

Supersingular Isogeny Diffie-Hellman

Valeriia Kulynych

Université de Toulon

May 25th, 2018

Outline

- 1 Supersingular Elliptic Curves
- 2 Isogeny Graphs
- 3 Diffie-Hellman Key Exchange Protocol
 - Classic Diffie-Hellman
 - Elliptic Curve Diffie-Hellman
 - Supersingular Isogeny Diffie-Hellman

Elliptic curves

Definition

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

- 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 $P \oplus Q$.

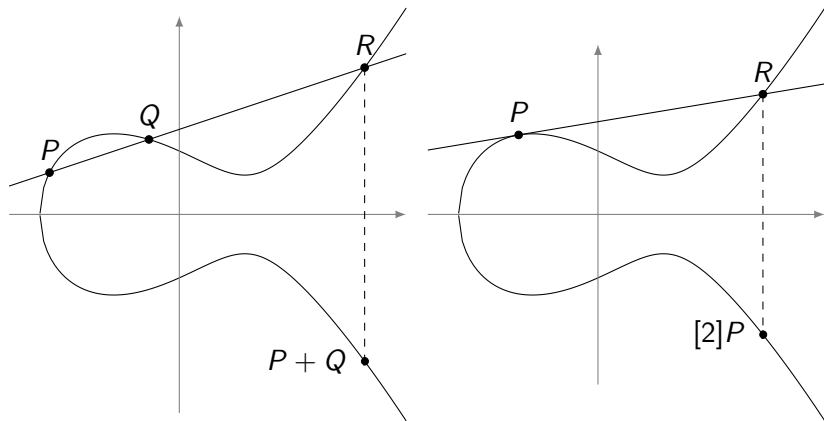


Figure: An elliptic curve defined over \mathbb{R} , and the geometric representation of its group law.

Supersingular Elliptic Curves

Definition

For every n , we have a multiplication map

$$[n] : E \rightarrow E$$

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

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** $\phi : E_1 \rightarrow E_2$ defined over \mathbb{F}_q is a non-constant morphism that maps the identity into the identity (and this is a 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 $\phi : E_1 \rightarrow E_2$ 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

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

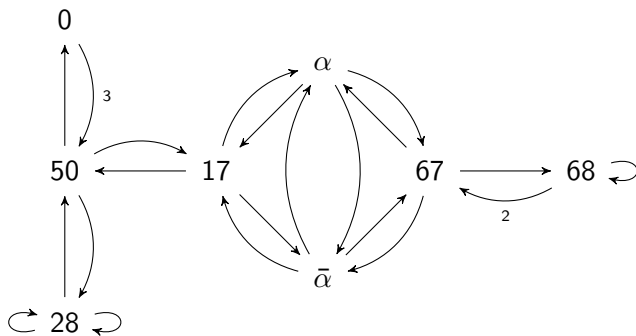


Figure: Supersingular Isogeny Graph $X_{\bar{\mathbb{F}}_{83},2}$

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 any 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 **discrete 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	$S = [a]B$	$S = [b]A$

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 $v_1 \rightarrow \cdots v_i$, 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 $\ell_A^{\varepsilon_A} \ell_B^{\varepsilon_B}$.

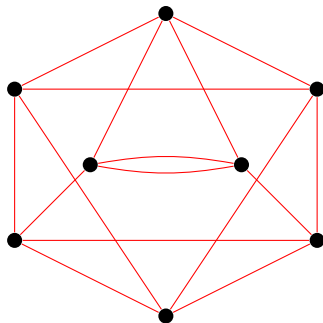
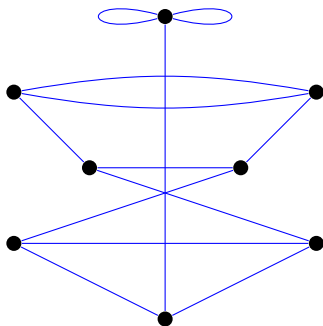


Figure: Supersingular isogeny graphs of degree 2 (left, blue) and 3 (right, red) on \mathbb{F}_{97^2} .

Illustration of SIDH

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

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

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

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

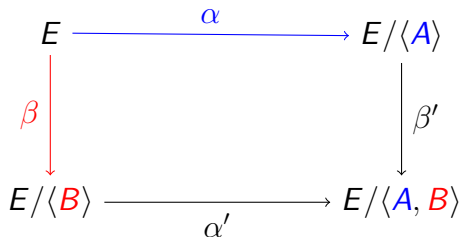


Figure: Commutative isogeny diagram constructed from Alice's and Bob's secrets. Quantities known to Alice are drawn in blue, those known to Bob are drawn in red.

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.

Solution of the 1st problem

- 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

$$E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2.$$

- We choose p so that $E(\mathbb{F}_{p^2})$ contains two large subgroups $E[\ell_A^{\varepsilon_A}]$ and $E[\ell_B^{\varepsilon_B}]$ of coprime order.
- Once subgroups are fixed, we look for a prime of the form $p = \ell_A^{\varepsilon_A} \ell_B^{\varepsilon_B} f \mp 1$, where f is a small cofactor.
 - *On practice*, we can choose $f = 1$.

$\implies E(\mathbb{F}_p^2)$ contains $\ell_A^{\varepsilon_A - 1}(\ell_A + 1)$ cyclic subgroups of order $\ell_A^{\varepsilon_A}$, each defining a distinct isogeny; \implies a single point $A \in E(\mathbb{F}_q)$ is enough to represent an isogeny walk of length ε_A .

Solution of the 2nd problem

Solution is to publish some additional data.

- They have publicly agreed on a prime p and a supersingular curve E such that

$$E(\mathbb{F}_{p^2}) \simeq (\mathbb{Z}/\ell_A^{\epsilon_A}\mathbb{Z})^2 \oplus (\mathbb{Z}/\ell_B^{\epsilon_B}\mathbb{Z})^2 \oplus (\mathbb{Z}/f\mathbb{Z})^2.$$

- They fix public bases of their respective torsion groups:

$$E[\ell_A^{\epsilon_A}] = \langle P_A, Q_A \rangle,$$

$$E[\ell_B^{\epsilon_B}] = \langle P_B, Q_B \rangle.$$

- They choose random secret subgroups defined as follows

$$\langle A \rangle = \langle [m_A]P_A + [n_A]Q_A \rangle \subset E[\ell_A^{\epsilon_A}],$$

$$\langle B \rangle = \langle [m_B]P_B + [n_B]Q_B \rangle \subset E[\ell_B^{\epsilon_B}].$$

Solution of the 2nd problem

- After computing secret isogenies α and β , Alice publishes $\alpha(P_B)$ and $\alpha(Q_B)$ and Bob publishes $\beta(P_A)$ and $\beta(Q_A)$.
- Alice computes $\beta(A) = [m_A]\beta(P_A) + [n_A]\beta(Q_A)$ and Bob computes $\alpha(B) = [m_B]\alpha(P_B) + \alpha(Q_B)$.
- They compute isogenies α', β' , whose kernels are generated respectively by $\langle \beta(A) \rangle$ and $\langle \alpha(A) \rangle \implies$ They compute the shared secret $E/\langle A, B \rangle$.

Parameters	Primes $\ell_A, \ell_B, p = \ell_A^{\varepsilon_A} \ell_B^{\varepsilon_B} f \mp 1$, A supersingular curve E over \mathbb{F}_{p^2} of order $(p \pm 1)^2$, A basis $\langle P_A, Q_A \rangle$ of $E[\ell_A^{\varepsilon_A}]$, A basis $\langle P_B, Q_B \rangle$ of $E[\ell_B^{\varepsilon_B}]$,	
	Alice	Bob
Random secret	$A = [m_A]P_A + [n_A]Q_A$	$B = [m_B]P_B + [n_B]Q_B$
Secret isogeny	$\alpha : E \rightarrow E_A = E/\langle \alpha A \rangle$	$\beta : E \rightarrow E_B = E/\langle B \rangle$
Exchange data	$E_A, \alpha(P_B), \alpha(Q_B) \longrightarrow$	$\longleftarrow E_B, \beta(P_A), \beta(Q_A)$
Shared secret	$E/\langle A, B \rangle = E_B/\langle \beta(A) \rangle$	$E/\langle A, B \rangle = E_A/\langle \alpha(B) \rangle$

Figure: Supersingular Isogeny Diffie-Hellman key exchange protocol.

Security of SIDH

Definition (Supersingular Decision Diffie-Hellman)

Given a tuple sampled with probability $1/2$ from one of the following two distributions:

1 $(E/\langle A \rangle, \phi(P_B), \phi(Q_B), E/\langle B \rangle, \psi(P_A), \psi(Q_A), e/\langle A, B \rangle)$, where

- $A \in E$ is a uniformly random point of order $\ell_A^{\varepsilon_A}$,
- $B \in E$ is a uniformly random point of order $\ell_B^{\varepsilon_B}$,
- $\phi : E \rightarrow E/\langle A \rangle$ is the isogeny of kernel $\langle A \rangle$, and
- $\psi : E \rightarrow E/\langle B \rangle$ is the isogeny of kernel $\langle B \rangle$;

2 $(E/\langle A \rangle, \phi(P_B), \phi(Q_B), E/\langle B \rangle, \psi(P_A), \psi(Q_A), E/\langle C \rangle)$, where A, B, ϕ, ψ are as above, and where $C \in E$ is a uniformly random point of order $\ell_A^{\varepsilon_A} \ell_B^{\varepsilon_B}$;

determine from which distribution the tuple is sampled.

Security of SIDH

- The best known algorithms for SSDDH have **exponential complexity**, even on a quantum computer.
- Although there is no efficient algorithms to solve SSDDH at the time of writing, several polynomial-time attacks have appeared against variations of SIDH.

Analogue between DH instantiations

	DH	ECDH	SIDH
Elements	Integers g modulo prime	Points P in elliptic curve group	Curves E in isogeny class
Secrets	Exponents x	scalars k	isogenies ϕ
Computations	$(g, x) \rightarrow g^x$	$(P, k) \rightarrow [k]P$	$(E, \phi) \rightarrow \phi(E)$
Hard problem	Given g, g^x . Find x	Given $P, [k]P$. Find k	Given $E, \phi(E)$. Find ϕ

IsogenyCryptoDeFeo Luca De Feo. *Mathematics of isogeny based cryptography*, Lecture notes, École Mathématique Africaine, Thiès, Sénégal, 2017, 44 pp.

<https://arxiv.org/abs/1711.04062> Luca De Feo, David Jao, Jerome Plut. *Towards Quantum-Resistant Cryptosystems From Supersingular Elliptic Curve Isogenies*, Journal of Mathematical Cryptology, 2014, 8 (3), pp. 209-247.

<https://eprint.iacr.org/2011/506.pdf> Steven D. Galbraith and Ilya Chevyrev. *Distinguishing Maximal Orders of Quaternion Algebra by their Shoert Elements*. ANTS, 2014, August 7, 2014, Korea. [https://www.math.auckland.ac.](https://www.math.auckland.ac.nz/~sgal018/ANTS2014.pdf)

[nz/~sgal018/ANTS2014.pdf](https://www.math.auckland.ac.nz/~sgal018/ANTS2014.pdf) Antoine Joux. *Algorithmic*

cryptanalysis. CRC Press, 2009. Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992.