An introduction to isogeny-based crypto

Chloe Martindale

Technische Universiteit Eindhoven
PQCrypto Summer School 2017

July 3, 2017

Diffie-Hellman key exchange

- Let S be a set (e.g. $\mathbb{F}_p$ or $E(\mathbb{F}_p)$).
- Let G be a group (e.g. $\mathbb{Z}$) that *acts* on S as

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (a, x) & \mapsto & a * x \end{array}$$

Diffie-Hellman key exchange

- Let S be a set (e.g. $\mathbb{F}_p$ or $E(\mathbb{F}_p)$).
- Let G be a group (e.g. $\mathbb{Z}$) that *acts* on $\mathbb{F}_p$ as

$$\begin{array}{ccc} \mathbb{Z} \times \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ (a, x) & \mapsto & x^a \end{array}$$

Diffie-Hellman key exchange

- Let S be a set (e.g. $\mathbb{F}_p$ or $E(\mathbb{F}_p)$).
- Let G be a group (e.g. $\mathbb{Z}$) that *acts* on $E(\mathbb{F}_p)$ as

$$\begin{array}{ccc} \mathbb{Z} \times E(\mathbb{F}_p) & \longrightarrow & E(\mathbb{F}_p) \\ (n, P) & \mapsto & nP \end{array}$$

Diffie-Hellman key exchange

- Let S be a set (e.g. $\mathbb{F}_p$ or $E(\mathbb{F}_p)$).
- Let G be a group (e.g. $\mathbb{Z}$) that *acts* on S as

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (a, x) & \mapsto & a * x \end{array}$$

a

$a*(b*x)$

x

$a*x$

$\longrightarrow$

$b*x$

$\longleftarrow$

b

$b*(a*x)$

- $k = a*(b*x) = b*(a*x)$

Diffie-Hellman key exchange

- Let S be a set (e.g. $\mathbb{F}_p$ or $E(\mathbb{F}_p)$).
- Let G be a group (e.g. $\mathbb{Z}$) that *acts* on S as

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (a, x) & \mapsto & a * x \end{array}$$

x

$a{*}x$

$\longrightarrow$

$b{*}x$

$\longleftarrow$

a

$a{*}(b{*}x)$

b

$b{*}(a{*}x)$

- $k = a{*}(b{*}x) = b{*}(a{*}x)$
- Finding a or b given x, $a{*}x$, and $b{*}x$ should be *hard*!

Quantum-hard Diffie-Hellman

- Classical Diffie-Hellman: $S = \mathbb{F}_p$ and $G = \mathbb{Z}$ with $(a, x) \mapsto x^a$ is not hard enough with a quantum computer.
- Elliptic Curve Diffie-Hellman: $S = E(\mathbb{F}_p)$ and $G = \mathbb{Z}$ with $(n, P) \mapsto nP$ is not hard enough with a quantum computer.
- *Supersingular Isogeny Diffie-Hellman* has a chance of being quantum secure! What is it?

Definition

Let q be a prime power such that $2, 3 \not| q$. We define an elliptic curve over $\mathbb{F}_q$ to be a curve of the form

$$y^2 = x^3 + ax + b,$$

where a and b are elements of $\mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.

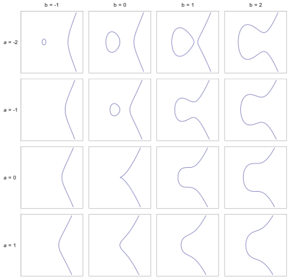
Elliptic Curves

Definition

Let q be a prime power such that $2, 3 \not| q$. We define an elliptic curve over $\mathbb{F}_q$ to be a curve of the form

$$y^2 = x^3 + ax + b,$$

where a and b are elements of $\mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.



Elliptic Curves

Definition

Let q be a prime power such that $2, 3 \not| q$. We define an elliptic curve over $\mathbb{F}_q$ to be a curve of the form

$$y^2 = x^3 + ax + b,$$

where a and b are elements of $\mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.

Definition

The *j-invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is given by

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

This defines E up to $\overline{\mathbb{F}_q}$-isomorphism.

Elliptic Curves

The *j-invariant* of an elliptic curve $E : y^2 = x^3 + ax + b$ is given by

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

Example

Define

$$E/\mathbb{F}_{11} : y^2 = x^3 + x + 1.$$

Then $j(E) = 1728 \frac{4}{31} \equiv 9$. Try the isomorphism $(x, y) \mapsto (4x, 8y)$:

$$(8y)^2 = (4x)^3 + 4x + 1.$$

Divide by 64:

$$E'/\mathbb{F}_{11} : y^2 = x^3 + 9x + 5.$$

$$j(E') = 1728 \frac{4 \cdot 9^3}{4 \cdot 9^3 + 27 \cdot 5^2} \equiv 9.$$

Back to Diffie-Hellman

- Let S be a set (e.g. $\mathbb{F}_p$ or $E(\mathbb{F}_p)$).
- Let G be a group (e.g. $\mathbb{Z}$) that *acts* on S as

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (a, x) & \mapsto & a * x \end{array}$$

a

$a{*}(b{*}x)$

x

$a{*}x$

$\longrightarrow$

$b{*}x$

$\longleftarrow$

b

$b{*}(a{*}x)$

Back to Diffie-Hellman

- Let $S = \{j(E_1), \ldots, j(E_n)\}$ be the set of j-invariants of elliptic curves over $\mathbb{F}_q$.
- We need a group G that *acts* on S as

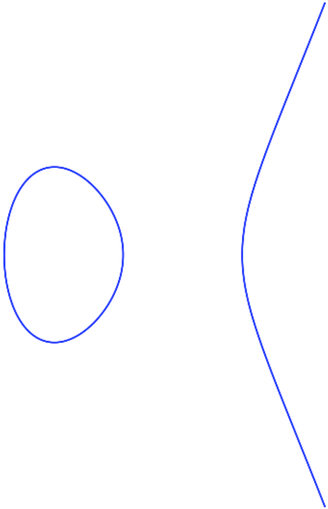
$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (a, j(E)) & \mapsto & a * j(E) \end{array}$$

Definition

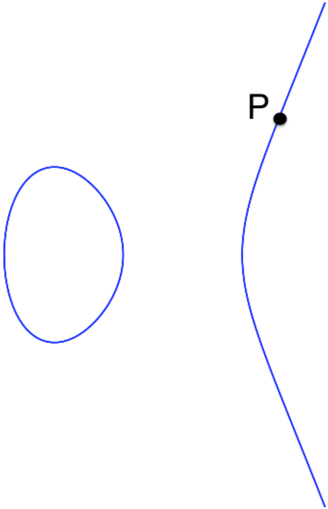
An *isogeny* of elliptic curves over $\mathbb{F}_q$ is a non-zero morphism $E \to E'$ that preserves the identity. It is given by rational maps.

Understanding isogenies I: the group law on elliptic curves

- For any field k (e.g. $\mathbb{F}_p$ or $\mathbb{Q}$), the k-rational points of E form a group $E(k)$.

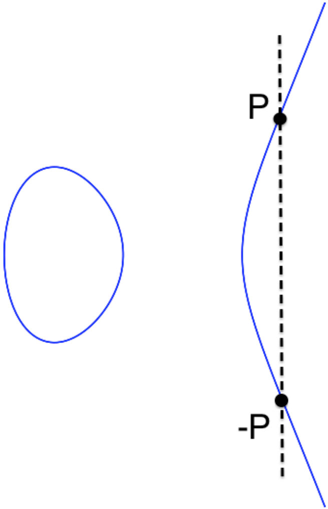


- For any field k (e.g. $\mathbb{F}_p$ or $\mathbb{Q}$), the k-rational points of E form a group $E(k)$.



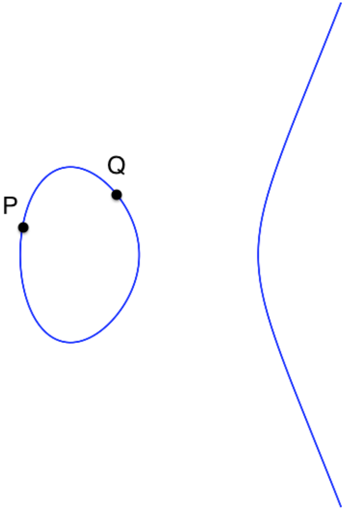
Understanding isogenies I: the group law on elliptic curves

- For any field k (e.g. $\mathbb{F}_p$ or $\mathbb{Q}$), the k-rational points of E form a group $E(k)$.



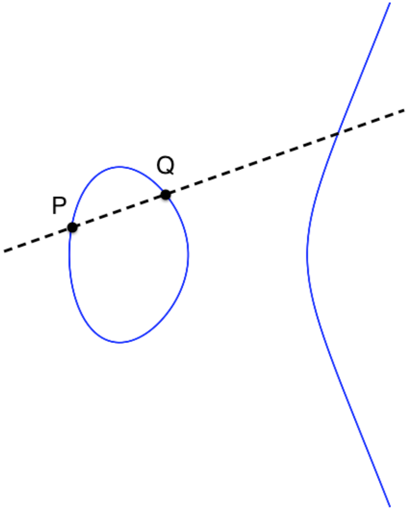
Understanding isogenies I: the group law on elliptic curves

- For any field k (e.g. $\mathbb{F}_p$ or $\mathbb{Q}$), the k-rational points of E form a group $E(k)$.



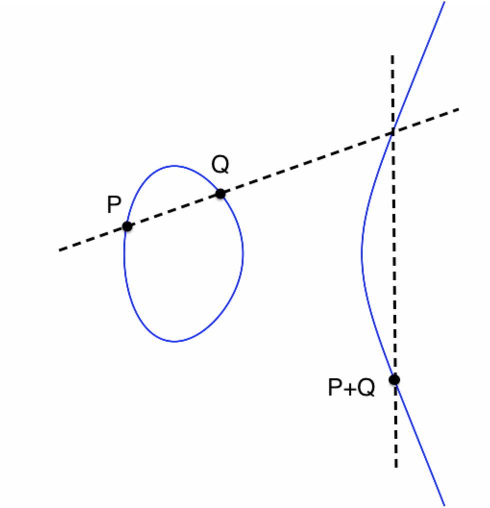
Understanding isogenies I: the group law on elliptic curves

- For any field k (e.g. $\mathbb{F}_p$ or $\mathbb{Q}$), the k-rational points of E form a group $E(k)$.



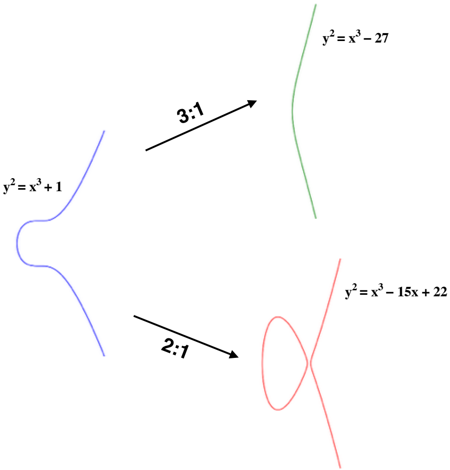
Understanding isogenies I: the group law on elliptic curves

- For any field k (e.g. $\mathbb{F}_p$ or $\mathbb{Q}$), the k-rational points of E form a group $E(k)$.



Understanding isogenies II: examples

An *isogeny* of elliptic curves over $\mathbb{F}_q$ is a non-zero morphism $E \to E'$ that preserves the identity. It is given by rational maps. (A morphism is a map of curves that preserves the group law).

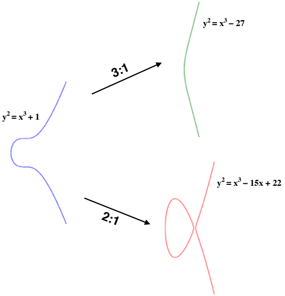


Understanding isogenies II: examples

- The top isogeny is

  $$(x,y) \mapsto ((x^3+4)/x^2, (x^3y-8y)/x^3).$$

- Define the curves over $\mathbb{F}_{17}$. Then it is '3:1' (and surjective), so for every $\mathbb{F}_{17}$-point on the green curve there are 3 $\mathbb{F}_{17}$-points on the blue curve which map to it.
- Exercise: which 3 points on the blue curve map to (3,0)?
- Sanity check: $j(E) = 0$, $j(E) = 1$, $j(E) = 0$. Exercise: check that E and E are isomorphic over $\mathbb{F}_{17^2}$ but not over $\mathbb{F}_{17}$.



Understanding isogenies III: useful facts

- If a (separable) isogeny φ has kernel of size ℓ (so φ is $\ell : 1$) the *degree* of φ is ℓ.
- Write

$$\begin{array}{rccc} [\ell] : & E & \longrightarrow & E \\ & P & \mapsto & \ell P \end{array}$$

  for the multiplication-by-ℓ map on E.
- For every isogeny $\varphi : E \to E'$, of degree n, there exists a *dual isogeny* $\varphi^\vee : E' \to E$ of degree ℓ such that $\varphi^\vee \circ \varphi = [\ell]$. That is, for every $P \in E(\overline{\mathbb{F}_p})$,

$$\varphi^\vee(\varphi(P)) = \ell P.$$

- For $P \in E(\overline{\mathbb{F}_q})$, if $\varphi(P) = \infty$, then $\ell P = \infty$, so

$$\ker(\varphi) \subseteq \ker([\ell]) =: E[\ell].$$

Understanding isogenies IV: counting the possibilities

Remember: if $\varphi : E \to E'$ is a separable isogeny and $\#\ker(\varphi) = \ell$, then $\ker(\varphi) \subseteq E[\ell]$.

Theorem

For every subgroup $H \subset E[\ell]$, there exists an elliptic curve E' and a separable isogeny $\varphi : E \to E'$ with $\ker(\varphi) = H$.

Theorem

For $E/\mathbb{F}_q$ an elliptic curve, if ℓ is a prime and $\ell \neq p$, then

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

Exercise: Show that there are $\ell + 1$ subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ of size ℓ.

Warning! Not every degree ℓ isogeny will be defined over $\mathbb{F}_q$. (It could be over $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}, \ldots$)

Back to Diffie-Hellman

- Remember: every size ℓ subgroup of $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ gives a unique (up to isomorphism) elliptic curve $E'/\overline{\mathbb{F}_q}$ and a unique separable degree-ℓ isogeny $\varphi : E \to E'$.
- Let $P \in E[\ell]$ be order ℓ (so $P \neq \infty$). Then $\langle P \rangle$ is a size ℓ subgroup of $E[\ell]$. Define E_P and φ_P to be the unique elliptic curve and degree ℓ-isogeny given by $\langle P \rangle$.
- Let $S = \{j(E_1), \ldots, j(E_n)\}$ be the set of j-invariants of elliptic curves over $\mathbb{F}_q$.
- We need a group G that *acts* on S as

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (a, j(E)) & \mapsto & a * j(E) \end{array}$$

Back to Diffie-Hellman

- Remember: every size ℓ subgroup of $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ gives a unique (up to isomorphism) elliptic curve $E'/\overline{\mathbb{F}_q}$ and a unique separable degree-ℓ isogeny $\varphi : E \to E'$.
- Let $P \in E[\ell]$ be order ℓ (so $P \neq \infty$). Then $\langle P \rangle$ is a size ℓ subgroup of $E[\ell]$. Define E_P and φ_P to be the unique elliptic curve and degree ℓ-isogeny given by $\langle P \rangle$.
- Let $S = \{j(E_1), \ldots, j(E_n)\}$ be the set of j-invariants of elliptic curves over $\mathbb{F}_q$.
- $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ *acts* on S as

$$\begin{array}{ccc} (\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}) \times S & \longrightarrow & S \\ (P, j(E)) & \mapsto & j(E_P). \end{array}$$

What about Alice and Bob?

Remember: The subgroup of $E[\ell]$ generated by an order ℓ point $P \in E[\ell]$ defines a unique (up to isomorphism) elliptic curve $E/\overline{\mathbb{F}_q}$ and degree ℓ isogeny $\varphi : E \to E$.

$$E/\mathbb{F}_q,\ P_A, Q_A \in E[\ell],$$
$$P_B, Q_B \in E[\ell]$$

$$m, n \in \mathbb{Z}/\ell\mathbb{Z}$$
$$R = mP_A + nQ_A$$
$$\varphi : E \to E$$

$$E,\ \varphi(P_B),\ \varphi(Q_B)$$
$$\longrightarrow$$
$$E,\ \varphi(P_A),\ \varphi(Q_A)$$
$$\longleftarrow$$

$$m, n \in \mathbb{Z}/\ell\mathbb{Z}$$
$$R = mP_B + nQ_B$$
$$\varphi : E \to E$$

$$m\varphi(P_A) + n\varphi(Q_A) = \varphi(R) =: R$$
$$\varphi : E \to E$$

$$m\varphi(P_B) + n\varphi(Q_B) = \varphi(R) =: R$$
$$\varphi : E \to E$$

Exercise: prove that $j(E) = j(E)$. This is the shared private key!

How hard is this?

Remember: The subgroup of $E[\ell]$ generated by an order ℓ point $P \in E[\ell]$ defines a unique (up to isomorphism) elliptic curve $E/\overline{\mathbb{F}_q}$ and degree ℓ isogeny $\varphi : E \to E$.

$$E/\mathbb{F}_q,\ P_A, Q_A \in E[\ell],$$
$$P_B, Q_B \in E[\ell]$$

$$m, n \in \mathbb{Z}/\ell\mathbb{Z}$$
$$R = mP_A + nQ_A$$
$$\varphi : E \to E$$

$$E,\ \varphi(P_B),\ \varphi(Q_B)$$
$$\longrightarrow$$
$$E,\ \varphi(P_A),\ \varphi(Q_A)$$
$$\longleftarrow$$

$$m, n \in \mathbb{Z}/\ell\mathbb{Z}$$
$$R = mP_B + nQ_B$$
$$\varphi : E \to E$$

- It should be hard to find φ given E, $\varphi(P_B)$, $\varphi(Q_B)$.
- Remember that there are at most $\ell + 1$ possible isogenies of degree ℓ.
- How do we increase the possibilities?

Composing isogenies

(This slide has been edited following a comment in the lecture).
Remember: The subgroup of $E[\ell]$ generated by an order ℓ point $P \in E[\ell]$ defines a unique (up to isomorphism) elliptic curve E and degree ℓ isogeny $\varphi : E \to E_P$.

$$m_1, \ldots, m_r, n_1, \ldots, n_r \in \mathbb{Z}/\ell\mathbb{Z},\ P_A, Q_A \in E[\ell^r]$$
$$R_1 = m_1 P_A + n_1 Q_A$$
$$\varphi_{R_1} : E \to E_{R_1}$$
$$R_2 = m_2 \varphi_{R_1}(P_A) + n_2 \varphi_{R_1}(Q_A)$$
$$\varphi_{R_2} : E_{R_1} \to E_{R_2} \ldots$$

$$\begin{tikzcd}
(E, R_1) \arrow[r, "\varphi_{R_1}"'] \arrow[rrr, bend left, "\varphi_A"] & (E_{R_1}, R_2) \arrow[r, "\varphi_{R_2}"'] & \cdots \arrow[r, "\varphi_{R_{r-1}}"'] & (E_{R_r}, R_r)
\end{tikzcd}$$

- There are up to $(\ell + 1)^r$ possibilities for φ_A!

Understanding isogenies V: isogeny graphs

Remember:

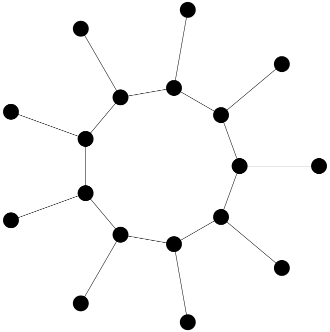
- From every elliptic curve $E/\mathbb{F}_q$ there are $\ell + 1$ possible degree ℓ isogenies, but some of them might only be defined over $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}, \ldots$
- For every degree ℓ-isogeny $\varphi : E \to E'$ there exists a unique degree ℓ-isogeny (called the dual) $\varphi^\vee : E' \to E$ such that $\varphi^\vee \circ \varphi = [\ell]$.

Definition

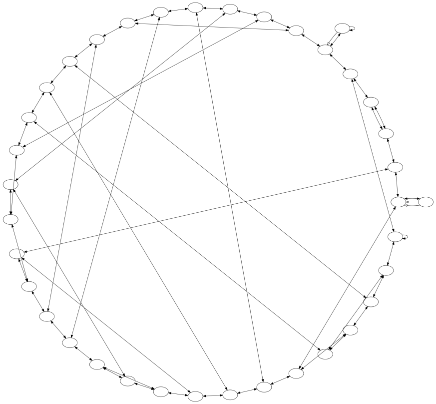
An *isogeny graph* is a graph where a vertex represents the j-invariant of an elliptic curve over $\mathbb{F}_q$ and an undirected edge represents a degree ℓ isogeny defined over $\mathbb{F}_q$ and its dual.

Understanding isogenies V: isogeny graphs

$p = q = 1000003$, $\ell = 2$, graph contains $j(E) = -3$:



$p = 431$, $q = 431^2$, $\ell = 2$, graph contains $j(E) = 0$:



Supersingular curves

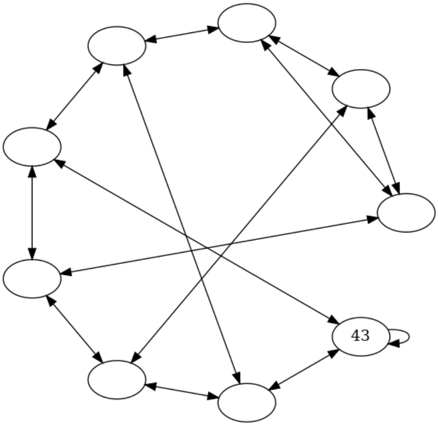
- Remember: for a prime $\ell \neq p$, the ℓ-torsion of $E/\mathbb{F}_q$ is

$$\{P \in E(\overline{\mathbb{F}_q}) : \ell P = \infty\} \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

- The q-torsion of E is either
  (a) $E[q] \cong \mathbb{Z}/q\mathbb{Z}$ - 'E is ordinary', or
  (b) $E[q] = \{\infty\}$ - 'E is supersingular'
- Theorem: every supersingular elliptic curve $E/\overline{\mathbb{F}_q}$ is defined over $\mathbb{F}_{p^2}$.
- If $p^2|q$ then all of the $\ell+1$ degree ℓ isogenies from a supersingular elliptic curve $E/\mathbb{F}_q$ are defined over $\mathbb{F}_q$!
- Theorem: the degree ℓ isogeny graph with vertices given by the supersingular j-invariants over $\mathbb{F}_q$ with $p^2|q$ is connected, and away from $j = 0$ and 1728, regular of degree $\ell + 1$. If $p \equiv 1 \bmod 12$, the graph is Ramanujan.

Ramanujan graphs

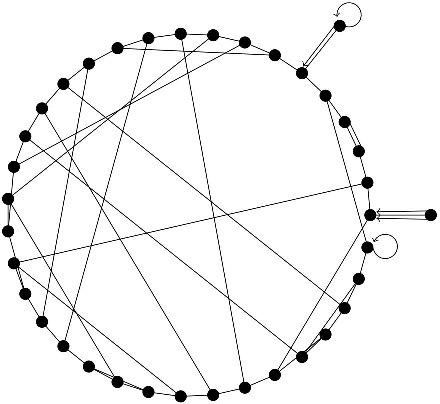
$p = 109$, $q = 109^2$, $\ell = 2$



- If Γ is a Ramanujan graph, Σ is a subset of Γ, and V is a vertex in Γ, then a 'long enough' random walk from V will land in Σ with probability at least $|\Sigma|/2|\Gamma|$.

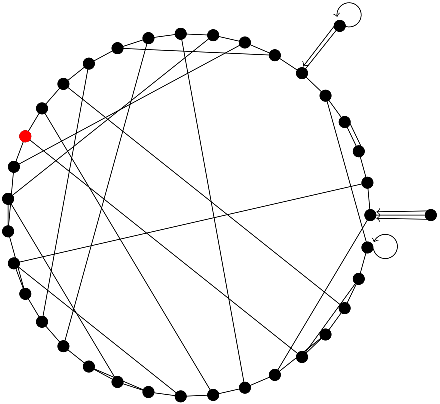
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



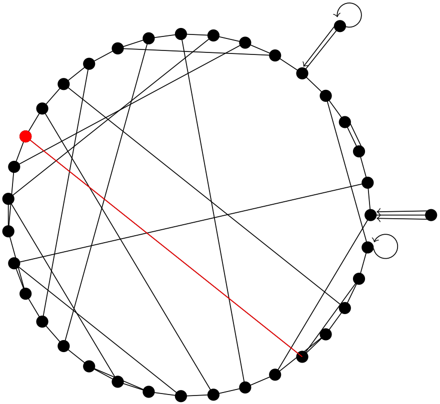
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



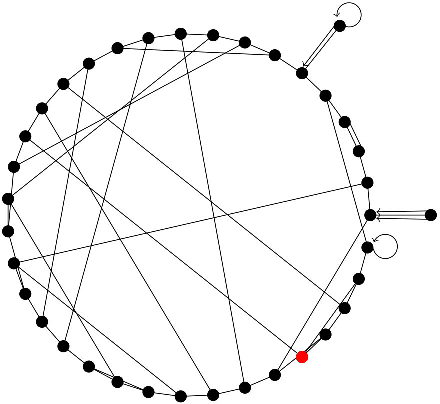
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



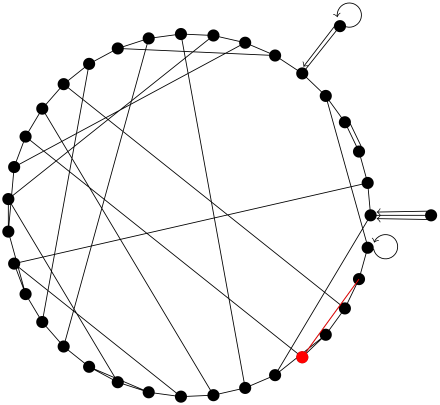
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



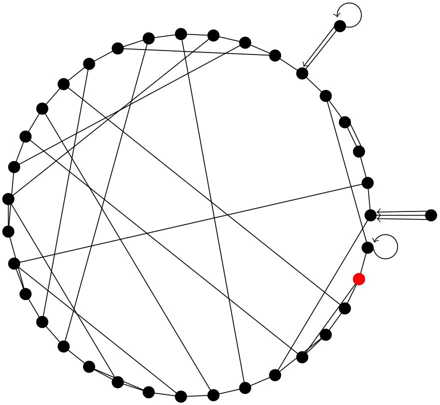
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



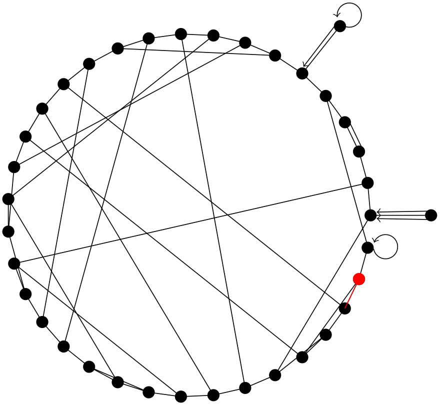
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



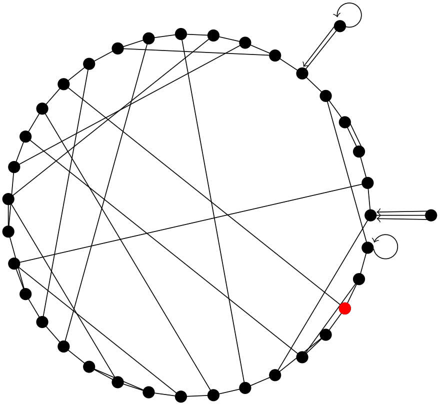
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



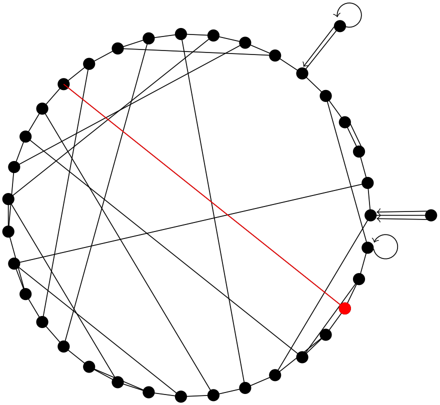
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



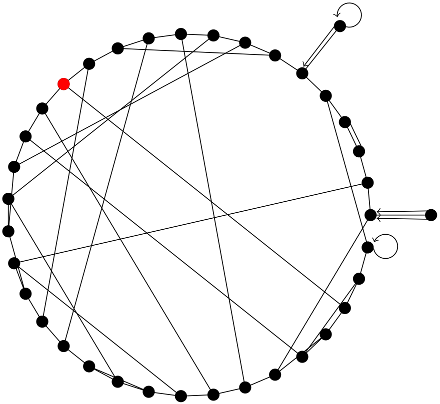
Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



Random walking on isogeny graphs

$p = 431, q = 431^2, \ell = 2$, graph contains $j(E) = 0$:



Alice and Bob do SIDH

Remember: The subgroup of $E[\ell^r]$ generated by an order ℓ^r point $P \in E[\ell^r]$ defines a unique (up to isomorphism) elliptic curve $E/\overline{\mathbb{F}_q}$ and degree ℓ^r isogeny $\varphi : E \to E$.

$$E/\mathbb{F}_q \text{ supersingular},$$
$$P_A, Q_A \in E[\ell^r],$$
$$P_B, Q_B \in E[\ell^r]$$

$$m, n \in \mathbb{Z}/\ell^r\mathbb{Z}$$
$$R = mP_A + nQ_A$$
$$\varphi : E \to E$$

$$E,\ \varphi(P_B),\ \varphi(Q_B)$$
$$\longrightarrow$$
$$E,\ \varphi(P_A),\ \varphi(Q_A)$$
$$\longleftarrow$$

$$m, n \in \mathbb{Z}/\ell^r\mathbb{Z}$$
$$R = mP_B + nQ_B$$
$$\varphi : E \to E$$

$$m\varphi(P_A) + n\varphi(Q_A) = \varphi(R)$$
$$=: R$$
$$\varphi : E \to E$$

$$j(E) = j(E)$$

$$m\varphi(P_B) + n\varphi(Q_B) = \varphi(R)$$
$$=: R$$
$$\varphi : E \to E$$

Recap of terms

- An *elliptic curve* over $\mathbb{F}_q$ with $2, 3 \not| q$ is given by an equation
$$y^2 = x^3 + ax + b$$
with $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$.
- There is a group law on elliptic curves where the identity element is called ∞.
- $\overline{\mathbb{F}_q}$ is the *algebraic closure* of $\mathbb{F}_q$ - this contains all the solutions to every polynomial with coefficients in $\mathbb{F}_q$.
- For $n \in \mathbb{Z}$, the n-torsion $E[n]$ of E is given by
$$E[n] = \{P \in E(\overline{\mathbb{F}_q}) : nP = \infty\}.$$
- An elliptic curve over $\mathbb{F}_q$ is *supersingular* if
$$E[q] \cong \{\infty\}.$$

Recap of terms

- An *isogeny* of elliptic curves is a map that preserves the geometric structure, the group law $(+)$ and the identity (∞).
- The *degree* of a separable isogeny φ is the size of the kernel, that is,

$$\deg(\varphi) = \#\{P \in E(\overline{\mathbb{F}_p}) : \varphi(P) = \infty\}.$$

Recap of ideas

- We can think of the setup of classical Diffie-Hellman as a group G (e.g. $\mathbb{Z}$ or $\mathbb{F}_p^*$) acting on a set S (e.g. $\mathbb{F}_p$) as

$$\begin{array}{ccc} G \times S & \longrightarrow & S \\ (a, x) & \mapsto & a * x := x^a. \end{array}$$

- We extend the classical Diffie-Hellman idea by using the set

$$S = \{j(E) : E/\mathbb{F}_{p^2},\ E \text{ supersingular elliptic curve}\},$$

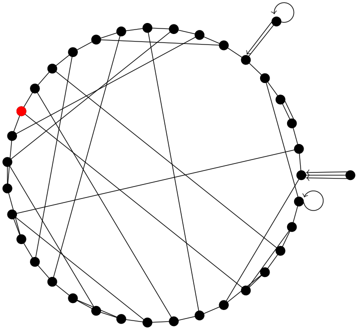
  and the group G acts on S by isogenies of degree ℓ^r.
- The supersingular isogeny Diffie-Hellman is 'hard enough' because there are many choices for each isogeny, and the choice is random.
- We analyse the randomness of the choice using isogeny graphs

Recap of supersingular isogeny graphs

Recall:

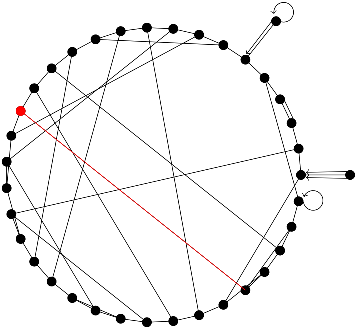
- A vertex of a supersingular isogeny graph is the j-invariant (isomorphism invariant) of a supersingular elliptic curve.
- An edge of a degree ℓ isogeny graph is a pair of degree ℓ isogenies $\varphi : E \to E'$ and $\varphi^\vee : E' \to E$ such that for $P \in E(\overline{\mathbb{F}_q})$, $\varphi^\vee(\varphi(P)) = \ell P$.
- Every vertex in a supersingular isogeny graph has $\ell + 1$ edges from it.
- A random walk on the graph will give a random vertex after enough steps.
- A path of lenth r represents an isogeny given by the composition of r degree ℓ isogenies.

Bob takes a random walk



- Bob starts with the public elliptic curve E
- Bob decides he will walk 4 steps
- Bob publishes $P_B, Q_B \in E[2^4]$ (because $\ell = 2$)
- Bob chooses random $m_1, n_1 \in \mathbb{Z}/2\mathbb{Z}$ (because $\ell = 2$)
- Bob computes a secret point $R_1 = m_1 P_B + n_1 Q_B$ on E

Bob takes a random walk

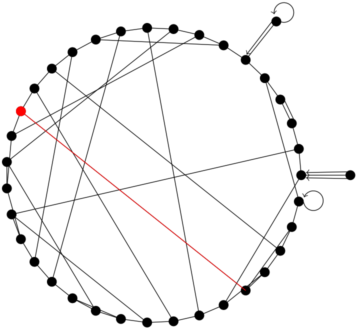


- Compute the elliptic curve E_{R_1} and degree 2 isogeny

$$E \to E_{R_1}$$

corresponding to R_1

Bob takes a random walk

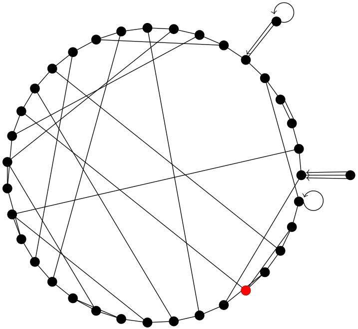


- Compute the elliptic curve E_{R_1} and degree 2 isogeny

$$E \to E_{R_1}$$

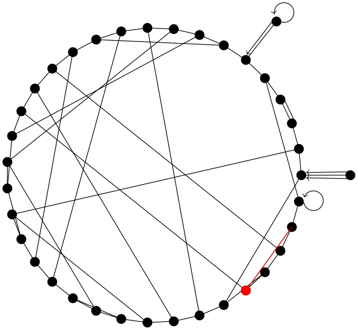
  corresponding to R_1
- Compute points $P_1 = \varphi_{R_1}(P_B)$ and $Q_1 = \varphi_{R_1}(Q_B)$ on E_{R_1}.

Bob takes a random walk



- Bob is now standing at supersingular elliptic curve E_{R_1}
- Choose random $m_2, n_2 \in \mathbb{Z}/2\mathbb{Z}$ (because $\ell = 2$)
- Compute secret point $R_2 = m_2 P_1 + n_2 Q_1$ on E_{R_1}

Bob takes a random walk



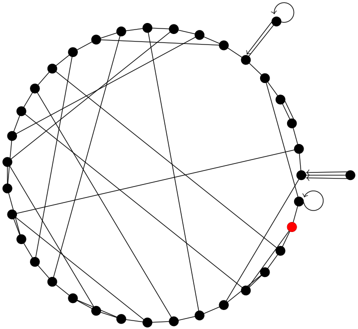
- Compute the elliptic curve E_{R_2} and degree 2 isogeny

$$E_{R_1} \to E_{R_2}$$

corresponding to R_2

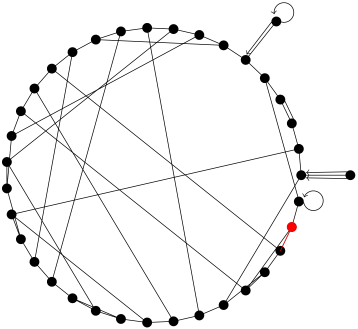
- Compute points $P_2 = \varphi_{R_2}(P_1)$ and $Q_2 = \varphi_{R_2}(Q_1)$ on E_{R_2}.

Bob takes a random walk



- Bob is now standing at supersingular elliptic curve E_{R_2}
- Choose random $m_3, n_3 \in \mathbb{Z}/2\mathbb{Z}$ (because $\ell = 2$)
- Compute secret point $R_3 = m_3 P_2 + n_3 Q_2$ on E_{R_2}

Bob takes a random walk

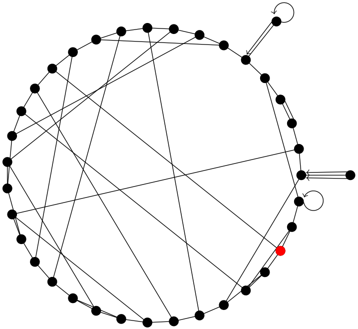


- Compute the elliptic curve E_{R_3} and degree 2 isogeny

$$E_{R_2} \to E_{R_3}$$

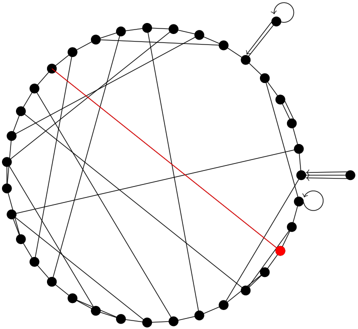
  corresponding to R_3
- Compute points $P_3 = \varphi_{R_3}(P_2)$ and $Q_3 = \varphi_{R_3}(Q_2)$ on E_{R_3}.

Bob takes a random walk



- Bob is now standing at supersingular elliptic curve E_{R_3}
- Choose random $m_4, n_4 \in \mathbb{Z}/2\mathbb{Z}$ (because $\ell = 2$)
- Compute secret point $R_4 = m_4 P_3 + n_4 Q_3$ on E_{R_3}

Bob takes a random walk



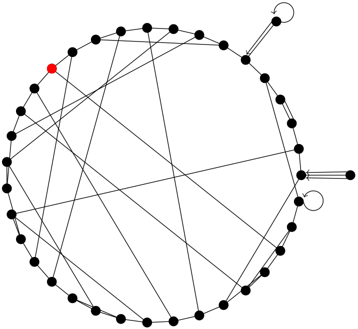
- Compute the elliptic curve E_{R_4} and degree 2 isogeny

$$E_{R_3} \to E_{R_4}$$

corresponding to R_4

- You have reached you destination! (Remember that Bob chose to walk 4 steps).

Bob takes a random walk



- Compute

$$\varphi_B := \varphi_{R_4} \circ \varphi_{R_3} \circ \varphi_{R_2} \circ \varphi_{R_1}$$

so that

$$\varphi_B : E \longrightarrow E_{R_4}.$$

- Look up Alice's public points P_A and Q_A and send her

$$\varphi_B(P_A) \text{ and } \varphi_B(Q_A).$$

Alice and Bob do SIDH

Remember: The subgroup of $E[\ell^r]$ generated by an order ℓ^r point $P \in E[\ell^r]$ defines a unique (up to isomorphism) elliptic curve $E/\overline{\mathbb{F}_q}$ and degree ℓ^r isogeny $\varphi : E \to E$.

$E/\mathbb{F}_q$ supersingular,
$P_A, Q_A \in E[\ell^r]$,
$P_B, Q_B \in E[\ell^r]$

$m, n \in \mathbb{Z}/\ell^r\mathbb{Z}$
$R = mP_A + nQ_A$
$\varphi : E \to E$

$$E,\ \varphi(P_B),\ \varphi(Q_B) \longrightarrow$$

$$E,\ \varphi(P_A),\ \varphi(Q_A) \longleftarrow$$

$m, n \in \mathbb{Z}/\ell^r\mathbb{Z}$
$R = mP_B + nQ_B$
$\varphi : E \to E$

$$m\varphi(P_A) + n\varphi(Q_A) = \varphi(R) =: R$$

$$\varphi : E \to E$$

$$j(E) = j(E)$$

$$m\varphi(P_B) + n\varphi(Q_B) = \varphi(R) =: R$$

$$\varphi : E \to E$$

Bonus: how random is SIDH?

Remember:

$$\ker(\varphi) = \{P \in E(\overline{\mathbb{F}_q}) : \varphi(P) = \infty\}$$
$$= \langle R \rangle$$
$$\cong \mathbb{Z}/\ell^r\mathbb{Z}.$$

$m, n \in \mathbb{Z}/\ell^r\mathbb{Z}$

$R = mP_B + nQ_B$

$\varphi : E \to E.$

- A truly random isogeny from a random path in a supersingular isogeny graph

$$\varphi_B = \varphi_{R_1} \circ \varphi_{R_2} \circ \cdots \circ \varphi_{R_r}$$

will have $\# \ker(\varphi_B) = \ell^r$ but maybe not $\cong \mathbb{Z}/\ell^r\mathbb{Z}$!

- Exercise: which other situations are there?

Computing random paths in isogeny graphs

Remember: Each size ℓ subgroup of $E[\ell]$ defines a unique (up to isomorphism) degree ℓ isogeny from E.

- Vélu's algorithm: given a size ℓ subgroup H of $E[\ell]$, computes the isogeny and the elliptic curve corresponding to H.
- Can compute a random path of length r by choosing a random size ℓ subgroup at each step and using Vélu r times to find φ_{R_1}, φ_{R_2}, …, φ_{R_r}. (Like 'Bob goes for a walk').
- More efficient (but maybe less secure): choose a random subgroup of $E[\ell^r]$ that is isomorphic to $\mathbb{Z}/\ell^r\mathbb{Z}$ and use Vélu once to compute φ_B. (Like 'Alice and Bob do SIDH').

Computing random paths in isogeny graphs

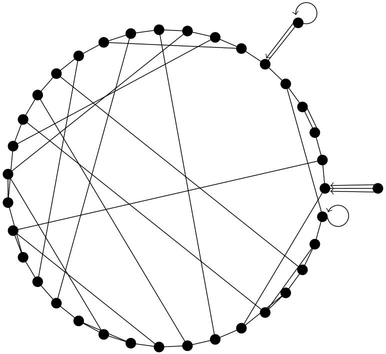
- Alternative to Vélu's algorithm: use modular polynomials

Definition

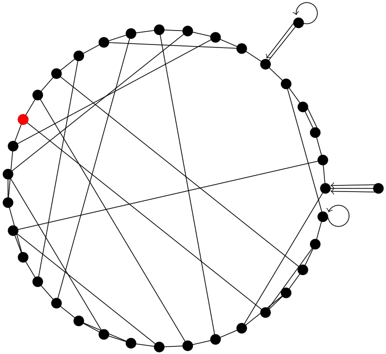
The *modular polynomial of level ℓ* is a symmetric polynomial $\Phi_\ell(X, Y) \in \mathbb{Z}[X, Y]$ of degree $\ell + 1$ in both X and Y such that for all (non-ℓ) prime powers q there exists a degree ℓ isogeny $E \to E'$ if and only if $\overline{\Phi_\ell(X, Y)} \in \mathbb{F}_q[X, Y]$ satisfies $\overline{\Phi_\ell}(j(E), j(E')) = 0$.

- Neighbours of $j(E)$ in the ℓ-isogeny graph are the roots of $\overline{\Phi_\ell(j(E), Y)}$.
- Elkie's has an algorithm to compute the isogeny $E \to E'$ and its kernel (if they exist) given $j(E)$ and $j(E')$.
- Compute a random path of length r in a degree ℓ supersingular isogeny graph starting at E using $\Phi_\ell(X, Y)$.

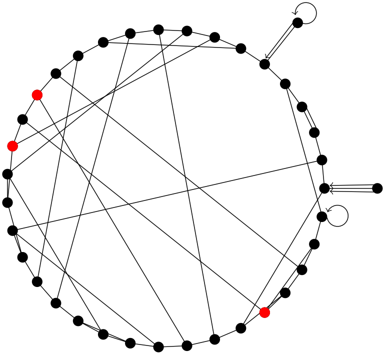
Finding a random curve with modular polynomials



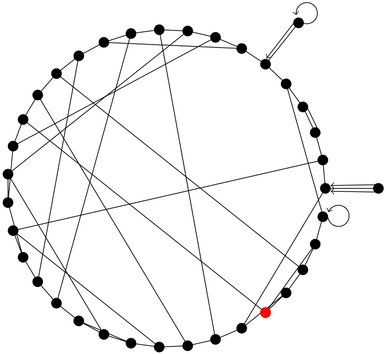
Finding a random curve with modular polynomials



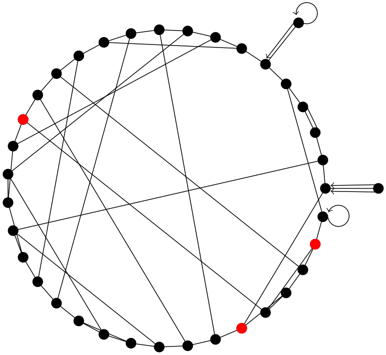
Finding a random curve with modular polynomials



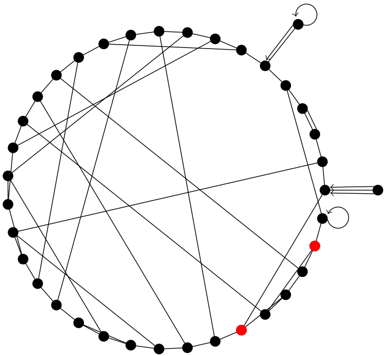
Finding a random curve with modular polynomials



Finding a random curve with modular polynomials

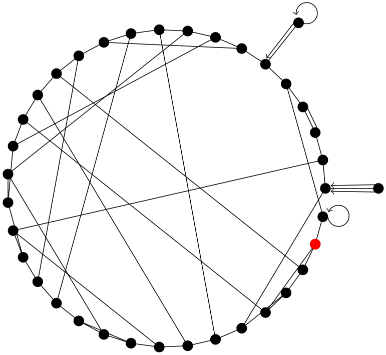


Finding a random curve with modular polynomials

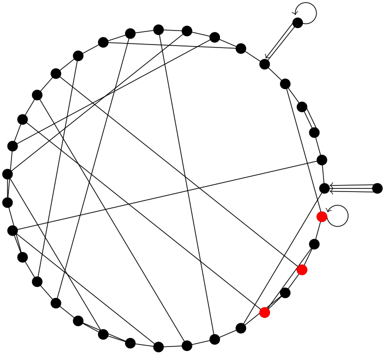


Edit: walking back is allowed in a random walk, but is not allowed in the SIDH protocol as this will give a final isogeny with non-cyclic kernel.

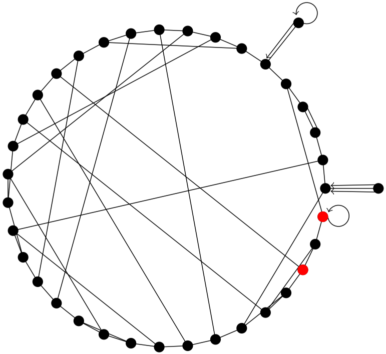
Finding a random curve with modular polynomials



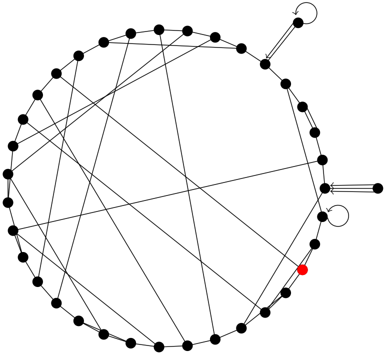
Finding a random curve with modular polynomials



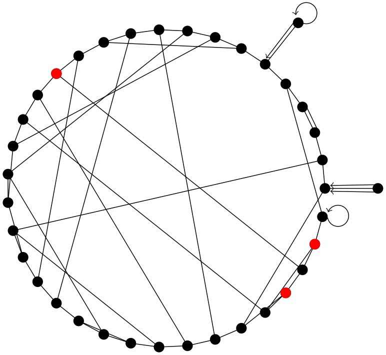
Finding a random curve with modular polynomials



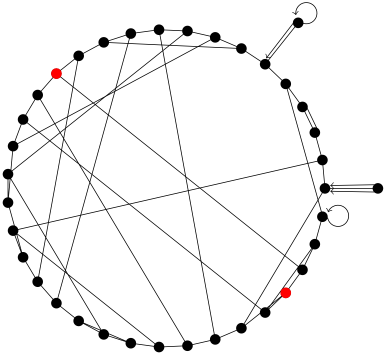
Finding a random curve with modular polynomials



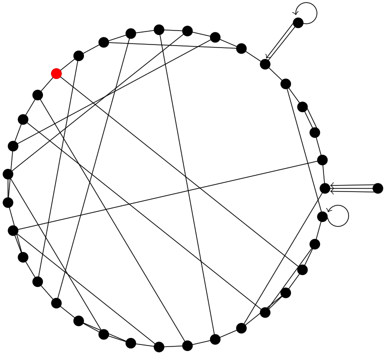
Finding a random curve with modular polynomials



Finding a random curve with modular polynomials



Finding a random curve with modular polynomials



Attacks on SIDH: Galbraith et. al. 2016

1. Attack in the case that Alice and Bob do not change their private keys $m_A, n_A \in \mathbb{Z}/\ell_A\mathbb{Z}$ and $m_B, n_B \in \mathbb{Z}/\ell_B\mathbb{Z}$.
   - This attack recovers the full private key in $O(r)$ steps.
   - The only known validation methods that prevent this are very costly.
2. Number theoretic attack in time $\log(\sqrt{q})$ (currently unfeasible due to lack of theory).
   - Relies on an efficient algorithm to compute 'endomorphism rings'.
3. Full break if the shared secret is partially leaked. (Edit: if you are watching the video, there was a comment from the audience saying that this is too generous, but following further discussion we concluded that it does in fact give a full break).

Potential attack on SIDH: Petit June 2017

- Constructs variations of SIDH which can be broken by exploiting $\phi_A(P_B)$ and $\phi_A(P_B)$.
- Does not (yet) apply to the current version of SIDH.

Where are we now with SIDH?

- Detailed cryptoanalysis needed to assess security
- Assuming the system is chosen to be secure against known attacks, best classical algorithm to find shared secret (based on finding an isogeny between 2 curves) is $O(p^{1/4})$ for elliptic curves over $\mathbb{F}_{p^2}$
- Best quantum attack is $O(p^{1/6})$
- Galbraith has an attack exploiting reused secret key pairs (m and n)
- Christophe Petit studies how to exploit the additional points $\varphi(P_A)$, $\varphi(P_B)$ - but his methods do not (yet) give an attack on SIDH
- ...

SIDH vs. Lattice based crypto

Name	Primitive	Time (ms)	PK size (bytes)
Frodo	LWE	2.600	11,300
NewHope	R-LWE	0.310	1,792
NTRU	NTRU	2.429	1,024
SIDH	Supersingular Isogeny	900	564

These are non-optimised timings!

Bibliography

- De Feo, Jao, Plût, *Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies* (2011)
- Galbraith et. al., *On the security of supersingular isogeny cryptosystems* (2016)
- Petit, *Faster algorithms for isogeny problems using torsion point images* (last week)