Supersingular Isogeny Diffie-Hellman

Valeriia Kulynych

Université de Toulon

May 25th, 2018

Outline

Elliptic curves

Definition

An elliptic curve is a pair (E, O), where E is a curve of genus 1 and $O \in E$.

- We consider curves defined over field K with characteristic $p > 0$.
- Composition law is defined as follows: Let $P, Q \in E$, L be the line connecting P and Q (tangent line to E if $P = Q$), and R be the third point of intersection of L with E. Let L' be the line connecting R and O. Then $P \oplus Q$ is the point such that L' intersects E at R, O and $P \oplus Q$.

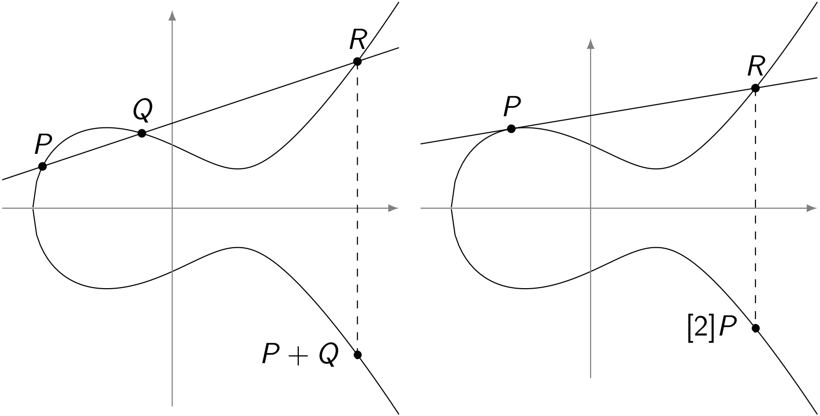

Figure: An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.

Supersingular Elliptic Curves

Definition

For every n, we have a multiplication map

$$[n] : E \to E$$

$$P \mapsto \underbrace{P \oplus \cdots \oplus P}_{n \text{ times}}.$$

Its kernel is denoted by $E[n]$ and is called the n-torsion subgroup of E. Then one can show that for any $r \geq 1$:

$$E[p^r](\bar{K}) \simeq \begin{cases} 0 \\ \mathbb{Z}/p^r\mathbb{Z} \end{cases}$$

In the first case, E is called supersingular. Otherwise, it is called ordinary.

Isogenies

Definition

Let E_1 and E_2 be elliptic curves defined over a finite field $\mathbb{F}_q$ of characteristic p. An isogeny $\phi : E_1 \to E_2$ defined over $\mathbb{F}_q$ is a non-constant morphism that maps the identity into the identity (and this a is group homomorphism).

Theorem (Sato-Tate)

Two elliptic curves E_1 and E_2 are isogenous over $\mathbb{F}_q$ if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

Isogenies

- Curves in the same isogeny class are either all supersingular or all ordinary.
- The degree of an isogeny ϕ is the degree of ϕ as a morphism. An isogeny of degree ℓ is called ℓ-isogeny.
- An isogeny could be identified with its kernel.Given a subgroup G of E, we can use Velu's formulas to compute an isogeny $\phi : E_1 \to E_2$ with kernel G and such that $E_2 \simeq E_1/G$.

Isogeny graphs

Definition

Let E be an elliptic curve over a field K. Let $S \subseteq \mathbb{N}$ be a finite set of primes. Define

$$X_{E,K,S}$$

to be the graph with vertex set being the K-isogeny class of E. Vertices are typically labelled by $j(E)$. There is an edge $(j(E_1), j(E_2))$ labelled by ℓ for each equivalence class of ℓ-isogenies from E_1 to E_2 defined over K for some $\ell \in S$. This graph is called isogeny graph.

Supersingular isogeny graph is always

- conncted;
- $\ell + 1$-regular, where ℓ is isogeny degree.

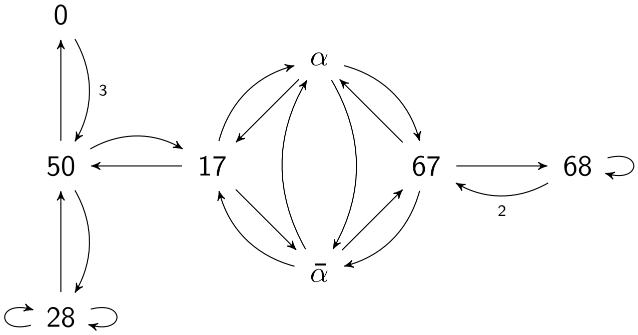

Figure: Supersingular Isogeny Graph $X_{\bar{\mathbb{F}}_{83},2}$

Classic Diffie-Hellman

Public parameters	A prime p, $p-1$ has large prime cofactor. A multiplicative generator $g \in \mathbb{Z}/p\mathbb{Z}$.	
	Alice	**Bob**
Pick random secret	$0 < a < p-1$	$0 < b < p-1$
Compute public data	$A = g^a$	$B = g^b$
Exchange data	$A \longrightarrow$	$\longleftarrow B$
Compute shared secret	$S = B^a$	$S = A^b$

- The protocol can be generalized by replacing the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ with anny other cyclic group $G = \langle g \rangle$.

Security of DH

Definition (Discrete logarithm problem)

Let G be a cyclic group generated by an element g. For any element $A \in G$, find the dicrete logarithm of A in base g, denoted $\log_g(A)$, as the unique integer in the interval $[0, \#G[$ such that

$$g^{\log_g(A)} = A.$$

We know several algorithms to compute discrete logarithms:

- in *generic* group G that require $O(\sqrt{(}q))$ computational steps, where q is the largest prime divisor of $\#G \implies G$ is usually chosen such that $\log_2 q \simeq 256$;
- in group $G = (\mathbb{Z}/p\mathbb{Z})^*$ of complexity better than $O(\sqrt{\#G})$.

Elliptic Curve Diffie-Hellman

Public parameters	Finite field $\mathbb{F}_p$, with $\log_2 p \simeq 256$, Elliptic curve $E/\mathbb{F}_p$, $\#E(\mathbb{F}_p)$ is prime, A generator P of $E(\mathbb{F}_p)$.	
	Alice	**Bob**
Pick random secret	$0 < a < \#E(\mathbb{F}_p)$	$0 < b < \#E(\mathbb{F}_p)$
Compute public data	$A = [a]P$	$B = [b]P$
Exchange data	$A \longrightarrow$	$\longleftarrow B$
Compute shared secret	$S = [a]B$	$S = [b]A$

Security of ECDH

Background

Let $G = (E, V)$ be an undirected graph, where $V = \{v_i | i \in I\}$ is the set of vertices, and E is the set of edges. A random walk of length i is a path $v_1 \to \cdots v_i$, defined by the random process that selects v_i uniformly at random among the neighbors of v_{i-1}.

Why do we use supersingular isogenies?

- One isogeny degree is sufficient to obtain an expander graph $\sim$ graph with short diameter and rapidly mixing walks $\implies$ we can construct more efficient protocols.
- There is no action of an abelian group on them $\implies$ harder to use quantum computers to speed up the supersingular isogeny path problem.

Idea of SIDH

- Secrets: Alice and Bob take secret random walks in two distinct isogeny graphs on the same vertex set. Alice's walk has length ε_A and Bob's has length ε_B.
  - *On practice*, we choose a large prime p and small primes ℓ_A and ℓ_B. The vertex set is elliptic curves j-invariant over $\mathbb{F}_{p^2}$. Alice's graph consists of ℓ_A-isogenies, Bob's - of ℓ_B-isogenies.
- Key idea: A walk of length ε_A in the ℓ_A-isogeny graph corresponds to a kernel of a size $\ell_A^{\varepsilon_A}$, and this kernel is cyclic $\iff$ the walk does not backtrack.
  - *On practice*, choosing a secret walk of length ε_A is equivalent to choosing a secret cyclic subgroup $\langle A \rangle \subset E[\ell_A^{\varepsilon_A}]$.
- Shared secret: A subgroup $\langle A \rangle + \langle B \rangle = \langle A, B \rangle$ defines an isogeny to $E/\langle A, B \rangle$. Since we choose $\ell_A \neq \ell_B$, the group $\langle A, B \rangle$ is cyclic of order $\ell_A^{\varepsilon_A} \ell_B^{\varepsilon_B}$.

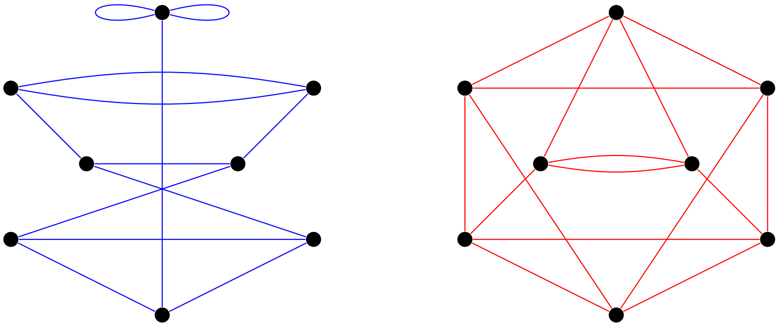

Figure: Supersingular isogeny graphs of degree 2 (left, blue) and 3 (right, red) on $\mathbb{F}_{97^2}$.

Illustration of SIDH

$$\ker \alpha = \langle A \rangle \subset E[\ell_A^{e_A}]$$

$$\ker \beta = \langle B \rangle \subset E[\ell_B^{e_B}]$$

$$\ker \alpha' = \langle \beta(A) \rangle$$

$$\ker \beta' = \langle \alpha(B) \rangle$$

$$\begin{tikzcd} E \arrow[r, "\alpha"] \arrow[d, "\beta"'] & E/\langle A \rangle \arrow[d, "\beta'"] \\ E/\langle B \rangle \arrow[r, "\alpha'"'] & E/\langle A, B \rangle \end{tikzcd}$$

Figure: Commutative isogeny diagram constructed from Alice's and Bob's secrets. Quantities known to Alice are drawn in blue, those known to Bob are drawn in red.

The problems we face

1. The points of $\langle A \rangle$ (or $\langle B \rangle$) may not be rational.
2. The diagram on previous slide shows no way how Alice and Bob could compute shared secret $E/\langle A, B \rangle$ without revealing their secrets.

Solutions

- In case of supersingular curves, we can control the group structure. It turns out that as we are dealing with the field $\mathbb{F}_p^2$ then
$$E(\mathbb{F}_q) \simeq (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2$$
.