Quantum-Resistant Diffie-Hellman Key Exchange from Supersingular Elliptic Curve Isogenies

Amir Jalali

Abstract—Possibility of the emergence of quantum computers in the near future pose a serious threat against the security of widely-used public key cryptosystems such as RSA or Elliptic Curve Cryptography (ECC). Algorithms involving isogeny computations on supersingular elliptic curves have been shown to be difficult to break, even to quantum computers. Thus, isogeny-based protocols represent promising solution to provide quantum-resistant cryptography. This paper, explores a relatively new scheme which allows two parties to generate DH secret shared using isogenies between supersingular elliptic curves. The reason behind using supersingular elliptic curve, is the development of a sub-exponential time quantum algorithm which is able to break isogenies between ordinary elliptic curves. On the other hand, in the case of supersingular elliptic curves, the fastest known quantum attack remains exponential, because of non-commutativity of the endomorphism ring. However, the non-commutativity feature causes the main technical difficulty in the supersingular case, because Diffie-Hellman key-exchange protocol require commutativity of elements to generate shared secret. In this paper, solution to this problem is also investigates and it is shown that providing the outputs of the isogeny on certain points can be deployed to overcome the non-commutativity problem in Diffie-Hellman Key-Exchange protocol.

Index Terms—Diffie-Hellman key-exchange, elliptic curve cryptography, isogeny-based cryptosystems, post-quantum cryptography, supersingular elliptic curves

Introduction

Post-quantum cryptography (PQC) refers to research on cryptographic primitives (mostly public-key cryptosystems) that are not efficiently breakable using quantum computers. These are some alternatives to be secure against quantum computer threats like the McEliece cryptosystem, lattice-based cryptosystems, code-based cryptosystems, multivariate public key cryptography, and the like. Recently, in [7], [8], [9], and [10], efficient implementation of quantum-safe cryptosystems have been implemented on embedded devices. However, none of these works consider making the current cryptosystems based on elliptic curves to be quantum resistance. Therefore, they all introduce and implement new cryptosystems with different performance metrics.

Supersingular Isogeny Diffie-Hellman (SIDH) key exchange is an elliptic curve based alternative to Elliptic Curve Diffie-Hellman (ECDH) which is not vulnerable to Shor’s attack. Isogeny computation construct an algebraic map between elliptic curves, which appear resistant against quantum attacks. Therefore, this kind of cryptosystem improves upon traditional ECC, and it is a promising candidate for quantum-resistant cryptography [13].

Based on recent announcement at PQC 2016 [5], NIST announced a preliminary plan to start the gradual transition to quantum-resistant protocols. Therefore, there is a vital need to discover and implement new protocols that are resistant to both classical and quantum computers. NIST is going to evaluate these PQC protocols based on level of security, speed, size, and tunable parameters. Among these schemes, isogeny-based cryptography provides a suitable replacement for standard ECC or RSA protocols, since it provides smaller key size, forward secrecy\(^1\), and it has a Diffie-Hellman key exchange method available. Moreover, isogeny-based cryptography adopts standard ECC point multiplication scheme, but takes it a step further by computing large isogenies to provide quantum-resistance.

Different cryptography protocols are compared based on different factors. There are often trade-offs to be made in the key size, computational efficiency, ciphertext, and signature size for a given level of security. Thus, it is difficult to compare one scheme against another considering only one dimension of performance. Nevertheless, among all present PQC candidates, isogeny-based cryptography asymptotically provides the smallest key size for a given post-quantum level of security. In Table 1, we provide the key sizes for different post-quantum algorithms for 128-bit security level based on what is currently available in the literature. Moreover, in [1], a key compression method for isogeny-based scheme is introduced, which reduces the key sizes by approximately half.

Preliminaries

This section provides a quick introduction to elliptic curve and isogenies. For a full mathematical background, we encourage the reader to [13] for a full explanation of isogenies and [18] for a complete reference at elliptic curve theory.

Isogenies on Elliptic Curves

Elliptic Curve Cryptography (ECC) basically deals with the curve arithmetic between points on curves to establish protocols. The most notable application, is the use of point doubling and point addition to generate scalar multiplication, \(Q = kP\). This work basically deals with Montgomery curves because of the fast scalar point multiplication and isogeny computations [14], which will be introduced in further details later. Therefore, we define a Montgomery curve, which will always have a corresponding isomorphic Weierstrass curve, over a field \(\mathbb{K}\) in the Montgomery form:

\[
E : By^2 = x^3 + Ax^2 + x
\]

\(^1\)A protocol is forward secret, if it only has to generate one random public key per session for key agreement.

An elliptic curve is composed of all points \((x, y)\) that satisfy the elliptic curve equation for values \(A, B \in K\) as well as a point at infinity, \(O\). The point at infinity acts as the identity element and the elliptic curve becomes an abelian group over point addition. The \(j\)-invariant is an important quantity of elliptic curves that determines its isomorphism. For Montgomery curves, this value is defined by:

\[
    j(E) = 256 \frac{(A^2 - 3)^3}{A^2 - 4}
\]

Isogeny-based cryptography utilizes unique algebraic maps between elliptic curves that satisfy group homomorphism. The idea of isogeny-based cryptography was first introduced by J. Silverman [18] and has been investigated for quantum-resistant cryptography by Jao et al. [13].

For two elliptic curves over a finite field to be isogenous, they must have the same number of points [20] and have the same \(j\)-invariant. We define an isogeny to be \(\phi : E \to E'\) such that \(\phi\) satisfies group homomorphism. The degree of an isogeny, \(\deg q\phi\), is its degree as an algebraic map. We are particularly interested in computing isogenies of high degree. A curve’s endomorphism ring is defined as the ring of all isogenous curves from a curve itself, under point addition and functional composition. A curve is considered supersingular if this endomorphism ring has \(\mathbb{Z}\)-rank equal to 4. Supersingular curves can be defined over \(\mathbb{F}_{p^2}\) or \(\mathbb{F}_p\). Therefore, a common field that includes all isogenous curves is \(\mathbb{F}_{p^2}\). Supersingular curves have the property that for every prime \(\ell \neq p\), there exist \(\ell + 1\) isogenies of degree \(\ell\) from a base curve. An isogeny can be computed over a kernel, \(\kappa\), such that \(\phi : E \to E/(\kappa)\) by using Vélu’s formulas [21]. By specifying curves with a smooth shape, rational points of smooth order act as a generator for the isogeny, allowing efficient computations of isogenies.

### Computing Multiple Isogenies

The degree of an isogeny is its degree as an algebraic map. As shown in [6], isogeny computations can be done iteratively. Given an elliptic curve \(E\) and a point \(R\) of order \(\ell\), we compute \(\phi : E \to E/(\ell\cdot R)\) by decomposing \(\phi\) into a chain of \(\ell\) isogenies, \(\phi = \phi_{\ell-1} \circ \cdots \circ \phi_0\), as follows. Set \(E_0 = E\) and \(R_0 = R\), and define:

\[
    E_i = E_i / (\ell^{i-1} \cdot R_i), \quad \phi_i : E_i \to E_{i+1}, \quad R_{i+1} = \phi_i(R_i)
\]

Essentially, point additions are used to compute the kernel at each iteration and Vélu’s formulas are used to compute \(\phi_i\) and \(E_{i+1}\). There is always an optimal strategy based on the least number of steps in the isogeny graph to determine the desired isogeny. Finding this strategy is essentially a non-trivial combinatorial problem that only has to be done once for particular degrees of isogenies. One can refer to [13] for further details calculating an optimal strategy over isogeny maps.

### Key-Exchange Protocol Based on Isogenies

Two parties, Alice and Bob, want to exchange a secret key over an insecure channel in the presence of malicious third-parties. They agree on a prime \(p\) of the form \(\ell_a \ell_b \cdot f \pm 1\) where \(\ell_a\) and \(\ell_b\) are small primes, \(a\) and \(b\) are positive integers, and \(f\) is a small cofactor to make the number prime. They define a supersingular elliptic curve, \(E(F_q)\) where \(q = p^2\). Lastly, they agree on four points on the curve that form two independent bases. These are a basis \(P_A, Q_A\) of \(E[\ell_A]\) over \(\mathbb{Z}/\ell_A^2\mathbb{Z}\) and a basis \(P_B, Q_B\) of \(E[\ell_B]\) over \(\mathbb{Z}/\ell_B^2\mathbb{Z}\). Essentially, each party takes seemingly random walks in the graphs of isogenies of degree \(\ell_A\) and \(\ell_B\) to both arrive at a curve with the same \(j\)-invariant, similar to Diffie-Hellman key-exchange. In a graph of supersingular isogenies, the infeasibility to discover a path that connects two particular vertices provides security for this protocol. A detailed discussion of the security of the protocol is given in [13]. The bottom line is that the isogenies change the endomorphic group in such a way that Shor’s Algorithm [17] and other attacks on the group structure are no longer feasible.

Alice chooses two private keys \(m_A, n_A \in \mathbb{Z}/\ell_A^2\mathbb{Z}\) with the stipulation that both are not divisible by \(\ell_A\). On the other side, Bob chooses two private keys \(m_B, n_B \in \mathbb{Z}/\ell_B^2\mathbb{Z}\), where both private keys are not divisible by \(\ell_B\). From there, the key-exchange protocol can be broken down into two rounds of the following:

1. Compute \(R = \langle m \cdot P + n \cdot Q \rangle\) for points \(P, Q\).
2. Compute the isogeny $\phi : E \rightarrow E/(R)$ for a supersingular curve $E$.

3. Compute the kernels $\phi(P)$ and $\phi(Q)$ for the first round.

The key exchange protocol is shown in Figure 1. For a better illustration, we provide a step-by-step example of this protocol in the appendix. Alice performs the double point multiplication with her private keys to obtain a kernel, $R_A = \langle [m_A]P + [n_A]Q \rangle$. She performs the isogeny quickly by performing many small isogenies of size $\ell_A$. She then computes the projection $\phi_A(P_B), \phi_A(Q_B) \subset E_A$ of the basis $P_B, Q_B$ for $E[\ell_B]$ under her secret isogeny $\phi_A$, which can be done efficiently by pushing the points $P_B$ and $Q_B$, and computing an isogeny through the isogeny at each smaller isogeny. Over a public channel, she sends these points and curve $E_A$ to Bob. Likewise, Bob performs his own double-point multiplication and computes his isogeny over the supersingular curve $E$ with $\phi_B : E \rightarrow E = E/(\langle [m_B]P + [n_B]Q \rangle)$. He also computes his projection $\phi_B(P_A), \phi_B(Q_A) \subset E_B$ of the basis $P_A, Q_A$ for $E[\ell_A]$ under his secret isogeny $\phi_B$ and sends these points and curve $E_B$ to Alice. For the second round, Alice performs the double point multiplication and computes its isogeny over the supersingular curve $E$ with $\phi_B : E \rightarrow E_B = E/(\langle [m_B]P + [n_B]Q \rangle)$. Bob also performs a double point multiplication and computes a second isogeny $\phi_B : E_A \rightarrow E_{BA} = E_A/(\langle [m_B]\phi_A(P_B) + [n_B]\phi_A(Q_B) \rangle)$. Alice and Bob now have isogenous curves and can use the common $j$-invariant as a shared secret key.

$$E_{AB} = \phi_B(\phi_A(E)) = \phi'_B(\phi_B(E)) = E/[m_A]P + [n_A]Q, [m_B]P + [n_B]Q_B,$$

$$j(E_{AB}) \equiv j(E_{BA}).$$

Parameter Generation for Key-Exchange

The common system parameters for isogeny-based cryptosystems are the prime curve $E$, and points $P_A, P_B, Q_A, Q_B$ over $E$. After finding a prime of form $p = \ell_A^{\alpha} \ell_B^{\beta} \cdot f + 1$, a supersingular curve can be found over $\mathbb{F}_p$, with cardinality $(p + 1)^2 = (\ell_A^{\alpha} \ell_B^{\beta} \cdot f)^2$ by constructing the isogeny graph consisting of all supersingular curves denoted over $\mathbb{F}_p$ and performing random walks to determine a starting curve $E$. The basis for Alice, $P_A, Q_A$ can be obtained by selecting random points on $E$ and ensuring that the order of the point is $\lambda_A$ by multiplying $P$ by powers of $\ell_A$. If the order is exact, then the second point $Q_A$ is also found by picking a random point and testing that the order is $\ell_A^\alpha$. The set $P_A, Q_A$ is a valid basis if the two points are independent, which is checked by computing the Weil pairing $e(P_A, Q_A)$ in $E_0[\ell_A]$ and verifying that the result has order $\ell_A^\alpha$. If this fails, different point $Q_A$ can be randomly chosen and tested again for independence. After this passes, a valid basis has been generated. The same procedure occurs for Bob’s basis $P_B, Q_B$. This parameter generation only has to occur once to setup a key-exchange protocol. Parameters can be reused multiple times for various key-exchanges. Lastly, each party computes their optimal strategy for isogenies, which is explained in [13].

The parameter generation requires the Weil pairing as well as large factoring of polynomials. It only needs to be performed once, so the parameter generation was left outside of the key-exchange protocol.

CONCLUSION

Possibility of the emergence of quantum computers in the near future, pose a serious threat against the security of widely-used public key cryptosystems such as RSA or Elliptic Curve Cryptography (ECC). Whether the quantum computers will appear in future or not, working around more secure and reliable cryptosystems is a wise practice. Algorithms involving isogeny computations on supersingular elliptic curves have been shown to be difficult to break, even for quantum settings. Thus, isogeny-based protocols represent promising solution to provide quantum-resistant cryptography. In this paper, we explored a relatively new scheme which allows two parties to generate DH secret shared using isogenies between supersingular elliptic curves. The reason behind using supersingular elliptic curve, is the development of a sub-exponential time quantum algorithm which is able to break isogenies between ordinary elliptic curves. Moreover, ordinary elliptic curves are much slower than supersingular curves in the matter of isogeny computations.

One of the main advantages of this scheme is that it is working with elliptic curve cryptosystem. This makes it much easier to move towards quantum-resistant cryptosystem from classical elliptic cryptography. Furthermore, working around elliptic curve cryptography as cryptography primitives, leads to better flexibility of key-exchange protocols. That is, hybrid key-exchange protocols can be implemented based on the same public parameters.

REFERENCES


