Introduction to mathematical cryptography

Lecture 5: Isogeny-based cryptography

Sabrina Kunzweiler

Preliminary Arizona Winter School 2025

Quantum computers and cryptography

What is a quantum computer?

- based on quantum mechanics
- superposition and entanglement of elements

Does it work?

- small scale prototypes (Google, IBM, ...)
- unclear when/if a practical quantum computer will exist

(startup: Alice & Bob)

Consequences for cryptography

- Peter Shor (1996): Integer Factorization and DLP can be solved on a quantum computer in polynomial time

$\Rightarrow$ Practical quantum computers would make today's public key cryptography insecure.

Post-quantum cryptography

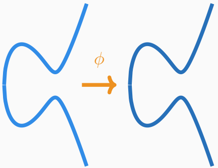
Development of cryptography that is secure against attacks from quantum computers

Candidates for post-quantum cryptography

- Lattices
- Codes
- Multivariate polynomials
- Hash functions

- this lecture : **Isogenies**

Isogeny-based cryptography: based on the hard problem of finding isogenies between (supersingular) elliptic curves



outline: (1) group actions, (2) isogenies, (3) CSIDH

Cryptographic group actions

Group actions and key exchange

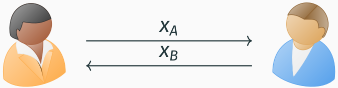
Group action

A map $\star : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$, with $\mathbb{G}$ a group, $\mathcal{X}$ a set:

1. $id \star x = x \ \ \forall\, x \in \mathcal{X}$ (identity),
2. $(g \circ h) \star x = g \star (h \star x) \ \ \forall\, g, h \in \mathbb{G}, x \in \mathcal{X}$ (compatibility).

- regular if for all $x, y \in \mathcal{X}$, $\exists$ unique $g \in \mathbb{G}$ with $y = g \star x$
- commutative if $\mathbb{G}$ is commutative

Group action Diffie-Hellman key exchange



Alice	Bob
$(g_a \in \mathbb{G})$	$(g_b \in \mathbb{G})$
$x_A \leftarrow g_a \star x_0$	$x_B \leftarrow g_b \star x_0$
$x_{AB} \leftarrow g_a \star x_B$	$x_{BA} \leftarrow g_b \star x_A$

- Commutative group action $\star : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$, and some $x_0 \in \mathcal{X}$
- Secret keys: $g_a, g_b \in \mathbb{G}$
- Public keys: $x_a, x_b \in \mathcal{X}$

Examples of group actions

(a) $\mathbb{G} = (\mathbb{Z}/(p-1)\mathbb{Z})^*$ and $\mathcal{X} = \mathbb{F}_p^*$

$$\star : (\mathbb{Z}/(p-1)\mathbb{Z})^* \times \mathbb{F}_p^* \to \mathbb{F}_p^*, \quad (n, x) \mapsto x^n.$$

- identity: $1 \star x = x^1 = x$ for all $x \in \mathbb{F}_p^*$.
- compatibility: $(n_1 \cdot n_2) \star x = x^{(n_1 \cdot n_2)} = (x^{n_2})^{n_1} = n_1 \star (n_2 \star x)$ for all $n_1, n_2 \in (\mathbb{Z}/(p-1)\mathbb{Z})^*$ and $x \in \mathbb{F}_p^*$.

$\Rightarrow$ **Diffie-Hellman** (Lecture 2)

(b) $\mathbb{G} = (\mathbb{Z}/N\mathbb{Z})^*$ and $\mathcal{X} = \langle P \rangle \subset E(\mathbb{F}_q)$ with $P \in E(\mathbb{F}_q)$, $ord(P) = N$:

$$\star : (\mathbb{Z}/N\mathbb{Z})^* \times \mathcal{X} \to \mathcal{X}, \quad (n, Q) \mapsto [n] \cdot Q.$$

- identity: $1 \star Q = [1]Q = Q \quad$ for all $Q \in \mathbb{G}$,
- compatibility: $(n_1 \cdot n_2) \star Q = [n_1 \cdot n_2]Q = [n_1]([n_2]Q) = n_1 \star (n_2 \star Q)$ for all $n_1, n_2 \in (\mathbb{Z}/N\mathbb{Z})^*$ and $Q \in E(\mathbb{F}_q)$.

$\Rightarrow$ **Elliptic curve Diffie-Hellman** (Lectures 3/4)

Cryptographic group actions

When is a group action $\star : \mathbb{G} \times \mathcal{X} \to \mathcal{X}$ useful for cryptography?

- Application of $\star$ should be a **cryptographic one-way function**:
  - Evaluating $g \star x$ is efficient for all g, x (we say $\star$ is effective[1])
  - GADLP is hard Given $x, y \in \mathcal{X}$, find $g \in \mathbb{G}$ with $y = g \star x$.
    Note: g is unique if $\star$ is a regular group action.
- Group action is **commutative** (depending on application):
  - Requirement so that group action Diffie-Hellman (slide 3) works.
  - There are other cryptographic protocols that work with non-commutative group actions.
    lattice isomorphism, code-equivalence, tensors

[1] Actually, more properties are required: group operation is efficient, sampling is efficient, etc.

Hardness of the GADLP

Classic attacks

Can we translate attacks on Group-DLP to solve GADLP?

- x does not work for all algorithms, e.g. Pohlig-Hellman algorithm
  $\Rightarrow$ GADLP does not get easier when $N = \#\mathbb{G}$ is composite.
- ✓ works for some algorithms, e.g. baby-step giant-step algorithm (Exercise)
  $\Rightarrow$ We can solve GADLP in time $O(\sqrt{N})$ where $N = \#\mathbb{G}$.

Quantum attacks

Best known attacks from the literature

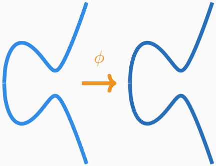
- x Shor's algorithm to solve Group-DLP quantum polynomial-time cannot be translated to solve GADLP.
- ✓ Algorithm by Greg Kuperberg (2005): subexponential in $N = \#\mathbb{G}$

Isogenies

Definition of isogeny

Isogeny

E, E' elliptic curves over k. An **isogeny** is a non-zero non-zero rational map $\phi : E \to E'$ that induces a group homomorphism $E(\bar{k}) \to E'(\bar{k})$.
E and E' are called **isogenous**.



- rational map: (here) $\exists\ \phi_x(x, y), \phi_y(x, y)$ rational functions so that

$$\phi : (x, y) \mapsto (\phi_x(x, y), \phi_y(x, y))$$

  for all but finitely many points $(x, y) \in E(\bar{k})$.
- non-zero: exclude map $\phi : E \to E'$, $\phi : P \mapsto \infty$.
- group homomorphism: $\phi(P + Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E(\bar{k})$.

Example: scalar multiplication

Let $N \in \mathbb{Z} \setminus \{0\}$, and $E : y^2 = x^3 + ax + b$ an elliptic curve, then scalar multiplication by N

$$[N] : E \to E, \quad P \mapsto [N]P$$

is an isogeny.

- ✓ rational map: can be deduced from the group law.
- ✓ non-zero: since $N \neq 0$
- ✓ group homomorphism follows from the group law on E.

Case $N = 2$ Let $P = (x_1, y_1)$, then $[2]P = (x_3, y_3)$, where $x_3 = m^2 - 2x_1$ and $y_3 = m(x_1 - x_3) - y_1$ and $m = (3x_1^2 + a)/(2y_1)$ (Theorem 3.7(b)).

- $x_3 = \phi_x(x_1, y_1) = \frac{x_1^4 - 2ax_1^2 - 8bx_1 - a^2}{4(x_1^3 + ax_1 + b)}$,
- $y_3 = \phi_y(x_1, y_1) = \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8(x_1^3 + ax_1 + b)^2} \cdot y_1$.

Constructing an isogeny from its kernel

Vélu (simplified)

$E : y^2 = x^3 + ax + b$ over k and finite odd subgroup $G \subset E(\bar{k})$.
We set $E' : y^2 = x^3 + a'x + b'$ with

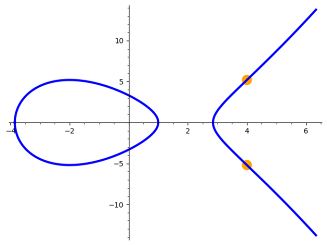
$$a' = a - 5 \sum_{Q \in G \setminus \{\infty\}} (3x(Q)^2 + a),$$

$$b' = b - 7 \sum_{Q \in G \setminus \{\infty\}} (5x(Q)^3 + 3ax(Q) + 2b).$$

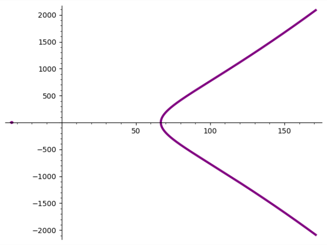
Then there exists an isogeny $\phi : E \to E'$ with kernel $\ker(\phi) = G$.

Example $E : y^2 = x^3 - 12x + 11$ over $\mathbb{Q}$,
$G = \langle (4, 3\sqrt{3}) \rangle = \{(4, 3\sqrt{3}), (4, -3\sqrt{3}), \infty\} \subset E[3]$.
We compute $a' = -12 - 5 \cdot 2 \cdot (3 \cdot 4^2 + (-12)) = -372$, and
$b' = 11 - 7 \cdot 2 \cdot (5 \cdot 4^3 - 12 \cdot 3 \cdot 4 + 2 \cdot 11) = -2761$

Example Isogeny $\phi : E \to E'$ (continued)



$$\xrightarrow{\phi}$$



$E : y^2 = x^3 - 12x + 11$

$E' : y^2 = x^3 - 372x - 2761$

```
sage: K = QQ.extension(x^2-3,sq3)
sage: E = EllipticCurve(K,[-12,11])
sage: P = E([4,3*sq3])
sage: phi = E.isogeny(P)
```

$G = \langle (4, 3\sqrt{3}) \rangle$.

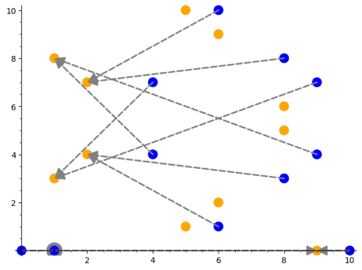
We can ask for various properties of ϕ in SageMath, such as the rational maps, codomain, evaluation at points, etc.

$$\phi(x, y) = \left(\frac{x^3 - 8x^2 + 88x - 180}{x^2 - 8x + 16}, \frac{x^3 - 12x^2 - 24x + 8}{x^3 - 12x^2 + 48x - 64} \cdot y \right)$$

Example over a finite field

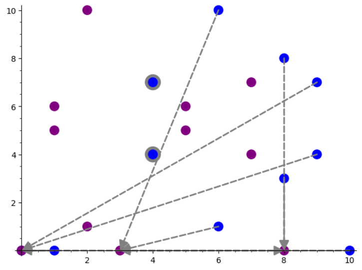
$E : y^2 = x^3 - x$ over $\mathbb{F}_{11}$

(a) Kernel $\langle(1,0)\rangle \subset E[2]$



codomain $E_1 : y^2 = x^3 + 8$

(b) Kernel $\langle(4,4)\rangle \subset E[3]$



codomain $E_2 : y^2 = x^3 + 2x$

An isogeny $E \to E'$ with kernel $G \cong \mathbb{Z}/\ell\mathbb{Z}$ is called **ℓ-isogeny**.

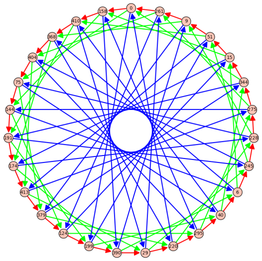
- $E \to E_1$ is a 2-isogeny
- $E \to E_2$ is a 3-isogeny.

Commutative Supersingular Isogeny Diffie-Hellman (CSIDH)

CSIDH

potential post-quantum replacement for Diffie-Hellman key exchange

- **CSIDH** = **C**ommutative **S**upersingular **I**sogeny **D**iffie-**H**ellman
- proposed by Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny and Joost Renes (2018)



- based on the commutative class group action on supersingular elliptic curves over $\mathbb{F}_p$
- described by talking walks in an isogeny graph

Elliptic curves in Montgomery form

Elliptic curve E is in **Montgomery form**[a] if

$$E_A : y^2 = x^3 + Ax^2 + x, \quad A \text{ with } A^2 \neq 4.$$

We say that A is **the Montgomery coefficient** of E.

[a] More general definition: $By^2 = x^3 + Ax^2 + x$ for some $B \neq 0$

Relation with short Weierstrass form

$$y^2 = x^3 + Ax^2 + x \qquad \begin{array}{c} \Rightarrow \\ (\Leftarrow)_{\bar{k}} \end{array} \qquad y^2 = x^3 + ax + b$$

$$y' = y, \quad x' = (x + A/3), \quad a = \tfrac{3-A^2}{3}, \quad b = \tfrac{2A^3-9A}{27}.$$

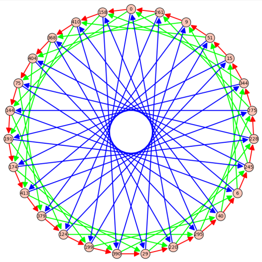
Supersingular elliptic curves

E over $\mathbb{F}_p$ is **supersingular**[a] if $\#E(\mathbb{F}_p) = p + 1$.

[a] There are more general deifnitions for arbitrary finite fields

- supersingular $\hat{=}$ "unusual"; **not** singular (elliptic curves are are smooth)
- Elliptic curves that are not supersingular are called **ordinary**
- **Examples**
  - $E : y^2 = x^3 + 1$ over $\mathbb{F}_p$ is supersingular if $p \equiv 2 \pmod 3$. We proved $\#E(\mathbb{F}_p) = p + 1$ in Lecture 3.
  - $E : y^2 = x^3 + x$ over $\mathbb{F}_{67}$. Here $\#E(\mathbb{F}_{67}) = 68$. Example for the MOV algorithm, Lecture 4.
  - $E : y^2 = x^3 + x$ over $\mathbb{F}_p$ if and only if $p \equiv 3 \pmod 4$. Reference in the lecture notes.

CSIDH Isogeny Graph



Isogeny Graph over $\mathbb{F}_{419}$ with 3-, 5-, and 7- isogenies.

Prime field: $\mathbb{F}_p$ with $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ where $\ell_1, \ldots, \ell_n$ small odd pairwise distinct primes.

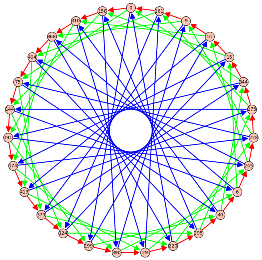
Vertices (V): supersingular elliptic curves in Montgomery form over $\mathbb{F}_p$

- cardinality: $O(\sqrt{p})$
- labeled by Montgomery coefficient A $\Rightarrow E_A : y^2 = x^3 + Ax^2 + x$

Edges (E): ℓ_i-isogenies over $\mathbb{F}_p$ for $i = 1, \ldots, n$

Edges in the CSIDH graph

Recall $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, let E_A over $\mathbb{F}_p$ supersingular.



Isogeny Graph over $\mathbb{F}_{419}$ with 3-, 5-, and 7- isogenies.

- $\#E_A(\mathbb{F}_p) = p + 1 = 4 \cdot \ell_1 \cdots \ell_n$

$\Rightarrow$ For each ℓ_i, there is a unique group of order ℓ_i, say $G_i \subset E(\mathbb{F}_p)[\ell_i]$ this defines an isogeny $E_A \to E_{A_i}$

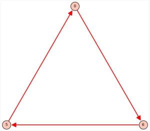
$\to$ edge from A to A_i.

We can walk in the isogeny graph by computing isogenies.

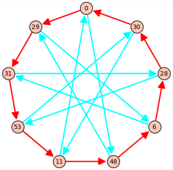
Tiny examples with $p = 4 \cdot \ell_1 \cdots \ell_n - 1$

Smallest example is $p = 3$: One vertex $A = 0$, no edges.

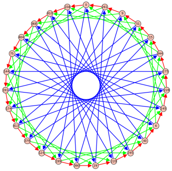
(a) $p = 4 \cdot 3 - 1 = 11$.
Three supersingular Montgomery curves
$A = 0, 5, 6$.



(b) $p = 4 \cdot 3 \cdot 5 - 1 = 59$.
Nine supersingular Montgomery curves
$A = 0, 6, 11, 28, 29, 30, 31, 48, 53$



(c) $p = 4 \cdot 3 \cdot 5 \cdot 7 - 1 = 419$.
27 supersingular Montgomery curves



```
sage: Fp = GF(11)
sage: E = EllipticCurve(Fp,[0,5,0,1,0])
sage: P = E([3,3])
sage: phi = E.isogeny(P, model="montgomery"); phi
Isogeny of degree 3 from Elliptic Curve defined by y^2 = x^3 + 5*
 x^2 + x over Finite Field of size 11 to Elliptic Curve defined by
  y^2 = x^3 + x over Finite Field of size 11
```

Group action on the CSIDH graph

Consider $p = 4 \cdot \ell_1 \cdots \ell_n - 1$, and $G = (V, E)$ the CSIDH isogeny graph over $\mathbb{F}_p$.

There is a commutative group action

$$\star : \mathbb{Z}^n \times V \to V$$

where elements of $\mathbb{Z}^n$ act as isogenies.

Evaluation of the group action $(a_1, \ldots, a_n) \star E_A = E_{A'}$

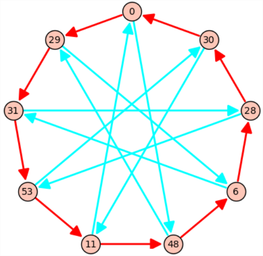
- $(a_1, \ldots, a_n)$: defines an path in the CSIDH graph
- Starting vertex: A
- $|a_i|$: number of ℓ_i-isogenies in the path
- sign of a_i: direction of the ℓ_i-isogenies $(\pm)$
- final vertex of the path: A’

Key exchange example

An example with $p = 59$. The starting vertex is fixed to 0.

$x_A = 6$ →

← $x_B = 28$



Alice: $\boxed{a = (2, -1)}$

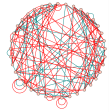
$\Rightarrow x_A = 6$

Bob: $\boxed{b = (-1, -2)}$

$\Rightarrow x_B = 28$

$K_{ab} = 11$

More on isogeny-based cryptography



1997
Couveignes

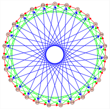
Hard homogeneous space
Group-action based cryptography
→ DH key exchange with isogenies.

Public-key cryptosystem based on isogenies
Independent discovery of Couveigne's (unpublished) ideas.

2006
Rostovtsev, Stolbunov

CGL hash function Cryptographic hash functions from expander graphs.

2009
Charles, Goren, Lauter



SIDH
Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies

2011
de Feo, Jao

CSIDH:
an efficient post-quantum commutative group action

2018,
Castryck, Lange, Martindale, Panny, Renes

SQISign:
compact post-quantum signatures from quaternions and isogenies

2020
de Feo, Kohel, Leroux, Petit, Wesolowski

most recent advances: isogenies of (higher dimensional) abelian varieties

- Cryptanalysis
- Improvements
- New constructions

Thanks