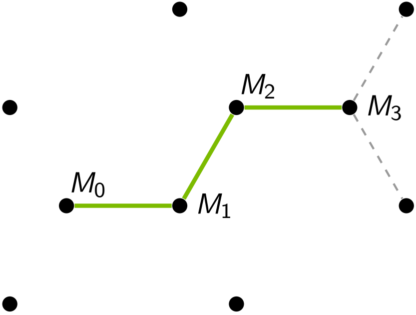
Isogenies of degree two..

A curve has three points of order two, one of which is $(0, 0)$



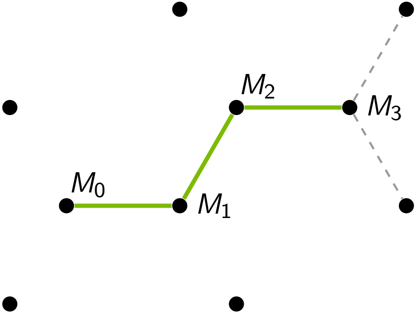
Isogenies of degree two..

A curve has three points of order two, one of which is $(0,0)$



Isogenies of degree two..

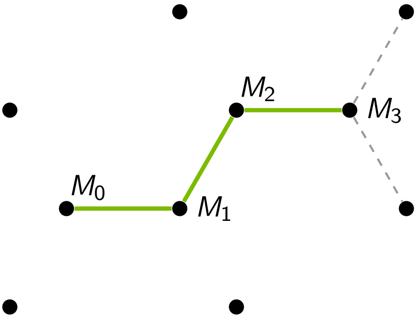
A curve has three points of order two, one of which is $(0,0)$



	2×2-isogeny	**4-isogeny**
Co-domain	$4\mathbf{S}$	$4\mathbf{S}+\mathbf{a}$

Isogenies of degree two..

A curve has three points of order two, one of which is $(0,0)$



	2×2-isogeny	**4-isogeny**
Co-domain	$4\mathbf{S}$	$4\mathbf{S} + \mathbf{a}$
Evaluate	$8\mathbf{M} + 12\mathbf{a}$	$6\mathbf{M} + 2\mathbf{S} + 10\mathbf{a}$

Other curve models..

- Apply to *Tate Normal Form*
  - $y^2 + axy + by = x^3 + cx^2$
  - Point $Q = (0,0)$ of order ℓ
- For ℓ have $b = c = 0$ and

$$(x_T, y_T) + (0,0) = \left(\frac{-y_T}{x_T^2}, \frac{-y_T}{x_T^3} \right) .$$

  Results (currently) not better than Montgomery!
- Other models..?

Thanks for your attention!

`http://www.cs.ru.nl/~jrenes/`

References I

[Aza+17] Reza Azarderakhsh, Matthew Campagna, Craig Costello, Luca De Feo, Basil Hess, Amir Jalali, David Jao, Brian Koziel, Brian LaMacchia, Patrick Longa, Michael Naehrig, Joost Renes, Vladimir Soukharev and David Urbanik. *Supersingular Isogeny Key Encapsulation – Submission to the NIST's Post-Quantum Cryptography Standardization Process*. Available at `https://csrc.nist.gov/CSRC/media/Projects/Post-Quantum-Cryptography/documents/round-1/submissions/SIKE.zip`. 2017.

[CH17] Craig Costello and Hüseyin Hisil. "A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies". In: *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*. 2017, pp. 303–329.

References II

[JF11] David Jao and Luca De Feo. "Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies". In: *Post-Quantum Cryptography (PQCrypto 2011)*. Ed. by Bo-Yin Yang. Vol. 7071. Lecture Notes in Computer Science. Springer, 2011, pp. 19–34.