A GENTLE INTRODUCTION TO SIDH

Federico Pintore

Most of the cryptographic schemes which use elliptic curves base their security on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). However, we should have said "on the classic hardness", since the ECDLP is hard for classic computers but it is "easy" for quantum computers (thanks to Shor's algorithm). This means that the elliptic-curve cryptosystems that we are currently using would be not secure in the presence of quantum computers.
In recent years, cryptographers have proposed new ways of using elliptic curves to construct cryptographic scheme, whose security is based on a problem different from the ECDLP. Such a problem involves the computation of a particular map - called isogeny - between two given elliptic curves, and it is difficult not just for classic computers, but even for quantum computers (so far!).
These proposals led to a new branch in cryptography: Isogeny-Based Cryptography. The above mentioned feature makes isogeny-based schemes good candidates for post-quantum cryptography, since they can be implemented by classical computers, but are resistant to attacks conducted by quantum computers.

So far, several isogeny-based schemes have been proposed. Here we want to present the (arguably) most famous: the Supersingular Isogeny Diffie-Hellman, SIDH in short. As the name suggests, such a protocol is a key-exchange *à la* Diffie-Hellman, and it uses isogenies.

■ 1.1 - Elliptic curves over Finite Fields

Let $\mathbb{F}_q$ a Finite Field, where q is a prime power p^m. We assume $p>3$.
An elliptic curve E defined over $\mathbb{F}_q$ is the locus of zeros of a cubic, bivariate polynomial of the form

$$y^2 - (x^3 + Ax + B) \quad \text{with } 4A^3 + 27B^2 \neq 0$$

where A, B belongs to $\mathbb{F}_q$, together with another element ∞, which is a formal point called "point at infinity". In other words:

$$E = \{ (x_0, y_0) \in \overline{\mathbb{F}_q} \mid (y_0)^2 = (x_0)^3 + A(x_0) + B \} \cup \{\infty\}$$

where $\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$.

If $\mathbb{K}$ is an extension field of $\mathbb{F}_q$, we define $E(\mathbb{K})$ as the set

$$E(\mathbb{K}) = \{ (x_0, y_0) \in \mathbb{K} \mid (y_0)^2 = (x_0)^3 + A(x_0) + B \} \cup \{\infty\}.$$

It is possible to define a sum in E, with ∞ as the identity element. In particular, given $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ in E, with $P_1, P_2 \neq \infty$, we define $P_3 = (x_3, y_3) = P_1 + P_2$ as

$$P_3 = \begin{cases} \left(\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2, \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1 \right) & \text{if } x_1 \neq x_2 \\ \infty & \text{if } x_1 = x_2 \text{ and } y_1 \neq y_2 \ (\Leftrightarrow y_1 = -y_2) \\ \left(\left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1, \left(\frac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3) - y_1 \right) & \text{if } P_1 = P_2 \text{ and } y_1 \neq 0 \\ \infty & \text{if } P_1 = P_2 \text{ and } y_1 = 0 \end{cases}$$

This sum makes E an **abelian** group. We observe that $E(\mathbb{K})$ is a subgroup of E, for every extension field $\mathbb{K}$ of $\mathbb{F}_q$.
In particular, $E(\mathbb{F}_q)$ is a subgroup of E, and it is called "rational subgroup of E" or "group of rational points of E".

In the following, we introduce some fundamental concepts concerning elliptic curves.

■ 1.2 - Torsion subgroups

Let z be a natural number. The set of z-torsion points of E is defined as:

$$E[z] = \{ P \in E \mid zP = \underbrace{P + P + \dots + P}_{z \text{ times}} = \infty \}$$

and it is a subgroup of E.

If $\gcd(z, p = \text{char}(\mathbb{F}_q)) = 1$, then it is possible to prove that $E[z] \overset{\text{group isomorphism}}{\simeq} \mathbb{Z}/z\mathbb{Z} \times \mathbb{Z}/z\mathbb{Z}$. As a consequence, $E[z]$ contains z^2 elements.
($\times$: direct product)

The group $\mathbb{Z}/z\mathbb{Z} \times \mathbb{Z}/z\mathbb{Z}$ is not cyclic, but it is generated by two elements.

What does it happen when $z = p$? There are two possibilities:

$$E[p] = \begin{cases} \{\infty\} \\ \mathbb{Z}/p\mathbb{Z}. \end{cases}$$

In the first case, the elliptic curve E is said ordinary, in the second case E is said supersingular. In the following we will deal only with supersingular elliptic curves.

★ Example 1

$\left[p=19,\ m=2,\ q=p^m=361,\ E: y^2=x^3+x \ \text{(supersingular)}\right]$

$E[2]$ is composed by all the points P in E such that $P+P=\infty$. Obviously $\infty \in E[2]$. From the addition defined in E (last item) it follows that $P=(x,y)\neq\infty$ has order 2 if and only if $y=0$. So to determine $E[2]$ we have to solve the equation

$$x^3+x=0 \iff x(x^2+1)=0$$

which has three solutions: $x=0$, $x=\pm i$ (note that $\left(\frac{-1}{p}\right)=-1$, so -1 is not a square in $\mathbb{F}_p$, so i belongs to $\mathbb{F}_{p^2}$). We can deduce:

$$E[2]=\{\infty,\ P_1=(0,0),\ P_2=(i,0),\ P_3=(-i,0)\}.$$

■ 1.3 - Isogenies and isomorphisms

Given two elliptic curves E_1, E_2 defined over $\mathbb{F}_q$, an isogeny $\phi: E_1 \to E_2$ is a surjective map such that:

i) $\phi(\infty)=\infty$

ii) $\phi(x,y)=\left(f_1(x)/f_2(x),\ y\,\frac{g_1(x)}{g_2(x)}\right)$ where $f_1, f_2, g_1, g_2 \in \overline{\mathbb{F}_q}[x]$.

For $P \in E_1$, we have:

$$\phi(P)=\infty \iff f_2(P)=0.$$

IF f_1, f_2, g_1, g_2 belongs to $\mathbb{K}[x]$, where $\mathbb{K}$ is an extension field of $\mathbb{F}_q$, then we say that the isogeny ϕ is defined over $\mathbb{K}$.

We define the degree of ϕ as:

$$\deg(\phi) \overset{\text{def}}{=} \max\{\deg(f_1), \deg(f_2)\}.$$

We are going to consider only separable isogenies, for which $\deg(\phi)=|\ker(\phi)|$.

It is possible to prove that

$$\phi(P+Q)=\phi(P)+\phi(Q) \qquad \forall P, Q \in E_1.$$

Hence, if the isogeny is defined over $\mathbb{F}_q$ (or any extension field $\mathbb{K}$), then the restriction $\phi: E_1(\mathbb{F}_q) \to E_2(\mathbb{F}_q)$ is a group homomorphism.

★ Example 2

$\left[p=19,\ m=2,\ q=p^m=361,\ E: y^2=x^3+x \ \text{(supersingular)}\right]$

The map:

$$\begin{aligned} \psi: E &\longrightarrow E \\ \infty &\longmapsto \infty \\ P=(x,y) &\longmapsto 2P=\left(\frac{(x^2-1)^2}{4(x^3+x)},\ y\,\frac{x^6+16x^4-5x^2-1}{8(x^3+x)^2}\right) \end{aligned}$$

is an isogeny defined over $\mathbb{F}_q$. We note that $\ker(\phi)=E[2]$, as we expected. Since domain and co-domain of ψ coincide, we say that ψ is an endomorphism of E.

One of the most relevant results concerning isogenies between elliptic curves defined over finite fields is the following.

■ Tate's theorem

Given two elliptic curves defined over $\mathbb{F}_q$, E_1 and E_2, there exists an isogeny $\phi: E_1 \to E_2$ defined over $\mathbb{F}_q$ if and only if

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

A nice property of isogenies is that they can be "factorised":

- let E_1, E_2, E_3 be elliptic curves defined over $\mathbb{F}_q$ and $\phi: E_1 \to E_2$, $\phi': E_2 \to E_3$ be two isogenies. Then $\phi' \circ \phi: E_1 \to E_3$ is an isogeny and $\deg(\phi' \circ \phi)=\deg(\phi')\deg(\phi)$.
- let E_1, E_2 be two elliptic curves defined over $\mathbb{F}_q$ and let $\phi: E_1 \to E_2$ be an isogeny defined over $\mathbb{F}_q$ with degree n. Then ϕ can be factored as a composition of isogenies defined over $\mathbb{F}_q$ of prime degrees.

The efficiency of isogeny-based cryptographic schemes relies on the above factorisation properties.

An isogeny

$$\phi: E_1 \longrightarrow E_2$$

is an isomorphism if its degree is 1 (so $\ker(\phi)=\{\infty\}$).

To check if two elliptic curves E_1, E_2 defined over $\mathbb{F}_q$ are isomorphic (over $\overline{\mathbb{F}_q}$) we can rely on j-invariants.

The j-invariant of an elliptic curve E defined over $\mathbb{F}_q$

$$E: y^2 = x^3 + Ax + B$$

is defined as

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2}.$$

An important result states that E_1, E_2 are isomorphic (over $\overline{\mathbb{F}_q}$) if and only if they have the same j-invariant.

Our path towards the introduction of SIDH is almost complete. We need to state only other two results:

■ Theorem 1

Let E be an elliptic curve defined over $\mathbb{F}_q$ and let H be a finite subgroup of $E(\mathbb{K})$, where $\mathbb{K}$ is an extension field of $\mathbb{F}_q$.
There are a unique elliptic curve E' and a separable isogeny

$$\phi: E \to E'$$

such that

1) $\ker(\phi) = H$;
2) ϕ and E' are defined over $\mathbb{K}$.

The isogeny ϕ is unique in the following sense: if E'' is an elliptic curve defined over $\mathbb{K}$ and $\Psi: E \to E''$ is an isogeny defined over $\mathbb{K}$ such that $\ker(\Psi) = H$, then there exists an isomorphism $f: E' \to E''$, defined over $\mathbb{K}$ and such that $f \circ \phi = \Psi$.

⚠ The elliptic curve E' is often denoted by E/H.

Vélu's formulas give a procedure to compute **E/H and ϕ**, which has a complexity linear in $|H|$ and requires field operations in $\mathbb{K}$.

If $\mathbb{K}$ is a finite field, then using standard arithmetic the procedure costs $O(m(\log(\#\mathbb{K}))^2)$ bit operations, where $m = |H|$.

Given a natural number ℓ such that $\gcd(\ell, p = \mathrm{char}(\mathbb{F}_q)) = 1$, we can deduce that:

- the isogenies of degree ℓ from E are the isogenies having as kernel subgroups of E of order ℓ (hence subgroups of $E[\ell]$).
- if ℓ is a prime, in $E[\ell] = \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ there are exactly $\ell+1$ subgroups of order ℓ, so there are exactly $\ell+1$ isogenies of degree ℓ from E.

★ Example 3

[$p = 19$, $m = 2$, $q = 19^2 = 361$, $E: y^2 = x^3 + x$ (supersingular), $E[2] = \{\infty, P_1 = (0,0), P_2 = (i,0), P_3 = (-i,0)\}$.]

The subgroups of order 2 of E are

- $H_1 = \{\infty, P_1 = (0,0)\}$
- $H_2 = \{\infty, P_2 = (i,0)\}$
- $H_3 = \{\infty, P_3 = (-i,0)\}$

and applying Velu's formula we obtain

- $E_1: y^2 = x^3 + 15x$ (defined over $\mathbb{F}_{19}$, supersingular)
- $\phi_1: E \longrightarrow E_1$
  $(x,y) \longmapsto \left(\frac{x^2+1}{x}, y\frac{x^2+18}{x^2}\right)$
- $E_2: y^2 = x^3 + 11x + 5i$ (defined over $\mathbb{F}_{19^2} = \mathbb{F}_{19}(i)$, supersingular)
- $\phi_2: E \longrightarrow E_2$
  $(x,y) \longmapsto \left(\frac{x^2+ix+17}{x+i}, y\frac{x^2+2ix+1}{x^2+2ix+18}\right)$
- $E_3: y^2 = x^3 + 11x + 14i$ (defined over $\mathbb{F}_{19^2} = \mathbb{F}_{19}(i)$, supersingular)
- $\phi_3: E \longrightarrow E_3$
  $(x,y) \longmapsto \left(\frac{x^2+18ix+17}{x-i}, y\frac{x^2+17ix+1}{x^2+17ix+18}\right)$

■ 2.1 - The Supersingular Isogeny Diffie-Hellman (SIDH) Scheme

Two parties, Alice and Bob, want to exchange a shared secret using a public channel.

The shared secret can be exploited by Alice and Bob to establish a simmetric key.

The protocol Alice and Bob are going to use to produce the shared secret is called Supersingular Isogeny Diffie-Hellman (SIDH in short). Such a protocol has some Fixed parameters, that are public. Every pair of users running the protocol has to use these parameters.

■ 2.2 - SIDH's public parameters

The public parameters for the SIDH are:

- a prime p of the form
$$p = 2^{e_2} 3^{e_3} f \pm 1$$
where $e_2, e_3, f \in \mathbb{N}$, f is a cofactor such that p is a prime, and $2^{e_2} \simeq 3^{e_3}$;
- the Finite Field $\mathbb{F}_{p^2}$;
- a supersingular elliptic curve
$$E_0 : y^2 = x^3 + A_0 x + B_0$$
defined over $\mathbb{F}_{p^2}$ and such that
$$|E_0(\mathbb{F}_{p^2})| = (2^{e_2} 3^{e_3} f)^2;$$
- a set of generators $\{P_A, Q_A\}$ of the torsion subgroup $E_0[2^{e_2}]$;
- a set of generators $\{P_B, Q_B\}$ of the torsion subgroup $E_0[3^{e_3}]$.

▲ Remark 1

It is possible to prove that a supersingular elliptic curve E_0 defined over $\mathbb{F}_{p^2}$ and with the desired number of rational points always exists.

▲ Remark 2

From the condition $|E_0(\mathbb{F}_{p^2})| = (2^{e_2} 3^{e_3} f)^2$ it follows that $E_0[2^{e_2}], E_0[3^{e_3}] \subseteq E_0(\mathbb{F}_{p^2})$, so that P_A, Q_A, P_B, Q_B are rational points. We note that in practice p is a "big" prime, hence $\gcd(2^{e_2}, p) = \gcd(3^{e_3}, p) = 1$ and so
$$E_0[2^{e_2}] = \mathbb{Z}/2^{e_2}\mathbb{Z} \times \mathbb{Z}/2^{e_2}\mathbb{Z}, \quad E_0[3^{e_3}] = \mathbb{Z}/3^{e_3}\mathbb{Z} \times \mathbb{Z}/3^{e_3}\mathbb{Z}.$$

★ Example 4

We Fix the prime $p = (2^3)(3^2) + 1 = 73$, with $e_2 = 3$, $e_3 = 2$, $f = 1$, $2^{e_2} = 8 \simeq 9 = 3^{e_3}$.
As base Field we consider
$$\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-5}) = \{u + v\sqrt{-5} \mid u, v \in \mathbb{F}_p\}$$
which has cardinality equal to 5329.
We set
$$E_0 : y^2 = x^3 + (51 + 40\sqrt{-5})x + (70 + 28\sqrt{-5})$$
which is a supersingular elliptic curve such that:
$$|E_0(\mathbb{F}_{p^2})| = (2^{e_2} 3^{e_3})^2 = 5184.$$
One can check that
$$\{P_A = (33 + 35\sqrt{-5}, 63 + 67\sqrt{-5}), Q_A = (28 + 67\sqrt{-5}, 17 + 58\sqrt{-5})\}, \quad \{P_B = (48 + 71\sqrt{-5}, 70 + 43\sqrt{-5}), Q_B = (18 + 44\sqrt{-5}, 22 + 47\sqrt{-5})\}$$
generate $E_0[2^{e_2}]$ and $E_0[3^{e_3}]$ respectively.

■ 2.3 - Public and secret keys

At the beginning of their interaction, Alice and Bob have to create their pairs of public-private keys.
Alice chooses a subgroup H_A of $E_0[2^{e_2}]$, having order 2^{e_2} (note that $E_0[2^{e_2}]$ also contains points of order $2, 2^2, \dots, 2^{e_2 - 1}$). To do this, she randomly selects
$$m_A, n_A \in \mathbb{Z}/2^{e_2}\mathbb{Z}$$
not both divisible by 2. This last condition assures that the point $R_A = m_A P_A + n_A Q_A$ has order 2^{e_2}.

Then Alice defines H_A as the cyclic subgroup generated by R_A, i.e. $H_A = \langle R_A \rangle$.

Using H_A, Alice computes the isogeny

$$\phi_A : E_0 \to E_0 / H_A$$

having H_A as kernel, and the images $\phi_A(P_B), \phi_A(Q_B)$. We note that:

- ϕ_A and E_0 / H_A are computed using Velu's Formulas (composing isogenies of degree 2);
- E_0 / H_A is an elliptic curve defined over $\mathbb{F}_{p^2}$, since $H_A \subseteq E_0(\mathbb{F}_{p^2})$. Thanks to Tate's theorem, we have $|E_0 / H_A(\mathbb{F}_{p^2})| = |E_0(\mathbb{F}_{p^2})| = (2^{e_2} 3^{e_3} f)^2$. Furthermore it is possible to prove that E_0 / H_A is supersingular.

Alice's public key is

$$(E_0 / H_A, \phi_A(P_B), \phi_A(Q_B))$$

while her private key is

$$(m_A, n_A).$$

Knowing ϕ_A is equivalent to knowing H_A, which in turn is equivalent to knowing a generator of H_A.

Analogously, Bob chooses a subgroup H_B of $E_0[3^{e_3}]$, having order 3^{e_3} ($E_0[3^{e_3}]$ also contains points of order $3, 3^2, \dots, 3^{e_3 - 1}$). To do this, he randomly selects

$$m_B, n_B \in \mathbb{Z} / 3^{e_3} \mathbb{Z}$$

not both divisible by 3. This assures that the point $R_B = m_B P_B + n_B Q_B$ has order 3^{e_3}.
He defines H_B as the subgroup generated by R_B, i.e. $H_B = \langle R_B \rangle$.

Using H_B, Bob computes the isogeny

$$\phi_B : E_0 \longrightarrow E_0 / H_B$$

having H_B as kernel, and the images $\phi_B(P_A), \phi_B(Q_A)$. Bob's keys are:

$$\underbrace{(E_0 / H_B, \phi_B(P_A), \phi_B(Q_A))}_{\text{public key}} \quad , \quad \underbrace{(m_B, n_B)}_{\text{private key}}.$$

★ Example 5

$$\left[p = (2^3)(3^2) + 1 = 73 ; \mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-5}) = \{u + v\sqrt{-5} \mid u, v \in \mathbb{F}_p\} ; E_0 : y^2 = x^3 + (51 + 40\sqrt{-5})x + (70 + 28\sqrt{-5}) ; \right.$$
$$\left. \{P_A = (33 + 35\sqrt{-5}, 63 + 67\sqrt{-5}), Q_A = (28 + 67\sqrt{-5}, 17 + 58\sqrt{-5})\} = E_0[2^{e_2}] ; \{P_B = (48 + 71\sqrt{-5}, 70 + 43\sqrt{-5}), Q_B = (18 + 44\sqrt{-5}, 22 + 47\sqrt{-5})\} = E_0[3^{e_3}] \right]$$

Assuming that Alice chooses

$$\begin{cases} m_A = 3 \\ n_A = 4 \end{cases}$$

then $R_A = m_A P_A + n_A Q_A = (14\sqrt{-5}, 60 + 5\sqrt{-5})$ and using Velu's Formulas she obtains

$$\begin{cases} E_0 / \langle R_A \rangle : y^2 = x^3 + (4 + 48\sqrt{-5})x + (14 + 63\sqrt{-5}) \\ \phi_A(P_B) = (35 + 42\sqrt{-5}, 47 + 21\sqrt{-5}) \\ \phi_A(Q_B) = (14 + 6\sqrt{-5}, 71 + 56\sqrt{-5}). \end{cases}$$

IF Bob chooses

$$\begin{cases} m_B = 2 \\ n_B = 6 \end{cases}$$

then $R_B = m_B P_B + n_B Q_B = (9 + 2\sqrt{-5}, 54 + 33\sqrt{-5})$ and

$$\begin{cases} E_0 / \langle R_B \rangle : y^2 = x^3 + (60 + 5\sqrt{-5})x + (41 + 17\sqrt{-5}) \\ \phi_B(P_A) = (50 + 19\sqrt{-5}, 36 + 34\sqrt{-5}) \\ \phi_B(Q_A) = (12 + 56\sqrt{-5}, 23 + 46\sqrt{-5}). \end{cases}$$

2.4 - The protocol

ALICE

Public key : $E_0/\mathcal{H}_A,\ \phi_A(P_B),\ \phi_A(Q_B)$
Private key : (m_A, n_A)

BOB

Public key : $E_0/\mathcal{H}_B,\ \phi_B(P_A),\ \phi_B(Q_A)$
Private key : (m_B, n_B)

$E_0/\mathcal{H}_A,\ \phi_A(P_B),\ \phi_A(Q_B)$ —— message ——→

←—— message ——— $E_0/\mathcal{H}_B,\ \phi_B(P_A),\ \phi_B(Q_A)$

- Computes the isogeny

$$\phi_{BA} : E_0/\mathcal{H}_B \longrightarrow (E_0/\mathcal{H}_B)/\langle m_A\phi_B(P_A) + m_A\phi_B(Q_A)\rangle$$
$$\| \text{ notation}$$
$$E_{BA}$$

- Computes the isogeny

$$\phi_{AB} : E_0/\mathcal{H}_A \longrightarrow (E_0/\mathcal{H}_A)/\langle m_B\phi_A(P_B) + m_B\phi_A(Q_B)\rangle$$
$$\| \text{ notation}$$
$$E_{AB}$$

SHARED SECRET
$j(E_{BA}) = j(E_{AB})$

Straightforward computations show that the isogenies

$$\phi_{BA}\circ\phi_B : E_0 \longrightarrow E_{BA}$$

$$\phi_{AB}\circ\phi_A : E_0 \longrightarrow E_{AB}$$

have the same kernel $\langle R_A, R_B\rangle$. Hence, For Theorem 1, E_{BA} and E_{AB} must be isomorphic, i.e. they have the same j-invariant.

★ Example 6

$p = (2^3)(3^2)+1 = 73$; $\mathbb{F}_{p^2} = \mathbb{F}_p(\sqrt{-5}) = \{u+v\sqrt{-5} \mid u,v \in \mathbb{F}_p\}$; $E_0 : y^2 = x^3 + (51+40\sqrt{-5})x + (70+28\sqrt{-5})$;

$\{P_A = (33+35\sqrt{-5}, 63+67\sqrt{-5}),\ Q_A = (28+67\sqrt{-5}, 17+58\sqrt{-5})\} = E_0[2^{e_2}]$; $\{P_B = (48+71\sqrt{-5}, 70+43\sqrt{-5}),\ Q_B = (18+44\sqrt{-5}, 22+47\sqrt{-5})\} = E_0[3^{e_3}]$

$m_A = 3,\ n_A = 4,\ R_A = m_A P_A + n_A Q_A = (14\sqrt{-5}, 60+5\sqrt{-5})$, $E_0/\langle R_A\rangle : y^2 = x^3 + (4+48\sqrt{-5})x + (14+63\sqrt{-5})$,

$\phi_A(P_B) = (35+42\sqrt{-5}, 47+21\sqrt{-5})$, $\phi_A(Q_B) = (14+6\sqrt{-5}, 71+56\sqrt{-5})$

$m_B = 2,\ n_B = 6,\ R_B = m_B P_B + n_B Q_B = (9+2\sqrt{-5}, 54+33\sqrt{-5})$, $E_0/\langle R_B\rangle : y^2 = x^3 + (60+5\sqrt{-5})x + (41+17\sqrt{-5})$

$\phi_B(P_A) = (50+19\sqrt{-5}, 36+34\sqrt{-5})$, $\phi_B(Q_A) = (12+56\sqrt{-5}, 23+46\sqrt{-5})$

In E_B, we have that

$$m_A\phi_B(P_A) + n_A\phi_B(Q_A) = (49+30\sqrt{-5}, 70+60\sqrt{-5})$$

and the curve E_{BA} is

$$E_{BA} = E_B/\langle m_A\phi_B(P_A) + n_A\phi_B(Q_A)\rangle : y^2 = x^3 + (60+30\sqrt{-5})x + (17+61\sqrt{-5})$$

In E_A, we have

$$m_B\phi_A(P_B) + n_B\phi_A(Q_B) = (26+43\sqrt{-5}, 18+43\sqrt{-5})$$

and the curve E_{AB} is

$$E_{AB} = E_A/\langle m_B\phi_A(P_B) + n_B\phi_A(Q_B)\rangle : y^2 = x^3 + (60+38\sqrt{-5})x + (17+61\sqrt{-5})$$

It is easy to see that

$$j(E_{BA}) = j(E_{AB}) = 9$$

and then $j=9$ is the shared secret between Alice and Bob.

2.5 - Security of the protocol

The Supersingular Isogeny Diffie-Hellman is secure under the assumption that the following problem is hard:

> Given a tuple sampled with probability 1/2 from one of the following two distributions:
>
> i) $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E_{AB})$
>
> ii) $(E_A, E_B, \phi_A(P_B), \phi_A(Q_B), \phi_B(P_A), \phi_B(Q_A), E_C)$
>
> determine from which distribution the tuple is sampled.

We note that:

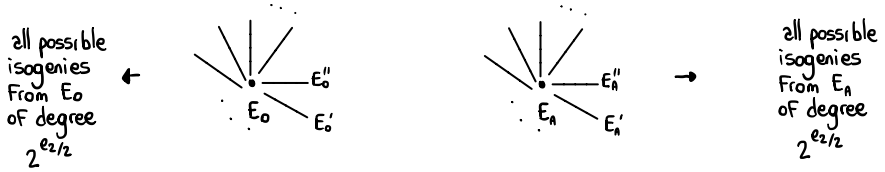
- $\phi_A : E_0 \to E_A$ is an isogeny whose kernel is equal to $\langle m_A P_A + m_A Q_A \rangle$;
- $\phi_B : E_0 \to E_B$ is an isogeny whose kernel is equal to $\langle m_B P_B + m_B Q_B \rangle$;
- m_A, m_A are chosen at random from $\mathbb{Z}/2^{e_2}\mathbb{Z}$ (not both divisible by 2);
- m_B, m_B are chosen at random from $\mathbb{Z}/3^{e_3}\mathbb{Z}$ (not both divisible by 3);
- $E_{AB} \overset{\text{isomorphic}}{\cong} E_0/\langle m_A P_A + m_A Q_A, m_B P_B + m_B Q_B \rangle$;
- $E_C \cong E_0/\langle m'_A P_A + m'_A Q_A, m'_B P_B + m'_B Q_B \rangle$ where m'_A, m'_A (respectively m'_B, m'_B) are chosen <u>at random</u> from $\mathbb{Z}/2^{e_2}\mathbb{Z}$ (respectively $\mathbb{Z}/3^{e_3}\mathbb{Z}$) and not both divisible by 2 (respectively 3).

It is conjectured that the above problem is computationally infeasible: for any polynomial time adversary, their advantage is a negligible function of the security parameter $\log p$. In particular, it is conjectured that the above problem is equivalent to the following (it could be stated also with 3 instead of 2, and e_3 instead of e_2):

> Let $\phi_A : E_0 \to E_A$ be an isogeny whose kernel is $\langle m_A P_A + m_A Q_A \rangle$, where m_A, m_A are chosen at random from $\mathbb{Z}/2^{e_2}\mathbb{Z}$ and not both divisible by 2. Given E_A and the values $\phi_A(P_B), \phi_A(Q_B)$, find a generator for the kernel $\langle m_A P_A + m_A Q_A \rangle$.

The best known classical algorithm for finding isogenies between supersingular curves has complexity $O(\sqrt{p}\log^2 p)$.
However, the above problem is not completely general since:
i) the degree of the isogeny is known in advance;
ii) such a degree is smooth.

In order to find an isogeny of degree 2^{e_2} between E_0 and E_A, it is possible to consider



and look for collisions. The classical complexity of this attack is $O(2^{e_2/2}) = O(\sqrt[4]{p})$ ($2^{e_2} \simeq \sqrt{p}$)

With quantum computers it is possible to improve the above algorithm achieving a complexity $O(\sqrt[6]{p})$.

Consequently, to obtain a classical security level of 128, 192, 256 bits, the prime p is chosen such that $\log_2 p$ is about 500, 750, 960 respectively. The corresponding quantum securities are about 80, 128, 160 bits.

The current optimized version of the SIDH protocol allows to exchange a secret in about 10 milliseconds for a p such that $\log_2 p \simeq 500$.

We conclude this short notes highlighting that SIDH is the base for one of the submissions, SIKE, to the NIST effort to standardise post-quantum cryptographic schemes. Site has been admitted in round III as an alternative candidate.