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 $P \oplus Q$.

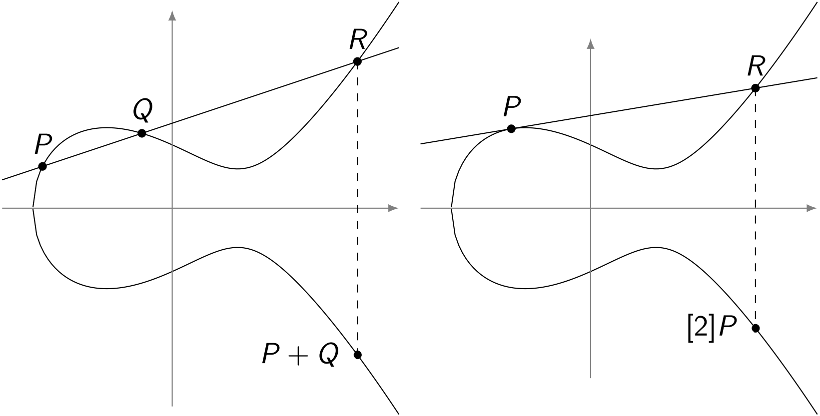

Figure: An elliptic curve defined over $\mathbb{R}$, and the geometric representation of its group law.

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 $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.

- 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.

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.

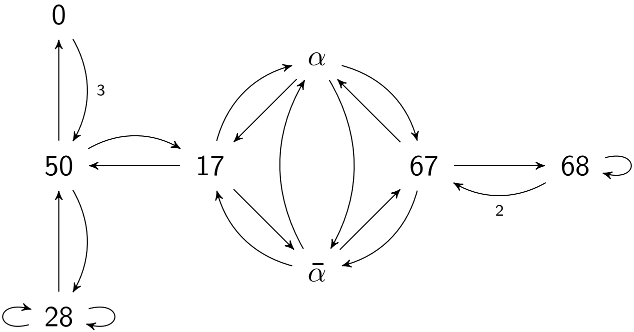

Figure: Supersingular Isogeny Graph $X_{\bar{\mathbb{F}}_{83},2}$

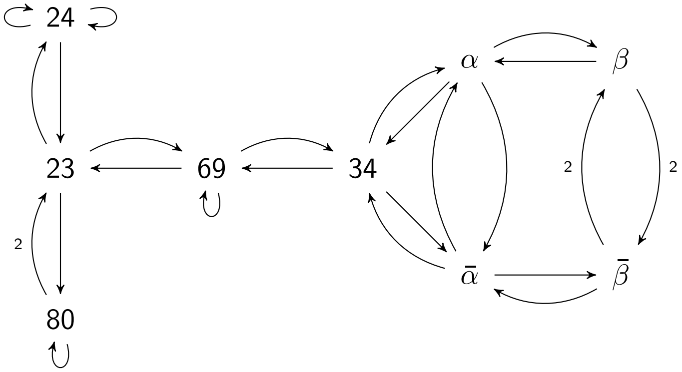

Figure: Supersingular Isogeny Graph $X_{\bar{\mathbb{F}}_{103},2}$

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 Classic Diffie-Hellman

Definition (Discrete logarithm)

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

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