Supersingular Isogeny Based Quantum-Resistant Key-Exchange Protocol Implemented in C++

Juntian Zheng Zihao Zhen Wuwei Yuan

1 Introduction

The Diffie-Hellman scheme is a fundamental protocol for public-key exchange, and many protocols are developed based on DH, such as ECDH (*Elliptic-curve Diffie-Hellman*). However, it is well-known that Shor's algorithm would solve the discrete-log algorithms and break the protocol on a quantum computer. In recent years, D. Jao and L. De Feo [JD11] introduced the protocol of SIDH (*Supersingular Isogeny Diffie-Hellman*), which overcomes the previous protocols in a variety of aspects. The SIDH protocol involves new computational assumptions which are not only believed to be more secure but also requires fully exponential time to attack even on quantum computers at current. Besides, the SIDH protocol is also performs faster and easier to implement.

In this report, we delve into the mathematics behind the elliptic curves in Section 2. We then explain the implementation and the security proof of the protocol in Section 3. Finally, we implement the SIDH protocol in C++ and successfully exchange the key between Alice and Bob in Section 4. For the implementation details, please refer to the repository `https://github.com/Alif-01/SIQRS`, which includes the C++ source code and also the LaTeXsource code of this report.

2 Preliminary

In this section we will briefly introduce some mathematical concepts, which serve as the foundation of isogeny-based cryptography. The proofs are omitted for simplicity. For a detailed description, please check [Sil09], [DF17] and [JD11].

Definition 1 (Elliptic Curves)**.** Let k be a field with characteristic different from 2 or 3, and $\overline{k}$ be its algebraic closure. An *elliptic curve* is the set of points in $\mathbb{P}^2(\overline{k})$ satisfying the equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3,$$

where $a, b \in k, 4a^3 + 27b^2 \neq 0$. Here $\mathbb{P}^k(\overline{k})$ is the 2-dimensional projective space on $\overline{k}$, i.e., the set

$$\{(X : Y : Z) \mid X, Y, Z \in \overline{k}, (X, Y, Z) \neq (0, 0, 0)\}$$

modulo the equivalence relation

$$(X : Y : Z) \sim (X' : Y' : Z') \Leftrightarrow \exists \lambda \in \overline{k}, X = \lambda X', Y = \lambda Y', Z = \lambda Z'.$$

A more convenient representation of elliptic curves is the affine form

$$y^2 = x^3 + ax + b,$$

which is just the dehomogenization of the definition above. Under this representation, an elliptic curve consists of the solutions of such an equation, together with a point at infinity $\mathcal{O} = (0 : 1 : 0)$.

For any elliptic curve E defined as above, the Bezout's theorem tells us that any line in $\mathbb{P}^2(\overline{k})$ will intersect E in exactly three points (including multiplicity). Therefore, for any two points $P, Q \in E$, we can find another point $R \in E$ that P, Q, R are colinear, and then define the addition rule on the elliptic curve by

$$P + Q + R = \mathcal{O},$$

It can be verified that this gives a abelian group structure over the curve.

Definition 2 (Rational Points)**.** The *rational points* of an elliptive curve E is the set

$$E(k) = \{(X : Y : Z) \in E \mid X, Y, Z \in k\}$$

of points that have coordinates defined in k. The rational points form a subgroup of the whole curve.

Definition 3 (Isomorphism & j-Invariant)**.** We can define the *algebraic maps* between elliptic curves as the homogeneous rational functions on their coordinates. An *isomorphism* between two curves is an invertible algebraic map. Two curves are isomorphic if and only if they have the same *j-invariant*

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

Definition 4 (Isogeny)**.** An *isogeny* is a surjective algebraic map between two curves that also keeps their group structures, i.e., it is a group homomorphism. For simplicity we only consider the separable mappings here. Furthermore, we have the following equivalent conditions for isogenies:

1. Algebraic map $\varphi : E \to E'$ is a surjective group homomorphism.
2. Algebraic map $\varphi : E \to E'$ is a group homomorphism with finite kernel.
3. Algebraic map $\varphi : E \to E'$ is non-constant and sends the point at infinity $\mathcal{O}$ to $\mathcal{O}'$.

For any isogeny $\varphi : E \to E'$, we know that $\ker \varphi$ is always finite, and we can define its degree $\deg \varphi$ as $|\ker \varphi|$. For any isogeny $\varphi : E \to E'$ with $\deg \varphi = l$, there exists a *dual isogeny* $\psi : E' \to E$ that $\deg \psi = l$ and

$$\psi \circ \varphi = [l]_E, \varphi \circ \psi = [l]_{E'},$$

in which $[l]_E$ means scalar multiplication by l. Furthermore, the composition of two isogenies $\varphi : E \to E'$ and $\psi : E' \to E''$ is still an isogeny, with $\deg(\psi \circ \varphi) = \deg \psi \cdot \deg \varphi$. This shows that the isogenies of some certain degree actually give an equivalent relationship between elliptic curves over a fixed field.

Proposition 5 (Isogeny from Kernel)**.** Given an elliptic curve E and a finite subgroup Φ of E, there is a unique pair (E', φ) that $\varphi : E \to E'$ is an isogeny with kernel Φ. The uniqueness here is up to isomorphisms on E'.

Definition 6 (Supersingular & Ordinary Curves)**.** We can separate all curves defined over some finite field $\mathbb{F}_q$ into two classes by the structures of their endomorphism ring $\mathrm{End}(E)$, which is the set of all isogenies from E to itself. For any curve E, its endomorphism ring $\mathrm{End}(E)$ can be in one of the following forms:

1. An order in an imaginary quadratic field. These curves are called ordinary curves.
2. An order in a quaternion algebra. These curves are called supersingular curves.

We will mainly focus on the supersingular curves in this project. The supersingular curves have a bunch of nice properties, especially the simple structure of abelian group and isogeny graph.

Proposition 7 (Group Structure of Supersingular Curves)**.** All supersingular curves are defined over $\mathbb{F}_{p^2}$ for some prime p. Given prime p and $q = p^2$, most of the supersingular curves defined over $\mathbb{F}_q$ (except for some special cases with $j(E) = 0$ or $j(E) = 1728$) have rational points of group structure $E(\mathbb{F}_q) \cong (\mathbb{Z}/(p \pm 1)\mathbb{Z})^2$.

Definition 8 (Isogeny Graph over Supersingular Curves)**.** All supersingular curves defined over $\mathbb{F}_q$ are isogenic to each other. An *isogeny graph* is an undirected graph that depicts the isogeny relations between different curves over a finite field $\mathbb{F}_q$. Its vertices consist of the isomorphic classes (or j-invariants) of curves, and each edge represents an isogeny (up to automorphisms at the destination curve) with a certain degree l between two curves. For supersingular curves, the graph contains $p/12 + O(1)$ vertices, and it's a Ramanujan graph with degree $l + 1$.

3 SIDH

In this section we will introduce the protocol of SIDH (*Supersingular Isogeny Diffie-Hellman*) key-exchange. Its basic idea is to let Alice and Bob individually walk on the isogeny graph, and finally converge to the same vertex. After that, the j-invariant of the converged vertex is used as their shared secret-key. For a detailed description, please check [JD11].

Protocol 9 (SIDH)**.** The protocol of SIDH is stated formally as follows:

- **Public parameters:** An prime number $p = 2^{e_2}3^{e_3} - 1$ and a supersingular curve E_0 defined over $\mathbb{F}_q = \mathbb{F}_{p^2}$ is fixed. The group structure of that curve is $E_0[\mathbb{F}_q] \cong (\mathbb{Z}/2^{e_2}\mathbb{Z})^2 \times (\mathbb{Z}/3^{e_3}\mathbb{Z})^2$. Find bases $\{P_A, Q_A\}, \{P_B, Q_B\}$ that generates the subgroups of order 2^{e_2} and 3^{e_3} respectively.
- **Secret parameters:** Both Alice and Bob generate their secret isogeny $\varphi_A : E_0 \to E_A$ and $\varphi_B : E_0 \to E_B$, composed of 2-isogenies and 3-isogenies respectively. The isogenies is represented by their kernels $\Phi_A = \langle [m_A]P_A + [n_A]Q_A \rangle, \Phi_B = \langle [m_B]P_B + [n_B]Q_B \rangle$.
- **Exchanging:** Alice and Bob exchange the equations of E_A and E_B to each other. Besides, to enable each other compute the successive isogenies, they also reveal some auxiliary points: Alice reveals $\varphi_A(P_B)$ and $\varphi_A(Q_B)$, while Bob reveals $\varphi_B(P_A)$ and $\varphi_B(Q_A)$. From the auxiliary points, they can reconstruct the successive isogenies

$$\varphi'_B : E_A \to E_A/\langle [m_B]\varphi_A(P_B) + [n_B]\varphi_A(Q_B) \rangle,$$
$$\varphi'_A : E_B \to E_B/\langle [m_A]\varphi_B(P_A) + [n_A]\varphi_B(Q_A) \rangle.$$

  Then both of φ'_A and φ'_B point to the same destination curve $E_{AB} = E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle$. The j-invariant of E_{AB} is then used as the exchanged secret-key.

Figure 1 shows the commutative diagram of the exchanging process.

$$\begin{array}{ccc} E_0 & \longrightarrow & E_A = E_0/\Phi_A \\ \downarrow & & \downarrow \\ E_B = E_0/\Phi_B & \longrightarrow & E_{AB} = E_A/\Phi'_B = E_B/\Phi'_A \end{array}$$

Figure 1: Isogeny Diagram

Now we briefly give a security reduction relating the protocol to the hardness of appropriate isogeny computation problem. The whole proof is given in [JD11].

Definition 10. Supersingular Decision Diffie-Hellman (SSDDH) Problem. Given a tuple sampled with probability 1/2 from one of the following two distributions:

- $(E_A, E_B, \varphi_A(P_B), \varphi_A(Q_B), \varphi_B(P_A), \varphi_B(Q_A), E_{AB})$, where $E_A, E_B, \varphi_A(P_B), \varphi_A(Q_B), \varphi_B(P_A), \varphi_B(Q_A)$ are as above and

$$E_{AB} \cong E_0/\langle [m_A]P_A + [n_A]Q_A, [m_B]P_B + [n_B]Q_B \rangle \tag{1}$$

- $(E_A, E_B, \varphi_A(P_B), \varphi_A(Q_B), \varphi_B(P_A), \varphi_B(Q_A), E_C)$, where $E_A, E_B, \varphi_A(P_B), \varphi_A(Q_B), \varphi_B(P_A), \varphi_B(Q_A)$ are as above and

$$E_{AB} \cong E_0/\langle [m'_A]P_A + [n'_A]Q_A, [m'_B]P_B + [n'_B]Q_B \rangle \tag{2}$$

  where m'_A, n'_A (respectively m'_B, n'_B) are chosen at random from $\mathbb{Z}/2^{e_2}\mathbb{Z}$ (respectively $\mathbb{Z}/3^{e_3}\mathbb{Z}$) and not both divisible by 2 (respectively 3).

determine from which distribution the tuple is sampled.

Theorem 11. (SIDH) Under the SSDDH assumption, the key-agreement protocol is session-key secure in the authenticated-links adversarial model of Canetti and Krawczyk.

The theorem can be proved directly followed the assumption. The proof refers to [JD11].

4 Implementation

4.1 Parameter Choices

In our implementation, we follow [CLN16] and choose

$$p = 2^{372} \cdot 3^{239} - 1.$$

Although p can be arbitrary for our protocol, the implementation of the protocol benefits from some special forms of p. Choosing $p \equiv -1 \pmod 4$ means that -1 is not a square in $\mathbb{F}_{p^2}$ and hence $\mathbb{F}_{p^2} = \mathbb{F}_p(i)$ for $i^2 = -1$, which makes the arithmetic simpler.

4.2 Implementation Details

We use the GMP library [Gt12] as our high precision arithmetic library. Based on GMP library, we build up several C++ classes and functions based on our purpose.

- Integer class: We wrap the GMP library into the integer class, which is more convenient to use.
- Fp class: We implement the basic $\mathbb{F}_p$ field using Integer class as well as computing the square root of an element.
- Fp2 class: Similar to $\mathbb{F}_p$, we implement the basic $\mathbb{F}_{p^2}$ field containing the square root algorithm.
- Curve class and RPoint class: We store the Weierstrass Form of the curve. Both curves and points are stored in projective coordinates to avoid finite field invert operation. The addition and doubling refer to [BL07].
- Isogeny class: The isogenies are computed using Velu's Formula.
- IsogenyChain class: The IsogenyChain class maintains compositions of 2-degree or 3-degree isogenies, and use them to construct long isogenies with smooth degree. The construction is achieved by a divide-and-conquer algorithm [JD11] on the triangle of isogeny chains. The algorithm takes time complexity of $\tilde{O}(\max\{e_2, e_3\})$.
- run_protocol() in Protocol.cc: We implement the SIDH key exchange protocol followed the algorithms described in the previous sections using the classes and tools above. Finally both Alice and Bob agreed on the same key.

4.3 Experiments

We run the test on our laptops. The result is shown below.

	768-bit p
Public parameter	2.05125s
Alice round 1	0.943308s
Bob round 1	0.90422s
Exchange message	0.393379s
Alice round 2	0.951511s
Bob round 2	0.968126s

5 Conclusion

We implement a conjecturally quantum-resistant key-agreement protocol (SIDH) using isogenies between supersingular elliptic curves of smooth order, which is first published in [JD11]. The fastest known attacks against this scheme, even on quantum computers, require fully exponential time.

In this report, we briefly introduce some mathmatical concepts as the foundation of isogeny-based cryptography, and then introduce the protocol of SIDH and our implementation, with some details. After that, we give a security proof of the protocol based on the hardness of SSDDH problem. Furthermore, based on this scheme, we can also implement a public-key cryptosystem, or give a zero-knowledge proof of identity, which are given in [JD11].

References

[BL07] D. J. Bernstein and T. Lange. *Explicit-Formulas Database*, 2007. `https://www.hyperelliptic.org/EFD/index.html`.

[CLN16] C. Costello, P. Longa, and M. Naehrig. Efficient algorithms for supersingular isogeny Diffie-Hellman. In *CRYPTO 2016, Part I*, *LNCS* 9814, pages 572–601. Springer, Heidelberg, August 2016.

[DF17] L. De Feo. Mathematics of isogeny based cryptography, 2017.

[Gt12] T. Granlund and the GMP development team. *GNU MP: The GNU Multiple Precision Arithmetic Library*, 5.0.5 edition, 2012. `http://gmplib.org/`.

[JD11] D. Jao and L. De Feo. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In *Post-Quantum Cryptography - 4th International Workshop, PQCrypto 2011*, pages 19–34. Springer, Heidelberg, November / December 2011.

[Sil09] J. Silverman. *The Arithmetic of Elliptic Curves*. 01 2009.