Supersingular Isogeny Diffie-Hellman (SIDH)

Katharina Koschatko

16.01.2020

Motivation

- FFDH and ECDH security relies on DLP
- Broken with quantum computer + Shor’s algorithm
- What we want:

Post quantum security

- NIST calling for **Post-Quantum Cryptography** proposals (November 30th , 2017)
- Approaches based on: lattices, hash functions, ...

  ... and: **isogenies**

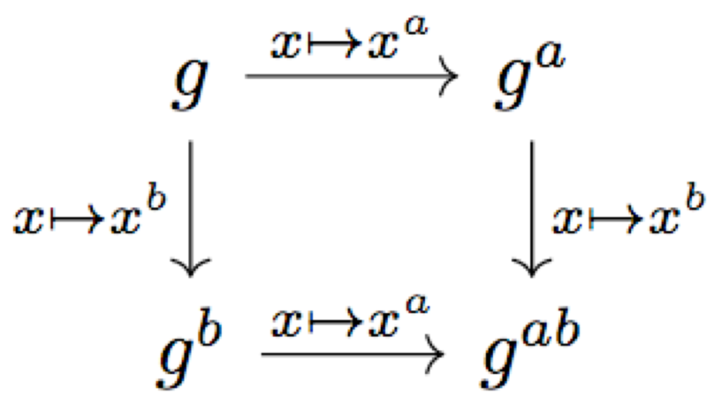
Outline

- Diffie-Hellman Key Agreement
- Supersingular Isogeny Diffie-Hellman (SIDH)
- Objects used in Supersingular Isogeny Cryptography
- Isogenies and isogenous elliptic curves
- Random walks in Supersingular Isogeny Graphs
- **Supersingular Isogeny Diffie-Hellman (SIDH)**

Diffie-Hellman Key Agreement

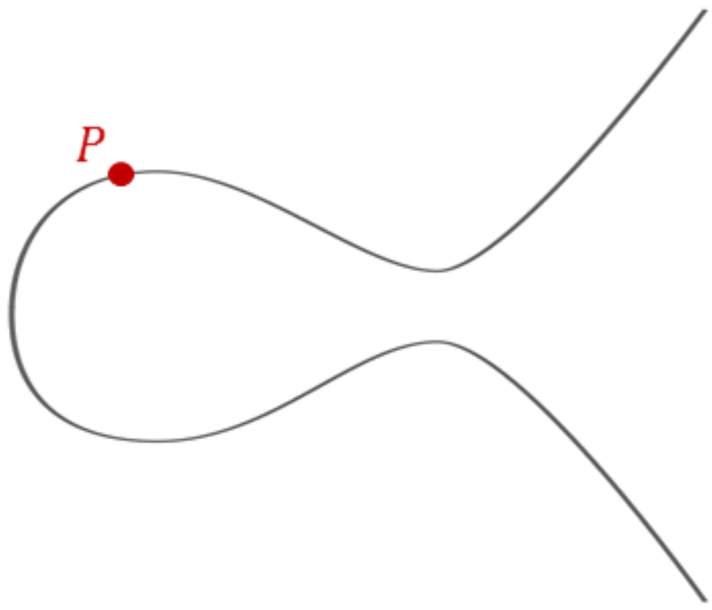
Finite Field Diffie-Hellman (FFDH)

- Given: prime p and a generator g of $\mathbb{Z}_p^*$
- Choose private keys: a, b
- Exchange public keys: g^{a}, g^b
- Compute shared secret: $g^{\mathrm{ab}} = \left(g^b\right)^a = (g^a)^b$



Elliptic Curve Diffie-Hellman (ECDH)

- Given: elliptic curve E and a point $P \in E(\mathbb{F}_p)$
- Choose private keys: a, b
- Exchange public keys: aP, bP
- Compute shared secret: $abP = a(bP) = b(aP)$



Supersingular Isogeny Diffie-Hellman (SIDH)

- Given:
  - Collection $\mathcal{J}$ of „special elliptic curves” over a finite field $\mathbb{F}_{p^2}$ that are somehow related to each other.
  - One „special elliptic curve“ E from this collection

- Idea:
  - Alice somehow gets from E to $E_A \in \mathcal{J}$ via $\phi_A: E \rightarrow E_A$
  - Bob secretly gets from E to $E_B \in \mathcal{J}$ via $\phi_B: E \rightarrow E_B$
  - Alice and Bob exchange E_A and E_B
  - Alice computes “shared” secret curve $E_{BA} = \phi'_A(E_B)$
  - Bob computes “shared” secret curve $E_{AB} = \phi'_B(E_A)$

Supersingular Isogeny Diffie-Hellman (SIDH)

What is unclear so far:

(1) How does Alice get to E_A? What is the secret?

How does Bob get to E_B? What is the secret?

→ **isogenies** and **isogeny graphs**

(2) How does Alice get to E_{BA}?

How does Bob get to E_{AB}?

→ **m-torsion** subgroups of $\mathrm{E}(\mathbb{F}_{p^2})$, **basis** points

(3) What is the "shared" secret here?

→ elliptic curve **isomorphisms** and **j-invariants**

Before we are getting started

In supersingular isogeny cryptography ...

- What does the finite field $\mathbb{F}_{p^2}$ look like?
  - $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ with $i^2 + 1 = 0$
  - e_A and e_B fixed public parameters
  - $p = 2^{e_A}3^{e_B} - 1$
- What does the abelian group $E(\mathbb{F}_{p^2})$ look like?
  - $E(\mathbb{F}_{p^2}) = \{(x, y) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$
  - Montgomery curve: $\mathrm{A}, B \in \mathbb{F}_{p^2}$ s.t. $B(A^2 - 4) \neq 0$ in $\mathbb{F}_q$

$$\mathrm{E_{AB}} : By^2 = x^3 + Ax^2 + x \quad \text{for}$$

Isogenies

Isogenies

Definition

Let E_1 and E_2 be elliptic curves over a finite field $\mathbb{F}_q$. An **isogeny** $\phi: E_1 \to E_2$ is a non-constant rational map defined over $\mathbb{F}_q$ which is also a group homomorphism from $E_1(\mathbb{F}_q)$ to $E_2(\mathbb{F}_q)$. If such a map exists we say E_1 is **isogenous** to E_2.

Group homomorphism:

- $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$
- $\forall\, P, Q \in E_1(\mathbb{F}_q) : \phi([m]P + [n]Q) = [m]\phi(P) + [n]\phi(Q)$

Isogenies, cnt.

- Two curves E_1 and E_2 are isogenous if any only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.
- An isogeny ϕ can be expressed in terms of two rational maps f and g over $\mathbb{F}_q$ such that

$$\phi\big((x,y)\big) = (f(x), y \cdot g(x))$$

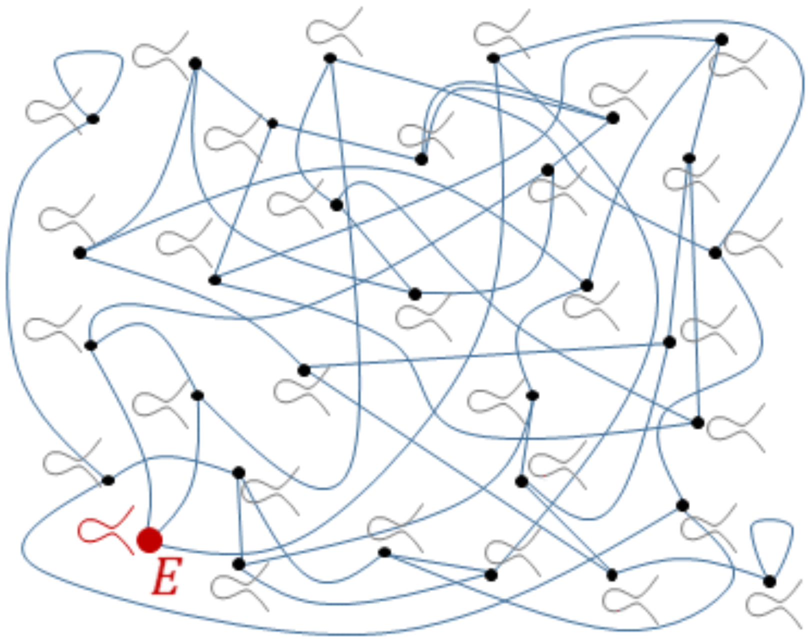
- f (and similarly g) can be written as $f(x) = \frac{p(x)}{q(x)}$ with polynomials $p(x)$ and $\mathrm{q}(x)$ over $\mathbb{F}_q$ that do not have a common factor.
- The degree $\deg(\phi)$ of the isogeny is defined as

$$\max\{\deg(p(x)), \deg(q(x))\}$$

Supersingular isogeny graphs

Consider $\mathbb{F}_{p^2}$ and super-singular elliptic curves.

- **Vertices**: all isogenous elliptic curves over $\mathbb{F}_{p^2}$.
- **Edges**: isogenies of a fixed prime degree ℓ (here: $\ell = 2$)



Connected, $(\ell + 1)$-regular graph.

Isogenies and subgroups of $E(\mathbb{F}_q)$

Theorem

For any finite subgroup H of $E(\mathbb{F}_q)$, there is a **unique** isogeny (up to isomorphism) $\phi: E \to E'$ such that

- $\ker(\phi) = H$, and
- $\deg(\phi) = |H|$,

where $|H|$ denotes the cardinality of H.

- In this case, we denote by E/H the curve E'.
- Given a subgroup $H \subseteq E(\mathbb{F}_q)$, Vélu's formulas can be used to find the isogeny ϕ and isogenous curve E/H.
- Vélu's formulas are computationally impractical for arbitrary groups.

Computation of 2-isogenies

Let $(x_2, y_2) \in E_{AB}$ be a point of order 2 with $x_2 \neq \pm 0$ and let $\phi_2 : E_{AB} \to E_{A'B'}$ be the unique (up to isomorphism) 2-isogeny with kernel $\ker(\phi_2) = \langle (x_2, y_2) \rangle$.

- The isogenous curve $E_{A'B'}$ can be computed as

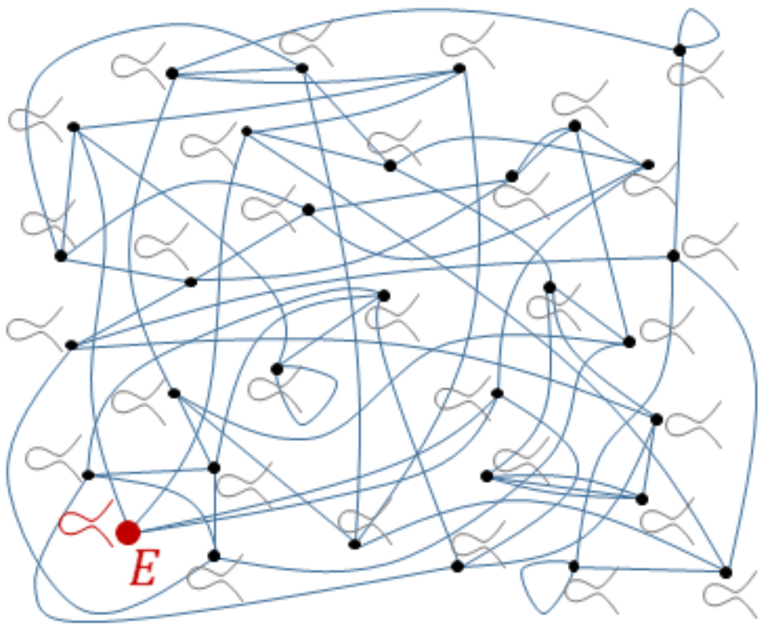
$$(A', B') = (2 \cdot (1 - 2x_2^2), B \cdot x_2)$$

- $\forall\, P \in E_{AB}(\mathbb{F}_q) \setminus \langle (x_2, y_2) \rangle :\ \phi_2 : (x_p, y_p) \mapsto (x_{\phi_2(P)}, y_{\phi_2(P)})$
  - $x_{\phi_2(P)} = f(x_2) = \frac{p(x_2)}{q(x_2)} = \frac{x_p^2 x_2 - x_p}{x_p - x_2}$
  - $y_{\phi_2(P)} = y_p \cdot g(x_2) = y_p \cdot \frac{x_p^2 x_2 - 2x_p x_2^2 + x_2}{(x_p - x_2)^2}$

What about large-degree isogenies?

Isogeny $\phi: E \to E/H$ for general subgroups H with $\deg(\phi) = |H| = \ell$ can be described as the composition of several 2-isogenies (or 3-isogenies):

$$\phi_n = \phi_{n-1} \circ \phi_{n-2} \circ \cdots \circ \phi_0$$



In other words:

Find a **random walk** in a supersingular isogeny graph.

Supersingular Isogeny Diffie-Hellman (SIDH)

Given a supersingular isogeny class $\mathcal{J}$ (over finite field $\mathbb{F}_{p^2}$ with $p = 2^{e_A}3^{e_B} - 1$) and a starting curve $E \in \mathcal{J}$.

Alice

- Secret key: cyclic group $\langle R_A \rangle$ of order 2^{e_A}
  $$\phi_A := E/\langle R_A \rangle$$
- Public key: curve
  $$E_A = \phi_A(E)$$
- New isogeny:
  $$\phi'_A := E_B/\langle \phi_B(R_A) \rangle$$
- Shared secret:
  $$E_{BA} = \phi'_A(E_B)$$

Bob

- Secret key: cyclic group $\langle R_B \rangle$ of order 3^{e_B}
  $$\phi_B := E/\langle R_B \rangle$$
- Public key: curve
  $$E_B = \phi_B(E)$$
- New isogeny:
  $$\phi'_B := E_A/\langle \phi_A(R_B) \rangle$$
- Shared secret:
  $$E_{AB} = \phi'_B(E_A)$$

Given a supersingular isogeny class $\mathcal{J}$ (over finite field $\mathbb{F}_{p^2}$ with $p = 2^{e_A}3^{e_B} - 1$) and a starting curve $E \in \mathcal{J}$.

Alice

- Secret key: cyclic group $\langle R_A \rangle$ of order 2^{e_A}

  $$\phi_A := E/\langle R_A \rangle$$

- Public key: curve

  $$E_A = \phi_A(E)$$

- New isogeny:

  $$\phi'_A := E_B/\langle \phi_B(R_A) \rangle$$

- Shared secret:

  $$E_{BA} = \phi'_A(E_B)$$

Bob

- Secret key: cyclic group $\langle R_B \rangle$ of order 3^{e_B}

  $$\phi_B := E/\langle R_B \rangle$$

- Public key: curve

  $$E_B = \phi_B(E)$$

- New isogeny:

  $$\phi'_B := E_A/\langle \phi_A(R_B) \rangle$$

- Shared secret:

  $$E_{AB} = \phi'_B(E_A)$$

m-torsion

Definition

For a positive integer m, the set $E[m]$ of **m-torsion elements** of an elliptic curve $E(\mathbb{F}_q)$ is defined as the set of points in $\mathrm{E}(\overline{\mathbb{F}}_q)$ such that $[m]P = \mathcal{O}$. $E[m]$ is a subgroup of $E(\mathbb{F}_q)$ and is called **m-torsion subgroup**.

- Let $\langle P_A, Q_A \rangle = E[2^{e_A}]$, i.e. P_A and Q_A form a basis of $E[2^{e_A}]$
- Let $\langle P_B, Q_B \rangle = E[2^{e_B}]$, i.e. P_B and Q_B form a basis of $E[2^{e_B}]$
- Alice chooses $R_A = m_A P_A + n_A Q_A$
- Bob chooses $R_B = m_B P_B + n_B Q_B$
- m_A, n_A, m_B, n_B are kept secret, P_A, Q_A, P_B, Q_B are public

Given a SI class $\mathcal{J}$, a starting curve $E \in \mathcal{J}$, points P_A, Q_A, P_B, Q_B.

Alice

- Secret key:
  - $R_A = m_A P_A + n_A Q_A$
  - $\phi_A := E/\langle R_A \rangle$
- Public key:
  - $E_A = \phi_A(E), \phi_A(P_B), \phi_A(Q_B)$ ⟷
- New isogeny:

$$\phi'_A := E_B/\langle \phi_B(R_A) \rangle$$

$$\phi_B(R_A) = \phi_B(m_A P_A + n_A Q_A) = m_A \phi_B(P_A) + n_A \phi_B(Q_A)$$

- Shared secret:

$$E_{BA} = \phi'_A(E_B)$$

Bob

- Secret key:
  - $R_B = m_B P_B + n_B Q_B$
  - $\phi_B := E/\langle R_B \rangle$
- Public key:
  - $E_B = \phi_B(E), \phi_B(P_A), \phi_B(Q_A)$
- New isogeny:

$$\phi'_B := E_A/\langle \phi_A(R_B) \rangle$$

$$\phi_A(R_B) = \phi_A(m_B P_B + n_B Q_B) = m_B \phi_A(P_B) + n_B \phi_A(Q_B)$$

- Shared secret:

$$E_{AB} = \phi'_B(E_A)$$

Given a SI class $\mathcal{J}$, a starting curve $E \in \mathcal{J}$, points P_A, Q_A, P_B, Q_B.

Alice

- Secret key:
  - $R_A = m_A P_A + n_A Q_A$
  - $\phi_A := E/\langle R_A \rangle$
- Public key:
  - $E_A = \phi_A(E), \phi_A(P_B), \phi_A(Q_B)$
- New isogeny:

$$\phi'_A := E_B/\langle \phi_B(R_A) \rangle$$

$$\phi_B(R_A) = \phi_B(m_A P_A + n_A Q_A) = m_A \phi_B(P_A) + n_A \phi_B(Q_A)$$

- Shared secret:

$$E_{BA} = \phi'_A(E_B)$$

Bob

- Secret key:
  - $R_B = m_B P_B + n_B Q_B$
  - $\phi_B := E/\langle R_B \rangle$
- Public key:
  - $E_B = \phi_B(E), \phi_B(P_A), \phi_B(Q_A)$
- New isogeny:

$$\phi'_B := E_A/\langle \phi_A(R_B) \rangle$$

$$\phi_A(R_B) = \phi_A(m_B P_B + n_B Q_B) = m_B \phi_A(P_B) + n_B \phi_A(Q_B)$$

- Shared secret:

$$E_{AB} = \phi'_B(E_A)$$

j-invariant

Definition

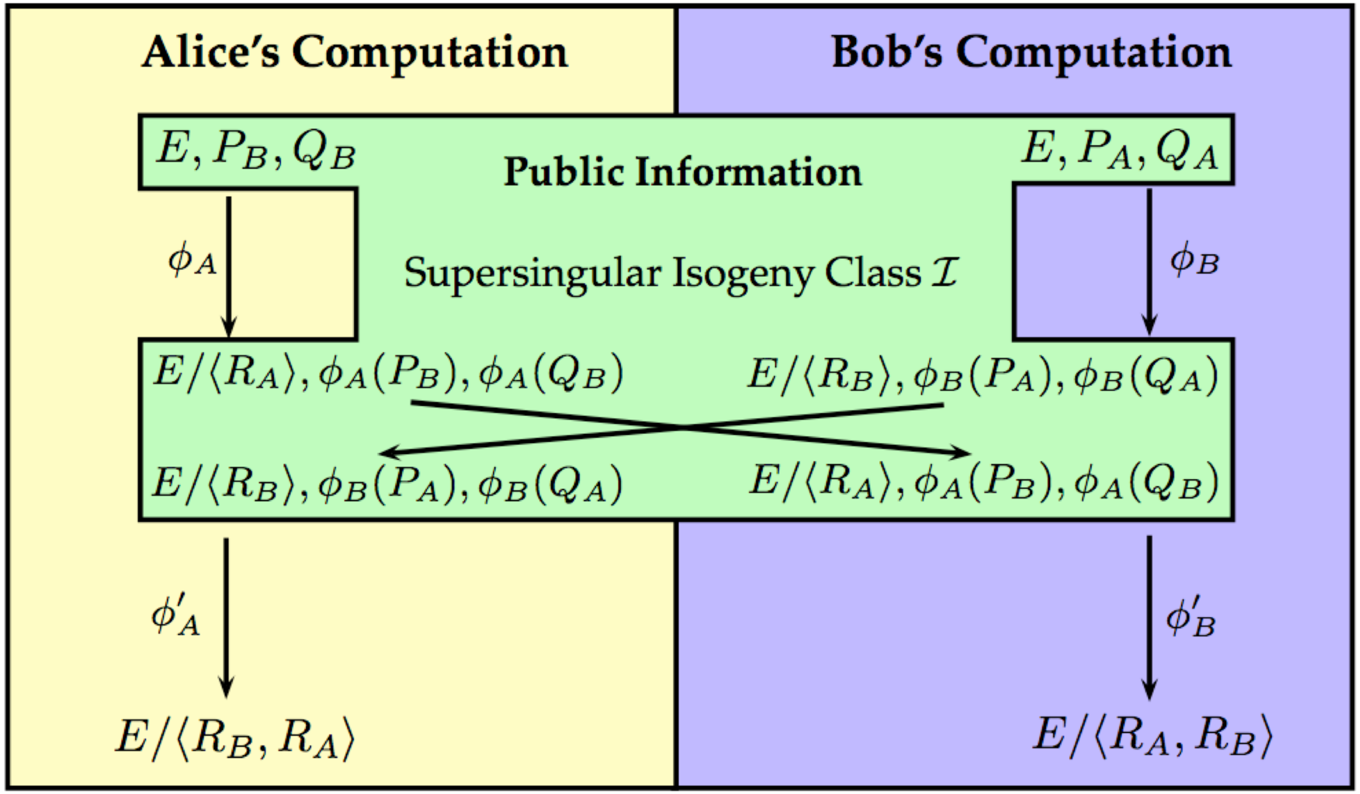
The j-invariant of an elliptic curve E_{AB} is computed as

$$j(E_{AB}) = \frac{256(A^2-3)^3}{A^2-4}.$$

The j-invariant of an elliptic curve over a field $\mathbb{F}_q$ is unique up to isomorphism of the elliptic curve.

- j-invariant is often used as shared secret since in supersingular isogeny cryptography since E_{AB} and E_{BA} are isomorphic.

SIDH



- Based on hidden-isogeny-problem.
- Not affected by Shor‘s algorithm.
- Affected by Grover‘s algorithm: double isogeny graph

Bibliography

- Luca De Feo. Mathematics of Isogeny Based Cryptography, 2017.
- Steven Galbraith and Frederik Vercauteren, Computational problems in supersingular elliptic curve isogenies, 2017.
- Wouter Castryck. Elliptic curves are quantum dead, long live elliptic curves, 2017.
- David Urbanik. A friendly introduction to Supersingular Isogeny Diffie-Hellman, 2017.
- Michael Naehrig. Supersingular Isogeny Diffie-Hellman, Real-World Cryptography Conference 2017, 2017.
- David Jao. Supersingular Isogeny Key Encapsulation. Submission to NIST standardization process on post-quantum cryptography, 2017.