A simple and compact algorithm for
SIDH with arbitrary degree isogenies

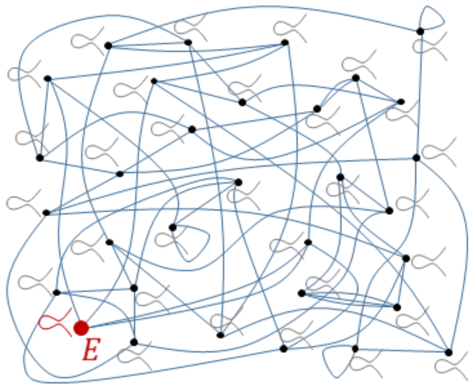
Craig Costello and Huseyin Hisil

December 5, 2017
ASIACRYPT
Hong Kong, China

INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH

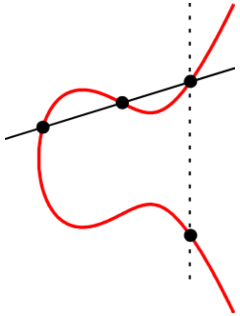
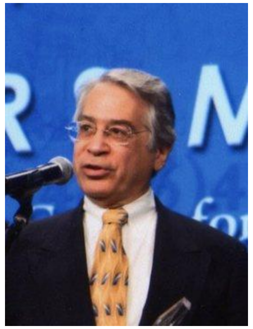
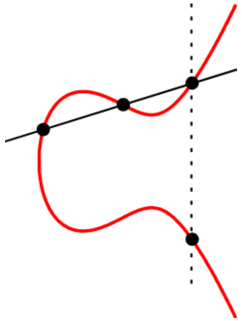
Microsoft Research

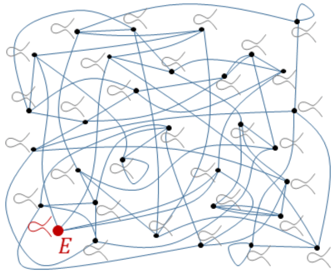
YASAR UNIVERSITY

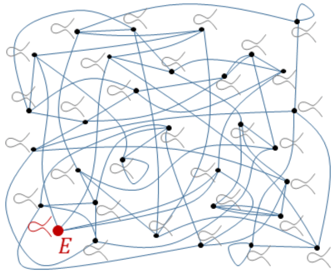


Diffie-Hellman instantiations

$\mathbb{Z}_q^*$  $g^a \bmod q$ / $g^b \bmod q$  $\mathbb{Z}_q^*$

  $[a]P$ / $[b]P$  



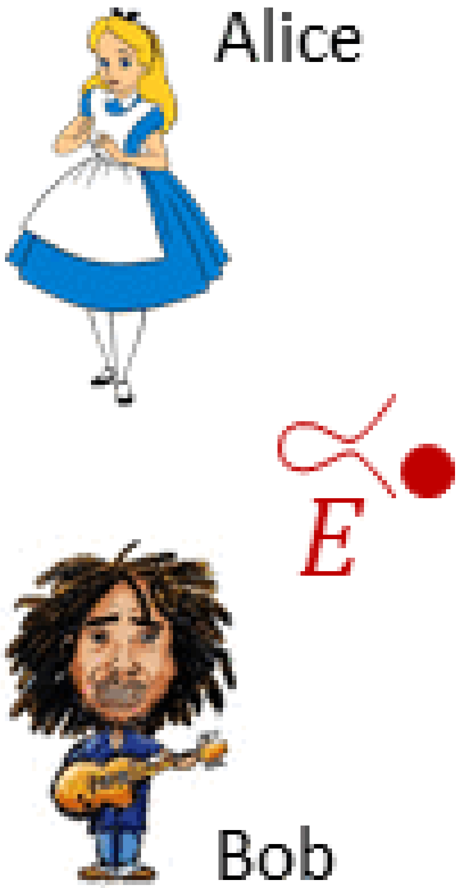
 $\phi_A(E)$ / $\phi_B(E)$  

Diffie-Hellman instantiations

	DH	ECDH	SIDH
Elements	integers g modulo prime	points P in curve group	curves E in isogeny class
Secrets	exponents x	scalars k	isogenies ϕ
computations	$g, x \mapsto g^x$	$P, k \mapsto [k]P$	$E, \phi \mapsto \phi(E)$
hard problem	given g, g^x find x	given $P, [k]P$ find k	given $E, \phi(E)$ find ϕ

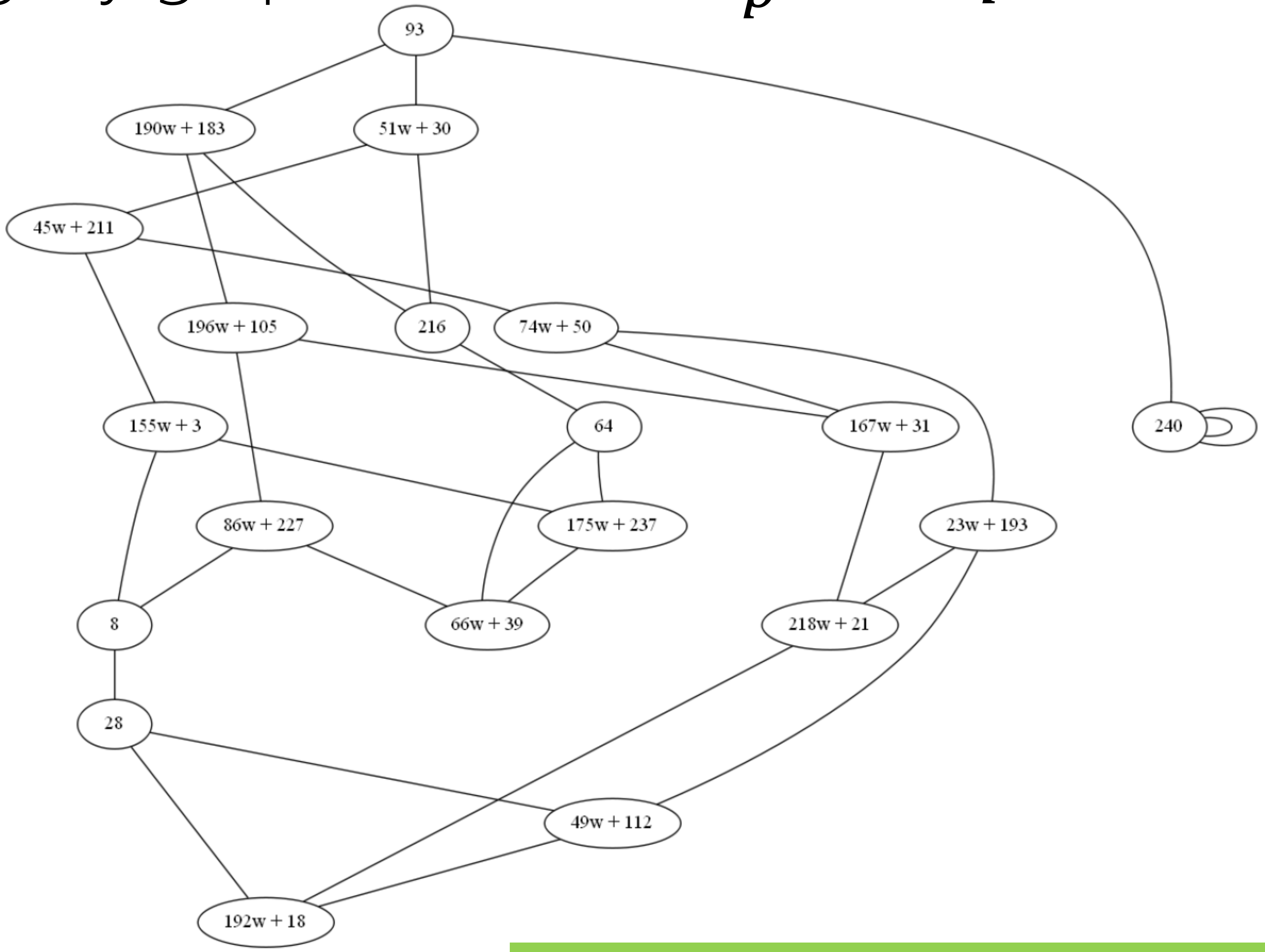
Setup: supersingular isogeny class over $\mathbb{F}_{p^2}$ …

roughly $p/12$ isomorphism classes within supersingular isogeny class…



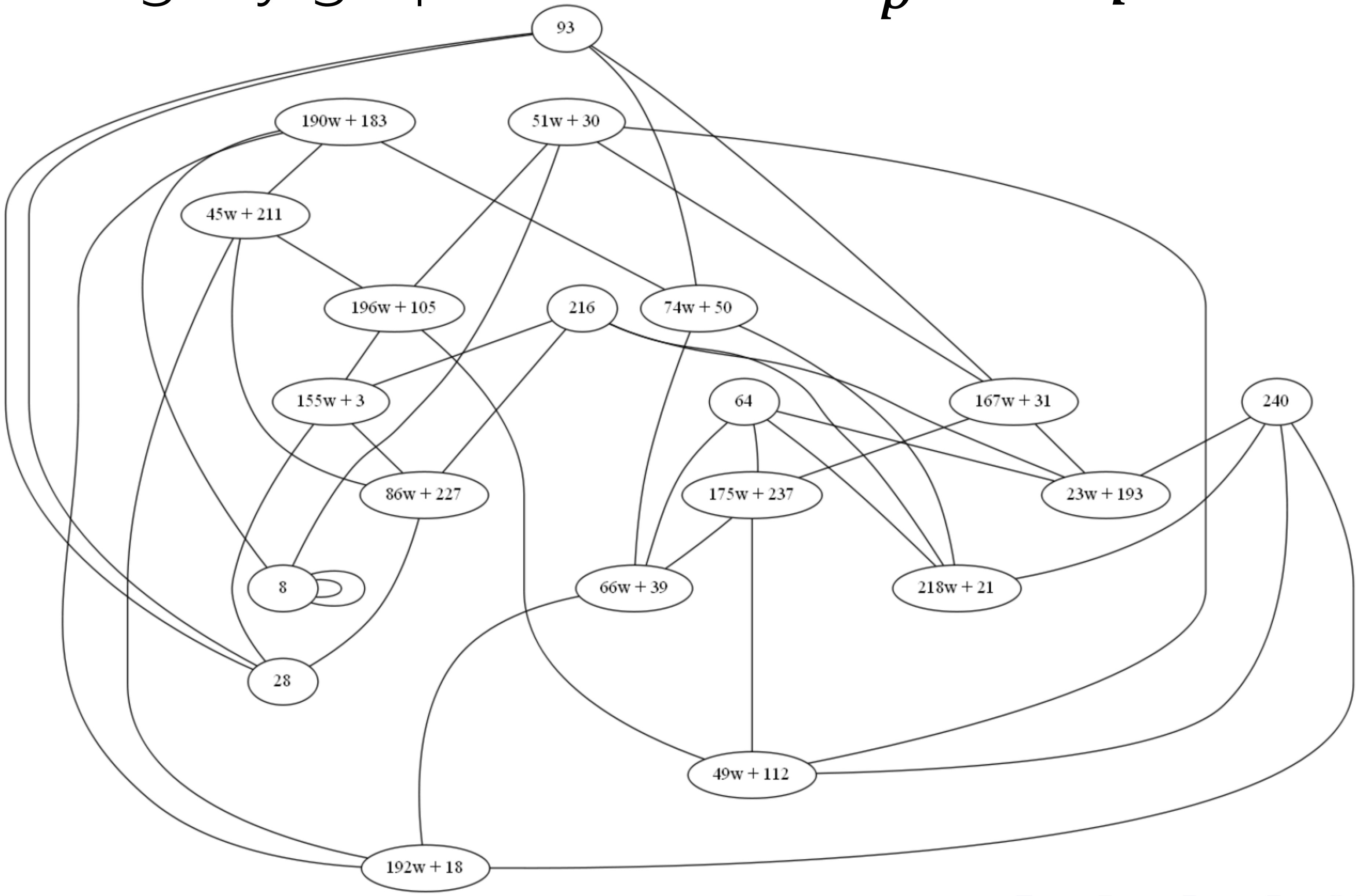
W. Castryck (GIF): "Elliptic curves are dead: long live elliptic curves" https://www.esat.kuleuven.be/cosic/?p=7404

Supersingular isogeny graph for $\ell = 2$: $\mathbb{F}_{p^2}$ with $p = 241$



Credit to Fre Vercauteren for example and pictures…

Supersingular isogeny graph for $\ell = 3$: $\mathbb{F}_{p^2}$ with $p = 241$



Credit to Fre Vercauteren for example and pictures…

(separable) isogenies ↔ subgroups

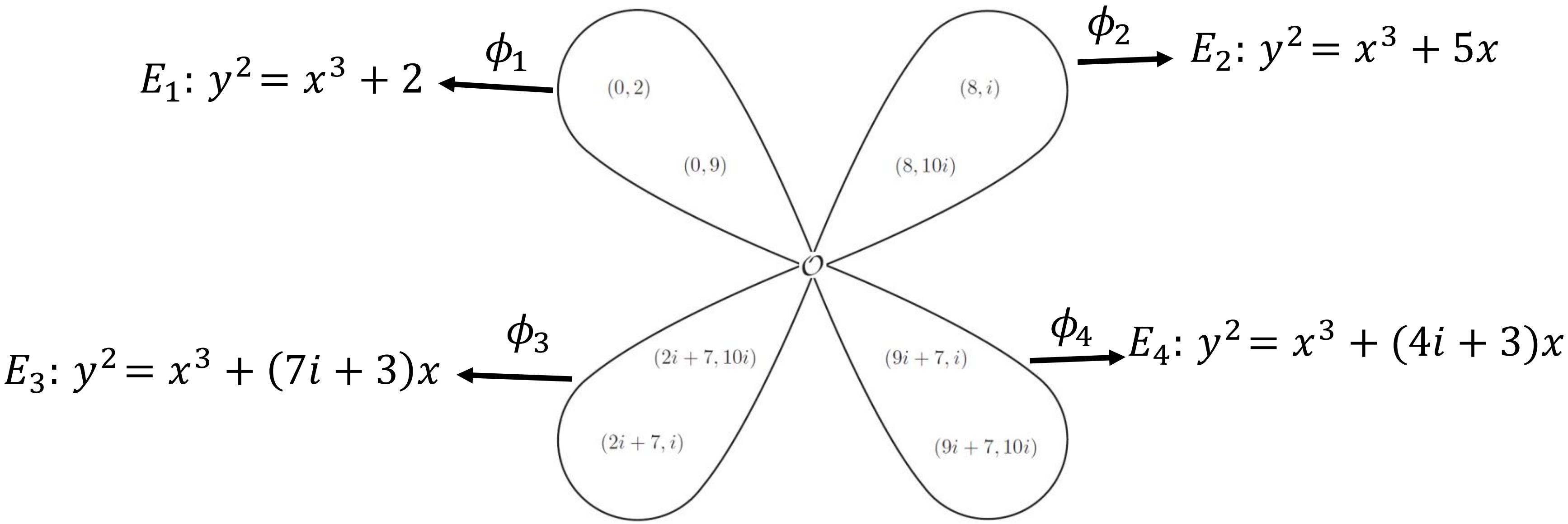
- An isogeny is a group homomorphism from E to E'

- Any finite subgroup $G \in E$, determines unique isogeny

$$\phi : \quad E \to E/G$$

- SIDH currently uses cyclic isogenies of degree $d = 2$ and $d = 3$
e.g.,

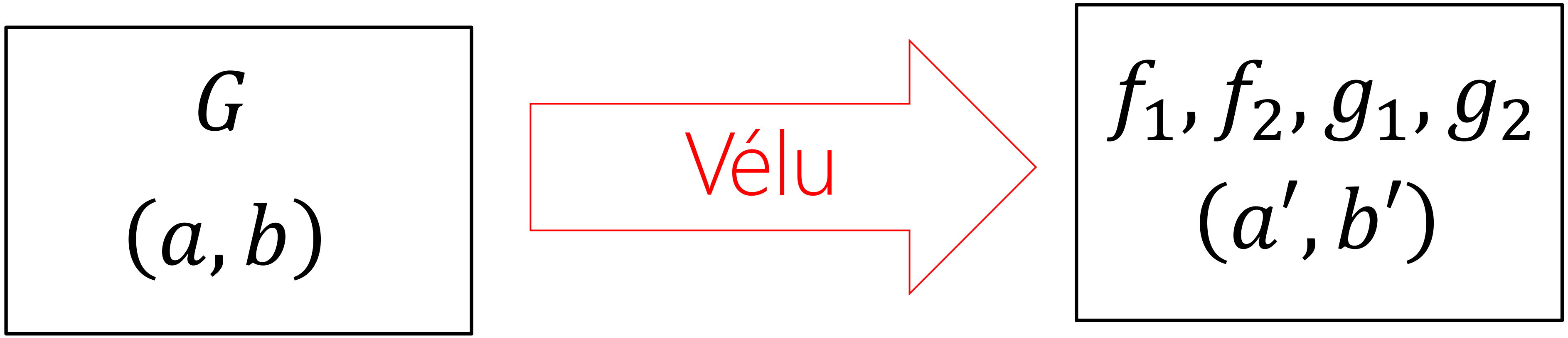
$$E/\mathbb{F}_{11^2}: y^2 = x^3 + 4$$
$$\#E(\mathbb{F}_{11^2}) = 12^2$$
$$d = 3$$



Computing isogenies with Vélu's formulas

- Consider the isogeny $\phi : E \to E/G, \quad (x,y) \mapsto \left(\frac{f_1(x,y)}{g_1(x,y)}, \frac{f_2(x,y)}{g_2(x,y)}\right)$

$$E : y^2 = x^3 + ax + b$$
$$E/G : y^2 = x^3 + a'x + b'$$



In SIDH: we need to compute the isogenous curve and evaluate isogenies at points

Point *and* isogeny arithmetic in $\mathbb{P}^1$

$$E_{a,b} : \quad by^2 = x^3 + ax^2 + x$$

$(x, y) \leftrightarrow (X : Y : Z)$

$(a, b) \leftrightarrow (A : B : C)$

$$E_{A/C\,,B/C}: \quad BY^2Z = CX^3 + AX^2Z + CXZ^2$$

$\mathbb{P}^1$ point arithmetic: $(X : Z) \mapsto (X' : Z')$

$\mathbb{P}^1$ isogeny arithmetic: $(A : C) \mapsto (A' : C')$

Motivation

$\mathbf{2}^{e}$ and $\mathbf{3}^{e}$ isogenies (on Montgomery curves) have been studied, but what about odd $\boldsymbol{\ell}^{e}$ for $\boldsymbol{\ell} \geq \mathbf{5}$?

Problems with Vélu's formulas on Montgomery curves…

- Let E be Montgomery. For the odd cyclic isogeny $\phi: \ E \to E/\langle P \rangle =: E'$, $\quad (x,y) \mapsto (X,Y)$, Vélu's formula says

$$X = x + \sum_{Q \in \langle P \rangle} 2 \cdot \frac{3x_Q^2 + 2Ax_Q + 1}{x - x_Q} + \frac{4y_Q^2}{(x - x_Q)^2}, \quad Y = y - \sum_{Q \in \langle P \rangle} \frac{8y_Q^2 y}{(x - x_Q)^3} + 2 \cdot (3x_Q^2 + 2Ax_Q + 1) \cdot \frac{(y + y_Q)}{(x - x_Q)^2}$$

- Vélu's formula also says that

$$E' : By^2 = x^3 + A_2 x^2 + A_4 x + A_6, \qquad A_4 \neq 1 \text{ and } A_6 \neq 0$$

(i.e., that the image curve is not Montgomery)

- Can (always) use isomorphism to convert E' to Montgomery form, but in general this requires root-finding

Theorem 1

Let P have odd order ℓ on Montgomery curve $E/K\colon By^2 = x^3 + Ax^2 + x$, and let $\phi : E \to E'$ with $E' = E/\langle P \rangle$. Then

$$\phi : (x, y) \mapsto \big(f(x), y \cdot f'(x)\big)$$

$$f(x) = x \cdot \prod_{1 \le i \le \ell - 1} \left(\frac{x \cdot x_{[i]P} - 1}{x - x_{[i]P}} \right)$$

$$E'\colon \quad B'y^2 = x^3 + A'x^2 + x$$

where $\quad A' = (6 \cdot \tilde{\sigma} - 6 \cdot \sigma + A) \cdot \pi^2$

$$B' = B \cdot \pi^2$$

with $\pi = \prod x_{[i]P}$, $\sigma = \sum x_{[i]P}$, $\tilde{\sigma} = \sum 1/x_{[i]P}$

Theorem 1 in the context of SIDH

Recall that in SIDH we only care about the $\boldsymbol{x}$-coordinate and $\boldsymbol{A}$ coefficient

$$\phi : E/\langle \ominus \rangle \to E'/\langle \ominus \rangle$$

$$x \mapsto x \cdot \prod_{1 \leq i \leq \ell - 1} \left(\frac{x \cdot x_{[i]P} - 1}{x - x_{[i]P}} \right)$$

$$A' = (6 \cdot \tilde{\sigma} - 6 \cdot \sigma + A) \cdot \pi^2$$

Theorem 1 in the context of SIDH

Recall that in SIDH we only care about the x-coordinate and $\boldsymbol{A}$ coefficient

$$\phi : E/\langle\ominus\rangle \to E'/\langle\ominus\rangle$$

$$x \mapsto x \cdot \prod_{\substack{1 \le i \le d \\ d=(\ell-1)/2}} \left(\frac{x \cdot x_{[i]P} - 1}{x - x_{[i]P}}\right)^2$$

$$x_{[i]P} = x_{[\ell-i]P}$$

$$A' = (6 \cdot \tilde{\sigma} - 6 \cdot \sigma + A) \cdot \pi^2$$

Theorem 1 in the context of SIDH

Recall that in SIDH we only care about the x-coordinate and A coefficient

$$\phi : E/\langle\ominus\rangle \to E'/\langle\ominus\rangle$$

$$(X : Z) \mapsto (X' : Z')$$

$$X' = X \cdot \left(\prod_i (X \cdot X_{[i]P} - Z_{[i]P} \cdot Z)\right)^2 \qquad Z' = Z \cdot \left(\prod_i (X \cdot Z_{[i]P} - X_{[i]P} \cdot Z)\right)^2$$

$$A' = (6 \cdot \tilde{\sigma} - 6 \cdot \sigma + A) \cdot \pi^2$$

with $\pi = \prod X_{[i]P}/Z_{[i]P}$, $\sigma = \sum X_{[i]P}/Z_{[i]P}$, $\tilde{\sigma} = \sum Z_{[i]P}/X_{[i]P}$

Theorem 1 in the context of SIDH

$$X' = X \cdot \left(\prod_i \Big((X - Z)\left(X_{[i]P} + Z_{[i]P}\right) + (X + Z)(X_{[i]P} - Z_{[i]P}) \Big) \right)^2$$

$$Z' = Z \cdot \left(\prod_i \Big((X - Z)\left(X_{[i]P} + Z_{[i]P}\right) - (X + Z)(X_{[i]P} - Z_{[i]P}) \Big) \right)^2$$

The simple and compact algorithm

Input: $\boldsymbol{x}(P) = (X_P : Z_P)$ and $\boldsymbol{x}(Q) = (X : Z)$ with $Q \notin \langle P \rangle$

Output: $\boldsymbol{x}(\phi(Q)) = (X_{\phi(Q)} : Z_{\phi(Q)})$ where $\ker(\phi) = \langle P \rangle$

Initialise: $T \leftarrow O_{E'}$, $X' \leftarrow 1$, $Z' \leftarrow 1$

for $i \in [1..d]$ do

$$(X_T : Z_T) = \boldsymbol{x}(T + P)$$
$$X' \leftarrow X' \cdot \big((X - Z) \cdot (X_T + Z_T) + (X + Z) \cdot (X_T - Z_T)\big)$$
$$Z' \leftarrow Z' \cdot \big((X - Z) \cdot (X_T + Z_T) - (X + Z) \cdot (X_T - Z_T)\big)$$

end for

return $(X \cdot X'^2 : Z \cdot Z'^2)$

$|\langle P \rangle| = 2d + 1$

What about computing the isogenous curve?

- Recall that the isogenous Montgomery curve has coefficient

$$A' = (6 \cdot \tilde{\sigma} - 6 \cdot \sigma + A) \cdot \pi^2$$

with $\pi = \prod X_{[i]P}/Z_{[i]P}$, $\sigma = \sum X_{[i]P}/Z_{[i]P}$, $\tilde{\sigma} = \sum Z_{[i]P}/X_{[i]P}$

- Relative to computing $x(P) \mapsto x(\phi(P))$, computing $A \mapsto A'$ becomes much more expensive as ℓ grows large…

- But for Montgomery curves, $A = -\alpha - 1/\alpha$ where $(\alpha, 0)$ is a point of order 2, so we can compute $(\alpha' : 0) = \phi((\alpha : 0))$ and recover $A' = -\alpha' - 1/\alpha'$ instead

- Now we only need one function for computing ℓ-isogenies on curves and points!

Upshot…

- Performance slowly degrades for odd ℓ-isogenies as ℓ increases, but not *too* bad…

- In traditional ECC, we are free to cherry-pick ***fastest*** prime characteristics, e.g.,

$$p = 2^{127} - 1, \qquad p = 2^{255} - 19, \qquad p = 2^{448} - 2^{224} - 1$$

- In SIDH, we are currently forced to choose much slower primes, like

$$p = 2^{250}3^{159} - 1, \qquad p = 2^{372}3^{239} - 1, \qquad p = 2^{486}3^{301} - 1$$

- Bos-Friedberger'17 get faster results for $p = 2^{391}19^{88} - 1$ than for $p = 2^{372}3^{239} - 1$, so the bottleneck party (e.g., server) computing 2-isogenies could be faster overall

- $p = 2^{448} - 2^{224} - 1$ and $p = 2^{480} - 2^{240} - 1$ are *almost** SIDH-friendly, e.g., $(p + 1) = 2^{224} \cdot \prod_i p_i^{e_i}$, but the larger p_i are just too big… is there some nice middle ground?

** Depends heavily on your definition of almost*

Some related stuff…

- Moody-Shumow had already figured this out in the case of (twisted) Edwards curves: see https://eprint.iacr.org/2011/430 👍

- Renes has, among several other things, recently solved the last piece of the Montgomery isogeny puzzle: efficient $\mathbf{2}$-isogenies 👍

- SIKE – supersingular isogeny key encapsulation was submitted to NIST last week. More work needed! 👍

Questions?