Introduction to Supersingular Isogenies Diffie-Hellman

Pedro M. Sosa

February 2, 2017

Abstract

The aim of this paper we will explore the construction and execution of the Supersingular Isogenies Diffie-Hellman key exchange algorithm (SIDH-KEX).

1 Background

In the last couple of years, there has been an important push towards the study and implementation of Post-Quantum cryptographic protocols. [**TODO**]

2 Motivation

3 Security and Efficiency

4 Preliminaries

In this section we will discuss some of the mathematical constructs and finer details necesesary to further understand the SIDH-KEX

Elliptic Curves Similar to other elliptic curve cryptographic schemes, we will assume our chosen elliptic curve E over F_{p^2} to be non-singular and of the Weierstrass form: $y^2 = x^3 + ax + b$.

Isogeny An isogeny is a surjective and homomorphic structure preserving function that maps two groups together. In the case of elliptic curves case, a isogeny ϕ will map points on the domain curve E to points on a co-domain curve E'.

j-Invariant The j-invariant is a descriptor that can be computed for any particular curve using said curves parameters. Most importantly, isomorphic curves will always share the same j-invariant value. The exact equation for the j-invariant will vary depending on the underlying form of the elliptic curve. In the case of elliptic curves in the Weierstrass form, the j-invariant is calculated as follows:

$$j(E) = 1728 \cdot \frac{4a^3}{4a^3+27b^2}$$

Supersingular curves While it might seem a bit confusing, supersingular curves are non-singular elliptic curves as one would expect to find in other elliptic curve scheme. The term *"supersingular"* actually refers to the fact that they have "singular" values of the j-invariant and it's Hasse invariant is 0. [**TODO: Refer to section blah for some proposed curves**]

5 Supersingular Isogeny Diffie-Hellman

5.1 Setup

Initially there will be 4 global public parameters:
- A prime p
- A supersingular elliptic curve E over F_{p^2}
- Four fixed points P_a, Q_a, P_b, Q_b on E

5.2 Key Exchange

- **Alice**
1. Randomly generate m_a, n_a
2. $R_a = m_a \cdot P_a + n_a \cdot Q_a$

3. Create an isogeny mapping using R_a such that $\phi_a : E \to E_a$
4. $P'_b, Q'_b = \phi_a(P_b), \phi_a(Q_b)$
5. Send E_a, P'_b, Q'_b
   - **Bob [TODO]**

5.3 Parameter Selection

The latest work by Costello et al. [**?**], defined the curve $E = y^2 + x^3 + x$ and the prime $p = 2^3 72 \cdot 3^2 39 - 1$. Furthermore they established the four points on E to be: - $P_a = [3^2 39](11, \sqrt{11^3 + 11})$
- $Q_a = \tau(P_a)$
- $P_b = [2^3 72](6, \sqrt{6^3 + 6})$
- $Q_b = \tau(P_b)$
where τ is a distortion map from $E(F_{p^2}) \to E(F_{p^2}) : (x, y) \to (-x, iy)$. This was done purposely so as to avoid having to store both Q_a and Q_b in memory and instead derive them from their respective P_i points.

6 Further Work