RIMS Kôkyûroku Bessatsu
B90 (2022), 97–116

Post-Quantum Cryptography from Supersingular Isogenies

By

Yusuke Aikawa*

Abstract

This paper is based on a presentation made at RIMS conference on "Theory and Applications of Supersingular Curves and Supersingular Abelian Varieties", so-called "Supersingular 2020".

Post-quantum cryptography is a next-generation public-key cryptosystem that resistant to cryptoanalysis by both classical and quantum computers. Isogenies between supersingular elliptic curves present one promising candidate, which is called isogeny-based cryptography. In this paper, we give an introduction to two isogeny-based key exchange protocols, SIDH [17] and CSIDH [2], which are considered as a standard in the subject so far. Moreover, we explain briefly our recent result [24] about cycles in the isogeny graphs used in some parameters of SIKE, which is a key encapsulation mechanism based on SIDH.

§ 1. Introduction

Public-key cryptography (PKC, for short) is an indispensable technology in the information society that enables us encrypted communication without sharing the key in advance. The hardness assumptions of some mathematical problems support the security of PKC; the integer factorization problem, the discrete logarithm problem for example. So it is important to analyze the difficulty of such mathematical problems on which the security of cryptography is based. These problems support cryptography in use now and are considered to be difficult to solve efficiently using classical computers so far. However, in 1994, Shor presented a quantum algorithm solving them in low-degree polynomial time [27], which is called Shor's algorithm now.

Received January 7, 2021. Revised April 26, 2021.
2020 Mathematics Subject Classification(s): 11T71, 14H52, 14K02
The author is supported by JST, ACT-X Grant Number JPMJAX2001, Japan.

*Information Technology R&D Center, Mitsubishi Electric Corporation, Kanagawa, Japan.
e-mail: `Aikawa.Yusuke@bc.MitsubishiElectric.co.jp`

Recently, many big IT companies in the world have been developing large-scale quantum computers with tremendous momentum. Quantum computers use properties of quantum mechanics to implement algorithms which are not possible to compute on classical computers. Shor's algorithm is a one of typical algorithms. As mentioned earlier, this algorithm solves the integer factorization problem and the discrete logarithm problem on a group in low-degree polynomial time. In this sense, the emergence of quantum computers threatens PKC, such as RSA cryptography and Elliptic Curve Cryptography. Therefore we need quantum-resistant cryptography whose security relies on the difficulty of new mathematical problems. That is, we need cryptography based on a mathematical problem which no polynomial-time quantum algorithm is known to solve. Such cryptography is called post-quantum cryptography (PQC, for short). Since 2016, the standardization process of PQC sponsored by NIST is in progress [1].

Isogeny-based cryptography is one of the promising candidates of PQC. It is considered so far that computing isogenies between given two elliptic curves over a finite field is computationally hard. Isogeny-based cryptography is built on the difficulty of this problem. This perspective provides a new crossover of mathematics and cryptography.

The first proposal of isogeny-based cryptography was made by Couveignes [8] in 1997 [1]. By introducing the concept of Hard Homogeneous Spaces (HHS, for short), Couveignes constructed a quantum-resistant key exchange protocol from HHS and exhibited the CM-action of an ideal class group of an imaginary quadratic field on ordinary elliptic curves as an instantiation of HHS. In 2006, Rostovtsev and Stolbunov [26] developed the same method independently. This cryptosystem is often called the CRS scheme now. However, the CRS scheme is significantly slow to compute an action of ideal class on an ordinary curve. Although there is an attempt to speed them up [12], this scheme is far from practical at this time. The problem of constructing ordinary curves suitable for isogeny computation still remains.

The first application of isogenies between supersingular elliptic curves to cryptography appeared in 2009. Charles, Lauter and Goren constructed a cryptographic hash function using supersingular isogeny graphs [3]. After that, in [17], Jao and De Feo proposed a Diffie-Hellman style key exchange protocol from supersingular isogenies, which is modeled as random walks in isogeny graphs. One of the crucial facts is that the order of supersingular elliptic curves is determined by the characteristic of the field of definition. Therefore, by using a prime of special form, we could take torsion points from a quadratic extension of the prime field. Then isogeny computations are implemented efficiently using Vélu's formula. This scheme was named Supersingular Isogeny Diffie-Hellman (SIDH). Moreover, the key encapsulation mechanism SIKE [16] based on SIDH was submitted to NIST's competition for the standardization for PQC.

[1] This work was not published but posted on IACR Cryptography ePrint Archive.

After the launch of NIST's standardization process of PQC, Castryck et al. [2] proposed an efficient action of an ideal class group on supersingular elliptic curves, which is the first practical instantiation of HHS. Using this action, they construct an efficient Diffie-Hellman style key exchange protocol from isogenies, which was named Commutative Supersingular Isogeny Diffie-Hellman (CSIDH).

These schemes, SIDH and CSIDH, are considered to be standard in isogeny-based cryptography now. A large number of studies have been conducted on them from both security and efficiency points of view. However, not all of them can be discussed here for want of space. In this paper, as an introduction to isogeny-based cryptography, we will explain how to use supersingular isogenies to construct PKC through the construction of SIDH and CSIDH.

Acknowledgements. The author deeply wishes to thank the organizers, Shushi Harashita, Momonari Kudo and Katsuyuki Takashima for giving me an opportunity to talk at "Supersingular 2020" and write this paper. This work was supported by the Research Institute for Mathematical Sciences, an International Joint Usage/Research Center located in Kyoto University. This work was also supported by Japan Science and Technology Agency, ACT-X Grant Number JPMJAX2001, Japan.

§ 2. Preliminaries

We begin by summarizing the definitions and the well-known facts about elliptic curves and isogenies necessary in the context of isogeny-based cryptography. We refer to [28], [30] for their mathematical general theory and to [4], [14] for their cryptographic use for example.

§ 2.1. Elliptic Curves

2.1.1. Basic Definitions and Properties We fix a prime $p > 3$ and a power $q = p^r$. *An elliptic curve* E over $\mathbb{F}_q$ is a smooth projective curve over $\mathbb{F}_q$ of genus one with a specified point ∞. Let E be an elliptic curve over $\mathbb{F}_q$. As is well known, the curve E has the Weierstrass model:

$$y^2 = x^3 + ax + b, \tag{2.1}$$

where $a, b \in \mathbb{F}_q$ and $4a^3 + 27b^2 \neq 0$, which ensure the smoothness of E. An important property of elliptic curves is that the set of rational points $E(\mathbb{F}_q)$ carries a group structure with the identity element ∞. Hasse's theorem states that we can write $\#E(\mathbb{F}_q) = q + 1 - t$ with $|t| \leq 2\sqrt{q}$. This t is called the Frobenius trace. The elliptic curve E is called *supersingular* if $p|t$ and *ordinary* otherwise. Hence orders of supersingular elliptic curves over a prime field $\mathbb{F}_p$ are determined by the characteristic $p > 3$: $\#E(\mathbb{F}_p) = p + 1$.

Let E_1 and E_2 are elliptic curves over $\mathbb{F}_q$. A morphism of curves $\phi : E_1 \to E_2$ satisfying $\phi(\infty) = \infty$ is called an *isogeny.* Two curves are called *isogenous* if there is a non-zero isogeny between them. Tate's theorem states that E_1 and E_2 are isogenous over $\mathbb{F}_q$ if and only if $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$. Every non-zero isogeny $\phi : E_1 \to E_2$ induces a field extension of function fields $\overline{\mathbb{F}}_q(E_1)/\phi^*\overline{\mathbb{F}}_q(E_2)$. We say that an isogeny ϕ is separable if the extension $\overline{\mathbb{F}}_q(E_1)/\phi^*\overline{\mathbb{F}}_q(E_2)$ is *separable.* We define the *degree* of a non-zero isogeny ϕ as $\deg\phi = [\overline{\mathbb{F}}_q(E_1) : \phi^*\overline{\mathbb{F}}_q(E_2)]$. An isogeny from a curve E to itself is called an *endomorphism* of E. An important example of endomorphisms is the scalar multiplication on a curve E by $n \in \mathbb{Z}$; $P \mapsto nP$. It is denoted by $[n]$. We write the kernel of $[n]$ as $E[n]$; $E[n] = \{P \in E(\overline{\mathbb{F}}_q) \mid nP = \infty\}$. If $(p, n) = 1$, we have $E[n] \simeq \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. The Frobenius map $(x, y) \to (x^q, y^q)$ is also a basic endomorphism on a curve defined over a finite field. Throughout this paper, we denote the Frobenius map by π_q. The Frobenius map satisfies the equation $\pi_q^2 - t\pi_q + q = 0$ as endomorphisms, where $t = q + 1 - \#E(\mathbb{F}_q)$ is the Frobenius trace.

We say that two elliptic curves E_1 and E_2 are *isomorphic* if there are isogenies $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on E_1 and E_2, respectively. The *j-invariant* of an elliptic curve E given by the Weierstrass model (2.1) is defined as: $j_E = 1728\frac{4a^3}{4a^3+27b^2}$. Two elliptic curves are isomorphic over $\overline{\mathbb{F}}_q$ if and only if their j-invariants are equal.

In cryptographic applications, instead of the Weierstrass model, we often use another useful model of elliptic curves, called Montgomery curves, which is introduced by Montgomery [23] in the context of an application of elliptic curves for integer factorizations, Lenstra's Elliptic Curve Method [21]. A Montgomery curve is given by the following equation:

$$E_{a,b} : by^2 = x^3 + ax^2 + x. \tag{2.2}$$

Montgomery curves have an efficient scalar multiplication algorithm, so-called the Montgomery ladder, which makes such curves suitable for cryptographic application of elliptic curves. In fact, as we will see later, the scalar multiplication plays a central role in the cryptography using elliptic curves. Therefore, such curves are indispensable for constructing efficient cryptographic schemes using elliptic curves.

The j-invariant of a Montgomery curve $E_{a,b}$ is computed as: $j_{E_{a,b}} = \frac{256(a^2-3)^3}{a^2-4}$. This shows that the $\overline{\mathbb{F}}_q$-isomorphic class of $E_{a,b}$ is completely determined by a^2 only and we can see the coefficient b as a twisted factor. Hence, if we work over isomorphism classes of elliptic curves, we simply write a Montgomery curve $E_a : y^2 = x^3 + ax^2 + x$ putting $b = 1$. For example, the elliptic curve of a Montgomery form $E_0 : y^2 = x^3 + x$ is supersingular if $p \equiv 3 \pmod 4$, which is often used in isogeny-based cryptography as the initial curve. One can see details of the arithmetic theory and cryptographic applications of Montgomery curves with a survey article [7].

2.1.2. Vélu's Formula

Let E be an elliptic curve. We describe a relationship between isogenies going out of E and finite subgroups of $E(\overline{\mathbb{F}}_q)$. Let $G \subset E(\overline{\mathbb{F}}_q)$ be a finite subgroup. We say that G is defined over $\mathbb{F}_q$ if $\sigma(P) \in G$ for $P \in G$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$. The proposition below plays a crucial role in isogeny-based cryptography. One can find the proof in [28].

Proposition 2.1. *Let E be an elliptic curve over $\mathbb{F}_q$ and $G \subset E(\overline{\mathbb{F}}_q)$ a finite subgroup defined over $\mathbb{F}_q$. Then there is an elliptic curve $E'/\mathbb{F}_q$ and a separable isogeny $\phi : E \to E'$ over $\mathbb{F}_q$ of degree $\#G$ with $\mathrm{Ker}(\phi) = G$. Moreover, the target curve E' is uniquely determined from G up to isomorphism. Hence we usually denote the target by E/G.*

Due to this correspondence, we can encode information of isogenies in terms of points on elliptic curves. For E and G, Vélu described how to write down equations for the target E/G and an isogeny $E \to E/G$ explicitly. As we will mention below, we compute small prime degree isogenies repeatedly in isogeny-based cryptography. So we often take G as a cyclic group $\langle P \rangle$ generated by ℓ-torsion point P for a small prime ℓ, which is distinct from the characteristic of the base field which we are working over. The following formula, which is called Vélu's formula, is one of the most important tools for computational aspects of isogeny-based cryptography. Although this formula is proved for the generalized Weierstrass forms, we describe a special case, from the Weierstrass form to the same form, only here.

Theorem 2.2 (Vélu's Theorem [29]). *Let E be an elliptic curve given by the Weierstrass model (2.1) and $G \subset E(\overline{\mathbb{F}}_q)$ a finite subgroup. Let G_2 be the set of points of order 2 in G. We divide G as $G = \{\infty\} \cup G_2 \cup G^+ \cup G^-$, where $P \in G^+$ if and only if $-P \in G^-$. For $P = (x_P, y_P)$, put:*

$$g_P^x = 3x_P^2 + a, \ g_P^y = -2y_P;$$

$$v_P = \begin{cases} g_P^x & (P \in G_2) \\ 2g_P^x & (\textit{otherwise}), \end{cases} \quad u_P = (g_P^y)^2.$$

Let $\widetilde{G}^+ = G^+ \cup G_2$ and set;

$$v = \sum_{P \in \widetilde{G}^+} v_P, \ w = \sum_{P \in \widetilde{G}^+} (u_P + x_P v_P).$$

Then, we can write a target E/G by the equation $y^2 = x^3 + (a - 5v)x + (b - 7w)$. And *an isogeny ϕ from E to E/G is given by;*

$$\phi(x,y) = \big(x + \sum_{P \in \widetilde{G}^{+}} (\frac{v_P}{x - x_P} - \frac{u_P}{(x - x_P)^2}), y - \sum_{P \in \widetilde{G}^{+}} \frac{2u_P y}{(x - x_P)^3} - v_P \frac{y - y_P - g_P^x g_P^y}{(x - x_P^2)}\big).$$

Thanks to Vélu's formula, one can compute an isogeny and its target curve by taking torsion points. Therefore, from the viewpoint of efficiency, it is desirable to obtain torsion points defined over an extension field of low degree. The technique of generating such torsion points can be achieved by using supersingular elliptic curves since the order of supersingular elliptic curves is determined by the characteristic p of the base field. Therefore, in isogeny-based cryptography, in order to take torsion points with coordinates in $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ we use a prime of special forms, see §3.1.2 and §3.2.2. This is a crucial technique which makes isogeny computation practical.

The complexity of Vélu's formula for an N-isogeny is $O(N)$ operations on a finite field, which is exponential complexity with respect to the degree of an isogeny. Hence, in order to compute an isogeny of degree of cryptographic size, 256-bit integers for example, we decompose it into chains of isogenies of small prime degree. This is a key idea which makes isogeny-based cryptography feasible.

As mentioned above, in the setting of elliptic curve cryptography, we often use Montgomery curves due to efficient scalar multiplications. A new formula for computing odd-degree isogenies from a Montgomery curve to a Montgomery curve was proposed by Costello and Hisil [6]. In isogeny-based cryptography, this formula is mainly used for computing isogenies.

2.1.3. Endomorphism Rings of Supersingular Elliptic Curves For a supersingular curve E over a finite field of the characteristic p, its endomorphism ring $\mathrm{End}(E)$ is isomorphic to a maximal order in $B_{p,\infty}$, where $B_{p,\infty}$ is the unique quaternion algebra ramified at p and ∞ up to isomorphism. We have $B_{p,\infty} = \mathbb{Q} + \mathbb{Q}\mathbf{i} + \mathbb{Q}\mathbf{j} + \mathbb{Q}\mathbf{k}$ with $\mathbf{i^2} = -1$, $\mathbf{j^2} = -p$ and $\mathbf{k} = \mathbf{ij} = -\mathbf{ji}$ if $p \equiv 3 \pmod 4$.

The Deuring corresponding [9] states that there is a one-to-one correspondence between the j-invariants of supersingular elliptic curves over $\mathbb{F}_{p^2}$ up to Galois conjugacy in $\mathbb{F}_{p^2}$ and maximal orders in the quaternion algebra $B_{p,\infty}$ via taking full endomorphism rings of supersingular elliptic curves. For example, if $p \equiv 3 \pmod 4$, the curve E_0 defined by $y^2 = x^3 + x$ is supersingular and we have $\mathrm{End}(E_0) \simeq \mathbb{Z} + \mathbb{Z}\mathbf{i} + \mathbb{Z}\frac{\mathbf{1+k}}{\mathbf{2}} + \mathbb{Z}\frac{\mathbf{i+j}}{\mathbf{2}}$. As we will see in §4, it is important to know the structure of the endomorphism ring of a supersingular elliptic curve in order to analyze the structure of isogeny graphs.

§ 2.2. Diffie-Hellman Key Exchange

Key exchange is a cryptographic method by which cryptographic keys are shared between two parties secretly. Let us consider the following situation: there are two parties, Alice and Bob, who want to communicate through an open communication channel, for example, the Internet. If they want to communicate secretly, how to send messages to each other? In this situation, the aim is to send messages to the opposite without leakage of what is written in the messages. Symmetric-key cryptography offers a powerful solution and has been used from ancient times. Symmetric-key cryptography works as follows (this is a rough sketch, for more detail see [18] for example): Firstly, Alice and Bob share a key k. Secondly, Alice inputs her message m and the key k into an encryption algorithm. Then she obtains a ciphertext as an output of the algorithm and sends it to Bob. Finally, when Bob receives it, he decrypts the ciphertext using the key k, yielding the message m. As we saw above, in the setting of symmetric-key cryptography, two parties must share the key k. Here, there is a serious problem: how they share the key?

In their revolutionary paper [10], Diffie and Hellman proposed a key exchange protocol, which enables two parties to derive a common secret key by their interaction over an open channel. Consider a situation that we have two parties, Alice and Bob, who want to establish a shared secret key. We describe how the Diffie-Hellman key exchange protocol works now:

- **Set-up**
  Generate a group G and an element $g \in G$ as a public parameter, typically G is cyclic and g a generator. Put $N = \#G$. Then two parties agree on G and g.

- **Key Generation**
  Alice chooses $a \in \mathbb{Z}/N$ secretly at uniformly random and computes $g_A = g^a$. Bob also chooses $b \in \mathbb{Z}/N$ and computes $g_B = g^b$.

- **Key Exchange**
  Both exchange g_A and g_B each other through an insecure channel. When Alice receives g_B from Bob, she computes $(g_B)^a = (g^b)^a = g^{ab}$ using her secret a. Bob does similarly. Then, they can share the common value g^{ab} secretly.

Once two parties share the common value g^{ab} in this way, they can communicate secretly using symmetric-key cryptography with the key g^{ab}. So the security of this protocol relies on the hardness of the problem below.

Problem 2.3 (Computational Diffie-Hellman (CDH) Problem). *Let G be a group and g an element in G. For given (g, g^a, g^b), compute g^{ab}.*

Considering a naive attack to this problem leads us to the discrete logarithm problem on G.

Problem 2.4 (Discrete Logarithm Problem (DLP) on a group G). *Let G be a group and $g \in G$. Let a be an integer. For given (g, g^a), compute $a \in \mathbb{Z}$.*

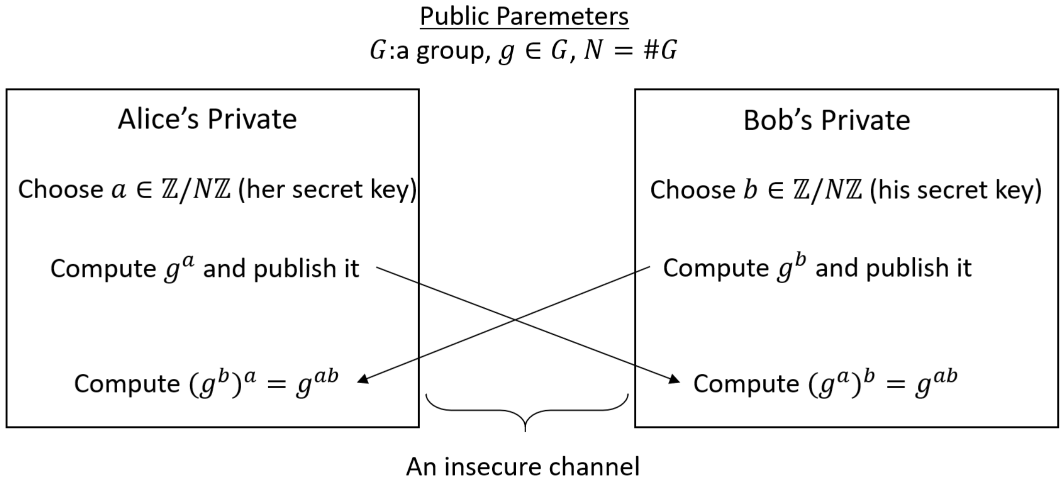
Public Paremeters
G:a group, $g \in G$, $N = \#G$
Alice's Private
Choose $a \in \mathbb{Z}/N\mathbb{Z}$ (her secret key)
Compute g^a and publish it
Compute $(g^b)^a = g^{ab}$
Bob's Private
Choose $b \in \mathbb{Z}/N\mathbb{Z}$ (his secret key)
Compute g^b and publish it
Compute $(g^a)^b = g^{ab}$
An insecure channel

Figure 1. Illustration of the DH key-exchange protocol

Solving the discrete logarithm problem of the group G reveals the shared key derived from the DH key exchange protocol over G. In other wards, the CDH problem is reduced to the DLP. Hence a choice of a group on which the protocol works has an impact on the security of the protocol. That is, we have to choose a group whose DLP is difficult to solve. In [10], the multiplicative group of a finite field $G = \mathbb{F}_q^\times$ is suggested.

2.2.1. Elliptic Curve Diffie-Hellman (ECDH) The most important instantiation of Diffie-Hellman key exchange is to use elliptic curve groups, which is called elliptic curve Diffie-Hellman (ECDH). Koblitz [19] and Miller [22] suggested replacing the finite fields with elliptic curves, with the hope that the discrete logarithm problem in elliptic curve groups is harder to solve than the discrete logarithm problem in the multiplicative group of a finite field. This intuition opens the door to vast research area of cryptography using elliptic curves, elliptic curve cryptography(ECC). A large number of studies have been conducted on this subject. However, to discuss such topics as a whole is out of the scope of this paper. As a reference of these topics, we suggest [4], [30] for example.

2.2.2. Shor's Algorithm As we saw above, the security of public-key cryptography relies on the hardness of some mathematical problems. That is, solving a problem on which the security of cryptography is based means that this cryptography is broken.

In 1997, Shor proposed a quantum algorithm solving the DLP on a group and the integer factorization problem in polynomial time, which is called Shor's algorithm now [27]. This algorithm has a huge impact on the security of public-key cryptography based on the hardness of these mathematical problems. Therefore, we have to construct a quantum-resistant cryptography whose security is based on new mathematical problems and analyze its security from both classical and quantum points of view.

§ 3. Key Exchange Protocols from Supersingular Isogenies

Isogeny-based cryptography is a public-key cryptography whose security is based on the hardness assumption on computation of isogenies between given two curves.

Problem 3.1 (General Isogeny Problem). *Let E_1 and E_2 are isogenous elliptic curves over a finite field. Then compute an isogeny linking them.*

In this research area, variants of the above problem are considered depending on the construction of schemes. At present, there are two standard key exchange protocols, SIDH [17], [11] and CSIDH [2], from isogenies between supersingular curves. In this section, we will explain these schemes.

§ 3.1. SIDH

3.1.1. Setting on SIDH SIDH (Supersingular Isogeny Diffie-Hellman) which is proposed by Jao and De Feo in 2011 [17] is the first key exchange protocol using supersingular elliptic curves.[2]

Let ℓ_A, ℓ_B are distinct small primes (typically $\ell_A = 2$, $\ell_B = 3$) and e_A, e_B integers such that $p = \ell_A^{e_A} \ell_B^{e_B} - 1$ is a prime of cryptographic size, for example $\log_2 p = 512$. Let E be a supersingular elliptic curve over $\mathbb{F}_p$. A key property is that the order of E is smooth; $\#E(\mathbb{F}_{p^2}) = (p+1)^2 = \ell_A^{2e_A} \ell_B^{2e_B}$. This is one of the important reasons for using supersingular curves in isogeny-based cryptography.

Lemma 3.2. *In the above setting, $E[\ell_A^{e_A}]$ and $E[\ell_B^{e_B}]$ are contained in $E(\mathbb{F}_{p^2})$.*

Due to this lemma, one can take a basis P_A, Q_A of $E[\ell_A^{e_A}]$ defined over $\mathbb{F}_{p^2}$. Then, for randomly picked integers $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}$ (at least one of m_A and n_A is coprime to ℓ_A), an $\mathbb{F}_{p^2}$-rational point $R_A = m_A P_A + n_A Q_A \in E[\ell_A^{e_a}]$ has order $\ell_A^{e_A}$. So the subgroup $\langle R_A \rangle$ induces an ℓ^{e_A}-isogeny , which is computed over $\mathbb{F}_{p^2}$ using Vélu's formula. This isogeny is interpreted as an e_A-step random walk in the ℓ_A-isogeny graph. Here, for a prime ℓ, the ℓ-isogeny graph over $\overline{\mathbb{F}}_q$ $\mathcal{G}_\ell(p)$ is a graph whose vertices consist of all elliptic curves over $\overline{\mathbb{F}}_q$ and edges (E_1, E_2) are defined if there is an ℓ-isogeny from E_1 to E_2. We note that the graph $\mathcal{G}_\ell(p)$ is undirected due to the existence of the dual isogeny.

3.1.2. Construction of SIDH

In the above setting, the SIDH key exchange protocol works as follows:

[2] As we mentioned in §1, a key exchange protocol based on ordinary curves is constructed in the context of instantiating Hard Homogeneous Spaces from the CM action.

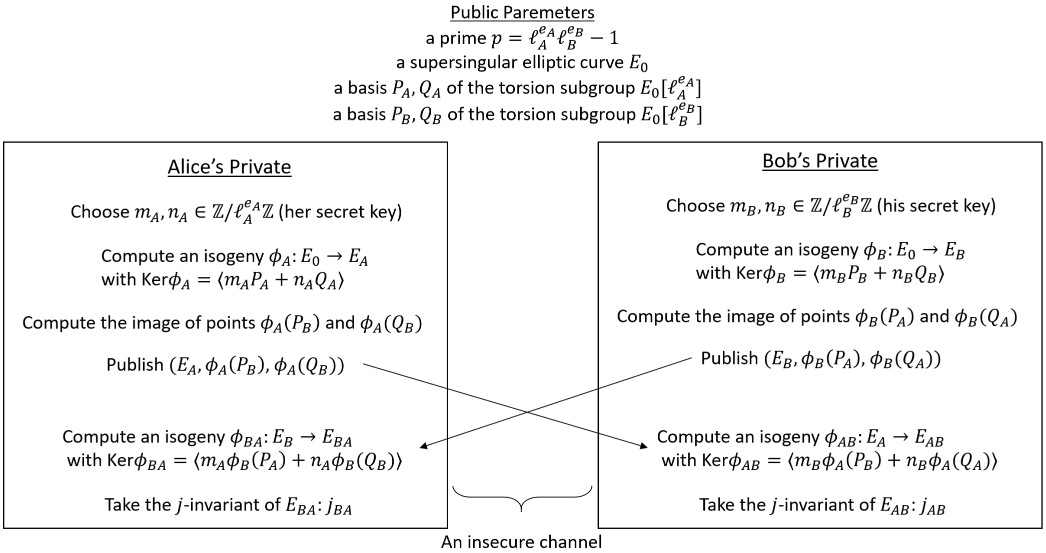
Public Paremeters
a prime $p = \ell_A^{e_A}\ell_B^{e_B} - 1$
a supersingular elliptic curve E_0
a basis P_A, Q_A of the torsion subgroup $E_0[\ell_A^{e_A}]$
a basis P_B, Q_B of the torsion subgroup $E_0[\ell_B^{e_B}]$
Alice's Private
Choose $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ (her secret key)
Compute an isogeny $\phi_A: E_0 \to E_A$
with Ker$\phi_A = \langle m_A P_A + n_A Q_A \rangle$
Compute the image of points $\phi_A(P_B)$ and $\phi_A(Q_B)$
Publish $(E_A, \phi_A(P_B), \phi_A(Q_B))$
Compute an isogeny $\phi_{BA}: E_B \to E_{BA}$
with Ker$\phi_{BA} = \langle m_A\phi_B(P_A) + n_A\phi_B(Q_B) \rangle$
Take the j-invariant of E_{BA}: j_{BA}
Bob's Private
Choose $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ (his secret key)
Compute an isogeny $\phi_B: E_0 \to E_B$
with Ker$\phi_B = \langle m_B P_B + n_B Q_B \rangle$
Compute the image of points $\phi_B(P_A)$ and $\phi_B(Q_A)$
Publish $(E_B, \phi_B(P_A), \phi_B(Q_A))$
Compute an isogeny $\phi_{AB}: E_A \to E_{AB}$
with Ker$\phi_{AB} = \langle m_B\phi_A(P_B) + n_B\phi_A(Q_A) \rangle$
Take the j-invariant of E_{AB}: j_{AB}
An insecure channel

Figure 2. Illustration of the SIDH key-exchange protocol

- **Set-up**
  Let λ be a security parameter. Two parties, Alice and Bob, agree on distinct small primes ℓ_A, ℓ_B and exponents e_A, e_Bsuch that $\ell_A^{e_A} \approx \ell_B^{e_B} \approx 2^\lambda$ and $p = \ell_A^{e_A}\ell_B^{e_B} - 1$ is a prime. Both also agree on the initial supersingular curve E_0 over $\mathbb{F}_{p^2}$ and basis P_A, Q_A of $E_0[\ell_A^{e_A}]$ and P_B, Q_B of $E_0[\ell_B^{e_B}]$.

- **Key Generation**
  Alice chooses secret integers $m_A, n_A \in \mathbb{Z}/\ell_A^{e_A}\mathbb{Z}$ and computes an isogeny $\phi_A : E_0 \to E_A$ induced by the cyclic subgroup generated by $R_A = m_A P_A + n_A Q_A$. Then she sends $(E_A, \phi_A(P_B), \phi_A(Q_B))$ to Bob. Bob similarly a secret integer $m_B, n_B \in \mathbb{Z}/\ell_B^{e_B}\mathbb{Z}$ and computes an isogeny $\phi_A : E_0 \to E_B$ induced by the cyclic subgroup generated by $R_B = m_B P_B + n_B Q_B$. Then he sends $(E_B, \phi_B(P_A), \phi_B(Q_A))$ to Alice.

- **Key Exchange** When Alice receives $(E_B, \phi_B(P_A), \phi_B(Q_A))$ from Bob, she computes an isogeny $\phi_{BA} : E_B \to E_{BA}$ induced by the cyclic subgroup generated by $R_{BA} = m_A\phi_B(P_A) + n_A\phi_B(Q_A)$. Then she computes the j-invariant j_{BA} of E_{BA}. Bob also computes an isogeny $\phi_{AB} : E_A \to E_{AB}$ induced by the cyclic subgroup generated by $R_{AB} = m_B\phi_A(P_B) + n_B\phi_A(Q_B)$ and takes j-invariant j_{AB} of E_{AB}

To see this protocol works correctly, we need to show that the resulting values j_{BA} and j_{AB} coincide. Such property is called the correctness of the protocol. In order to show the correctness of this protocol, it suffices to show that the kernels of compositions $\phi_{AB} \circ \phi_A$ and $\phi_{BA} \circ \phi_B$ coincide. We show $\mathrm{Ker}(\phi_{AB} \circ \phi_A) = \langle R_A, R_B \rangle$.

Since $\phi_{AB} \circ \phi_A(R_A) = \infty$ and

$$\begin{aligned}\phi_{AB} \circ \phi_A(R_B) &= \phi_{BA} \circ \phi_A(m_B P_B + n_B Q_B) \\ &= \phi_{BA}(m_B \phi_A(P_B) + n_B \phi_B(Q_B)) \\ &= \infty\end{aligned}$$

holds, we have $\langle R_A, R_B \rangle \subset \mathrm{Ker}(\phi_{AB} \circ \phi_A)$. Conversely, if $R \in E_0(\overline{\mathbb{F}}_{p^2})$ satisfies $\phi_{AB} \circ \phi_A(R) = \infty$, then there is an integer k such that

$$\begin{aligned}\phi_A(R) &= kR_{AB} \\ &= k(m_B \phi_A(P_B) + n_B \phi_A(Q_B)) \\ &= \phi(k(m_B P_B + n_B Q_B) = \phi_A(kR_B).\end{aligned}$$

Then we have $R - kR_B \in \mathrm{Ker}\phi_A$, so there is an integer k' such that $R - kR_B = k'R_A$. Hence $R = k'R_A + kR_B \in \langle R_A, R_B \rangle$. By the symmetric construction of the protocol, we also have $\mathrm{Ker}(\phi_{BA} \circ \phi_B) = \langle R_A, R_B \rangle$. Since the composites $\phi_{AB} \circ \phi_A$ and $\phi_{BA} \circ \phi_B$ have the same kernel, the target curves are isomorphic. Therefore, Alice and Bob can share the common value $j_{BA} = j_{AB} \in \mathbb{F}_{p^2}$ correctly.

3.1.3. Security of SIDH A task of an adversary is to reveal the shared value $j_{BA} = j_{AB}$ from the data transmitted through an insecure channel. This problem is reduced to the following isogeny problem, just as the CDH problem is reduced to DLP on a group in DH key exchange.

Problem 3.3 (SIDH Problem). *Let p, ℓ_A, ℓ_B , e_A, $e_B \in \mathbb{Z}$ and $(E_0, P_A, Q_A, P_B, Q_B)$ be public parameters. Let E_A be an $\ell_A^{e_A}$-isogenous curve to E_0. Then for given $(E_0, P_A, Q_A, E_A, \phi_A(P_B), \phi_A(Q_B))$, compute an isogeny $\phi_A : E_0 \to E_A$.*

§ 3.2. CSIDH

3.2.1. Hard Homogeneous Spaces

In 1997, Couveignes introduced the concept of Hard Homogeneous Spaces (HHS, for short) and constructed a variant of Diffie-Hellman style key exchange protocol based on HHS [8].

Let X be a set endowed with an action by a finite commutative group G. We say X is homogeneous space of G if the action is simply transitive; that is, the map $G \to X$; $g \mapsto g * x$ is bijective for any $x \in X$. A HHS is defined to be a homogeneous space satisfying the following conditions for any $x \in X$, $g \in G$:

1. Computing actions, $(g, x) \mapsto g * x$, is computationally easy;

2. Inverting actions, $(x, g * x) \mapsto g$, is computationally hard.

A key exchange protocol is constructed from a HHS as follows, similar to the DH key exchange;

- **Set-up**
  Generate a HHS X with a finite commutative group G and an element $x_0 \in X$ as a public parameter. Then two parties, Alice and Bob, agree on (X, G) and x_0.

- **Key Generation**
  Alice chooses $g_A \in G$ at uniformly random secretly and computes $x_A = g_A * x_0$. Bob also chooses $g_B \in G$ and computes $x_B = g_B * x_0$.

- **Key Exchange**
  Both exchange x_A and x_B each other through an insecure channel. When Alice receives x_B from Bob, she computes $g_A * x_B = (g_A g_B) * x_0$. Bob does similarly $g_B * x_A = (g_B g_A) * x_0$. Because of commutativity of G, $(g_A g_B) * x_0 = (g_B g_A) * x_0$ holds. Therefore, they can share the common value $(g_A g_B) * x_0$ secretly.

The difference between the DH key exchange and the HHS key exchange is whether the set of public keys has a group structure. Thanks to this lack of algebraic structure in the public key space of the key exchange based on a HHS, the HHS key exchange protocol avoids quantum attacks using Shor's algorithm.

3.2.2. Construction of CSIDH CSIDH is an instantiation of HHS using supersingular elliptic curves defined over a prime field $\mathbb{F}_p$. For a supersingular elliptic curve E, instead of the full endomorphism ring $\mathrm{End}(E)$, we consider the subring $\mathrm{End}_p(E)$ consisting of $\mathbb{F}_p$-endomorphisms, which is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field $\mathbb{Q}(\sqrt{t^2 - 4p})$ where $|t| \leq 2\sqrt{p}$ denotes the Frobenius trace. Conversely, for a given order $\mathcal{O}$ in the imaginary quadratic field and an element $\pi \in \mathcal{O}$, we set $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ to be the set of supersingular elliptic curves E defined over $\mathbb{F}_p$ such that there is an isomorphism $\mathrm{End}_p(E) \to \mathcal{O}$ whose image of the Frobenius map is the element $\pi \in \mathcal{O}$. When we work in this setting, by abusing the notation, we denoted the endomorphism corresponding to $\alpha \in \mathcal{O}$ by α. Let E be an element in $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$. Then the ideal class group $cl(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ as follows: Let I be an integral ideal in $\mathcal{O}$. We define the I-torsion subgroup $E[I] := \{P \in E(\overline{\mathbb{F}}_p) \mid \alpha(P) = \infty \text{ for all } \alpha \in I\}$. Since the subgroup $E[I]$ is finite, this induces an isogeny $\phi_I : E \to E/E[I]$ with $\mathrm{Ker}\phi_I = E[I]$. So we define an action of $[I] \in cl(\mathcal{O})$ on E as $[I] * E = E/E[I]$, where $[I]$ denotes the ideal class represented by an integral ideal $I \subset \mathcal{O}$. Then we have the following theorem whose proof can be found in [31].

Theorem 3.4. *Let $\mathcal{O}$ be an order in an imaginary quadratic field and $\pi \in \mathcal{O}$ such that $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$ is non-empty. Then the ideal class group $cl(\mathcal{O})$ acts on $\mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$*

simply transitively by;

$$cl(\mathcal{O}) \times \mathcal{E}\ell\ell_p(\mathcal{O},\pi) \to \mathcal{E}\ell\ell_p(\mathcal{O},\pi);\ ([I],E) \mapsto E/E[I],$$

in which we choose I as an integral representative.

Here, we explain how to compute the above group action efficiently. In CSIDH, we work over the following setting. Let $\ell_1,\dots,\ell_n$ be distinct small odd primes such that $p = 4\ell_1\cdots\ell_n - 1$ is a prime. Fix the elliptic curve E_0 defined by the equation $y^2 = x^3 + x$ over $\mathbb{F}_p$, which is supersingular since $p \equiv 3 \pmod 4$. Let $\pi = \sqrt{-p}$ and set $\mathcal{O} = \mathbb{Z}[\pi]$. Then we have $E_0 \in \mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ by Proposition 3.5 below. Because of $\pi^2 - 1 \equiv 0 \pmod{\ell_i}$, the primes ℓ_i split in $\mathcal{O}$ as $\ell_i\mathcal{O} = I_i \cdot \overline{I}_i$, where $I_i = (\ell_i, \pi - 1)$ and $\overline{I}_i = (\ell_i, \pi + 1)$.

By the form of I_i and $\overline{I}_i$, we describe the torsion subgroups of the ideals I_i and $\overline{I}_i$ as follows;

$$\begin{aligned} E[I_i] &= E[\ell_i] \cap E(\mathbb{F}_p) \\ E[\overline{I}_i] &= E[\ell_i] \cap \{P \in E(\overline{\mathbb{F}}_p) \mid \pi(P) = -P\}. \end{aligned}$$

This shows that a point of order ℓ_i defined over $\mathbb{F}_p$ induces an isogeny $\phi_{I_i} : E \to I_i * E$. On the other hand, a point of order ℓ_i defined over $\mathbb{F}_{p^2}$ but not $\mathbb{F}_p$ induces an isogeny $\phi_{\overline{I}_i} : E \to \overline{I}_i * E$. Note that these isogenies are defined over $\mathbb{F}_p$. Since we can easily generate such torsion points, the action of I_i and $\overline{I}_i$ on $\mathcal{E}\ell\ell_p(\mathcal{O},\pi)$ can be efficiently computed. In fact, for a supersingular curve E defined by $y^2 = x^3 + ax^2 + x$, we can generate an ℓ_i-torsion point over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$ easily. For randomly picked $x_0 \in \mathbb{F}_p$, the point $P = (x_0, \sqrt{x_0^3 + ax_0^2 + x_0})$ on E is defined over $\mathbb{F}_p$ (resp. over $\mathbb{F}_{p^2}$) if $x_0^3 + ax_0^2 + x_0$ is quadratic residue in $\mathbb{F}_p$ (resp. quadratic non-residue in $\mathbb{F}_p$). Since the order of E is $p + 1 = 4\ell_1\cdots\ell_n$, the scalar multiplication of P by $\frac{p+1}{\ell}$ defines a point of order ℓ_i over $\mathbb{F}_p$ or $\mathbb{F}_{p^2}$.

Next, we want to know the structure of $cl(\mathcal{O})$ completely in order to sample elements uniformly at random. However, in general, it is difficult to compute the structure of the ideal class group of an order with large discriminant of cryptographic size. So we have to make use of heuristic discussions, see [2] for details.

Let m be an integer such that $2m+1 \geq \sqrt[n]{\#cl(\mathcal{O})}$. Under some heuristics, we have a surjection heuristically;

$$[-m,m]^n \to cl(\mathcal{O});\ (e_1,\dots,e_n) \mapsto I_1^{e_1}\cdots I_n^{e_n},$$

where $[-m,m]^n = \{(e_1,\dots,e_n) \mid e_i \in \mathbb{Z},\ -m \leq e_i \leq m \text{ for any } i\}$. This heuristic shows that if we want to sample an element from $cl(\mathcal{O})$ uniformly at random, it suffices that we choose a vector of integers from $[-m,m]^n$ uniformly at random. Therefore, we

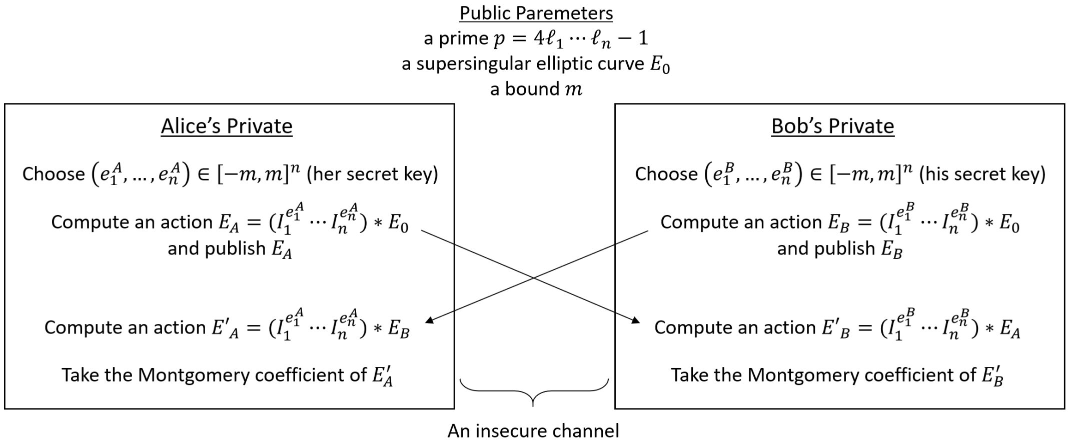
Public Paremeters
a prime $p = 4\ell_1 \cdots \ell_n - 1$
a supersingular elliptic curve E_0
a bound m
Alice's Private
Choose $(e_1^A, \ldots, e_n^A) \in [-m, m]^n$ (her secret key)
Compute an action $E_A = (l_1^{e_1^A} \cdots l_n^{e_n^A}) * E_0$ and publish E_A
Compute an action $E'_A = (l_1^{e_1^A} \cdots l_n^{e_n^A}) * E_B$
Take the Montgomery coefficient of E'_A
Bob's Private
Choose $(e_1^B, \ldots, e_n^B) \in [-m, m]^n$ (his secret key)
Compute an action $E_B = (l_1^{e_1^B} \cdots l_n^{e_n^B}) * E_0$ and publish E_B
Compute an action $E'_B = (l_1^{e_1^B} \cdots l_n^{e_n^B}) * E_A$
Take the Montgomery coefficient of E'_B
An insecure channel

Figure 3. Illustration of the CSIDH key-exchange protocol

can compute an action of any $I \in cl(\mathcal{O})$ by computing the actions of I_i or $\overline{I}_i$ one by one that can be computed efficiently.

Since all supersingular elliptic curves are defined over $\mathbb{F}_{p^2}$ and SIDH works over $\mathbb{F}_{p^2}$, we can use j-invariants as a shared value in the key exchange in order to ensure the correctness of the SIDH protocol. However, j-invariants are not $\mathbb{F}_p$-isomorphic invariant, hence sharing the j-invariants of the resulting curves in protocol does not imply the correctness of the CSIDH protocol. We note that the resulting curve is not necessarily defined over $\mathbb{F}_p$. The following proposition solves this problem and allows us to use Montgomery coefficients as a shared value in the CSIDH setting.

Proposition 3.5 (Proposition 8 in [2])**.** *Let $p \geq 5$ be a prime such that $p \equiv 3 \pmod 8$. Let E be a supersingular elliptic curve over $\mathbb{F}_p$. Then we have $\mathrm{End}_p(E) = \mathbb{Z}[\pi]$ if and only if there is $A \in \mathbb{F}_p$ such that E is isomorphic over $\mathbb{F}_p$ to the curve $E_A : y^2 = x^3 + Ax^2 + x$. Moreover, if such an A exists then it is unique.*

Therefore, the correctness of the CSIDH protocol follows from the above proposition and the commutativity of ideal class groups. Summarizing the above discussion, we can describe the CSIDH key-exchange protocol as in Fig. 3.

The hardness assumption supporting the security of CSIDH is the difficulty of inverting class group actions on supersingular curves.

Problem 3.6 (Ideal Class Group Action Invert Problem)**.** *Given a supersingular curve $E \in \mathcal{E}\ell\ell_p(\mathcal{O}, \pi)$, find an ideal $I \subset \mathcal{O}$ such that $E = I * E_0$.*

Remark. There is a sub-exponential attack to the above problem unlike SIDH. Childs, Jao and Soukharev [5] attempted to solve the problem of recovering I from a pair $(E_0, E_I = I * E_0)$ in a quantum setting. They reduced the problem to the abelian hidden-shift problem on an ideal class group. Before that, in 2004 and 2005, Kuperberg [20] and Regev [15] proposed quantum algorithms independently which could solve this problem in sub-exponential time.

§ 4. Cycles in Isogeny Graphs used in SIKE

We investigated the existence of cycles in isogeny graphs used in SIKE. This section is a résumé of this result in [24]. Throughout this section, we use the same notation as in §3.1. In [24], we discussed the following two questions. We consider the setting that Alice computes the public curve E_A from the initial curve E_0 using her secret isogeny ϕ_A.

- Question 1: Is there an isogeny from E_0 to the public curve E_A whose degree is smaller than the degree of her secret isogeny ϕ_A?
- Question 2: Is there isogeny to the public curve E_A distinct from ϕ_A which has the same degree as ϕ_A?

We gave answers of the above questions for SIKE parameters, SIKEp434 and SIKEp503 by combining a theoretical technique for finding cycles in isogeny graphs with numerical experiments.

§ 4.1. Setting on SIKE

SIKE [16] is a key encapsulation mechanism based on SIDH. This scheme is a 3rd Round alternative candidate in NIST's PQC competition [1]. In SIKE, we set $\ell_A = 2$, $\ell_B = 3$ and use the curve E_6 which is defined by the equation $y^2 = x^3 + 6x^2 + x$ as the initial curve. The curve E_6 is 2-isogenous to the curve E_0 which is difined by the equation $y^2 = x^3 + x$. The reason for using E_6 as the initial curve instead of E_0 is that the neighborhood of E_0 in the 2-isogeny graph $\mathcal{G}_2(p)$ has a special structure. In fact, elliptic curves which are 2-isogenous to E_0 are E_0 itself and E_6. Since the first step from E_0 is to E_6, use of E_0 as the initial curve slightly reduces the security of SIKE. So we use E_6 as the initial curve and do not use the 2-isogeny from E_6 to E_0. We define a SIKE path to be a path from E_6 in $\mathcal{G}_\ell(p)$ whose first step is not the one prohibited.

§ 4.2. Results

In order to answer two questions at the beginning of this section, we attempt to find two distinct paths from the initial curve without backtrackings having the same terminal. Finding such paths was studied in [13] in the context of finding a collision in the CGL hash function [3]. Their method is based on the fact that such paths correspond to cycles in $\mathcal{G}_\ell(p)$ and this cycle defines a non-integer endomorphism of the initial curve. We applied their method to the SIKE setting and proved the following theorem.

Theorem 4.1. *Let ℓ be a prime number that does not split in $\mathbb{Z}[\sqrt{-1}]$. Let ϕ and ψ are distinct s-step and t-step paths respectively from E_6 to E in $\mathcal{G}_\ell(p)$ without backtracking. Then we have one of the following:*

1. $\ell^{s+t} \geq \frac{p+1}{16}$
2. $\ell = 2$ *and either ϕ or ψ is not a SIKE path.*

Proof. We give a sketch of proof here, see [24] for details. We write isogenies ϕ and ψ as sequences of ℓ-isogenies: $\phi = (\phi_1, \ldots, \phi_s)$ and $\psi = (\psi_1, \ldots, \psi_t)$.

Firstly, we can show that there exist s' $(1 \leq s' < s)$ and t' $(0 \leq t' < t)$ such that $\alpha = \hat{\psi}_0 \circ \cdots \circ \hat{\psi}_{t'} \circ \phi_{s'} \circ \cdots \circ \psi_1$ is in $\mathrm{End}(E_6) \setminus \ell\mathrm{End}(E_6)$, where ψ_0 is the identity map on E_6 and $\hat{\psi}_i$ denotes the dual isogeny of ψ_i.

Secondly, we compute the structure of $\mathrm{End}(E_6)$;

$$\mathrm{End}(E_6) \simeq \mathbb{Z} + \mathbb{Z}(2\mathbf{i}) + \mathbb{Z}\frac{1+\mathbf{j}}{2} + \mathbb{Z}\frac{\mathbf{i}+\mathbf{k}}{4}$$

where $\mathbf{i^2} = -1,\ \mathbf{j^2} = -\mathrm{p},\ \mathbf{k} = \mathbf{ij} = \mathbf{ji}$. Then we can write $\alpha = a + 2b\mathbf{i} + c\frac{1+\mathbf{j}}{2} + d\frac{\mathbf{i}+\mathbf{k}}{4}$ for some $a, b, c, d \in \mathbb{Z}$ such that at least one of them is not divisible by ℓ.

Finally, we consider the norm equation;

$$\begin{aligned} \deg(\alpha) &= \mathrm{Nrd}(a + 2b\mathbf{i} + c\frac{1+\mathbf{j}}{2} + d\frac{\mathbf{i}+\mathbf{k}}{4}) \\ &= \frac{1}{16}((4a+2c)^2 + (8b+d)^2 + (4c^2+d^2)p). \end{aligned} \tag{4.1}$$

If either c or d is non-zero integer, the we have $\ell^{s+t} \geq \deg(\alpha) \geq \frac{p+1}{16}$. In the case $\ell \neq 2$, we have $\alpha \notin \mathbb{Z}+\mathbb{Z}(2\mathbf{i})$ since ℓ remains prime in $\mathbb{Z}+\mathbb{Z}(2\mathbf{i})$. We therefore obtain $\ell^{s+t} \geq \deg(\alpha) \geq \frac{p+1}{16}$. The case $\ell = 2$ and $c = d = 0$ is omitted. □

Let us apply this theorem to the existence of cycles in SIKE setting. Then we have $\ell_A^{e_A} \approx \ell_B^{e_B} \approx \sqrt{p}$. So the lower bound we gave in the above theorem is slightly short to claim that there are no distinct paths to the same target in SIKE. Our task is to check the existence of $\alpha \in \mathrm{End}(E_6) \setminus \mathbb{Z} + \mathbb{Z}2\mathbf{i}$ and $n \in \mathbb{Z}$ such that

$$\begin{gathered} \deg(\alpha) = \ell^n, \\ \frac{p+1}{16} < \ell^n \leq \ell^{2e} \end{gathered}$$

for $(\ell, e) = (2, e_A),\ (3, e_B)$. So we consider a equation

$$\ell^n = \frac{1}{16}((4a+2c)^2 + (8b+d)^2 + (4c^2+d^2)p) \tag{4.2}$$

from the equation (4.1) and try to find solutions with $a, b \in \mathbb{Z}$ and $(c, d) \in \mathbb{Z}^2 \backslash \{(0,0)\}$ for the SIKE parameters. Here, we consider the following equation instead of the equation (4.2) as it is;

$$16\ell^n - (4c^2+d^2)p = A^2 + B^2 \tag{4.3}$$

where $A = 4a + 2c$ and $B = 8b + d$. In order to find solutions of (4.2), we solve the equation (4.3) for all possible $n, c, d \in \mathbb{Z}$.

Case: SIKEp434

SIKEp434 uses $e_A = 216$, $e_B = 137$ and then $p = 2^{216}3^{137} - 1$. So we obtain values n satisfying the equation (4.2); $n = 2e_A - 2,\ 2e_A - 1\ ,2e_A$ for $\ell = 2$, and $n = 2e_B - 3,\ 2e_B - 2,\ 2e_B - 1,\ 2e_A$ for $\ell = 3$. We set; $D = \{2^{2e_A-2}, 2^{2e_A-1}, 2^{2e_A}, 3^{2e_B-3}, 3^{2e_B-2}, 3^{2e_B-1}, 3^{2e_B}\}$. This restricts possible values of c and d as $|c| \leq 3$ and $|d| \leq 5$ since $16\delta - (4c^2 + d^2)p$ is negative for all $\delta \in D$. Therefor, it is suffices to discuss the all equations (4.3) for such n, c, d.

Our computation showed that the solutions of the equations (4.3) for n, c, d above exist in the case $\ell = 3,\ n = 2e_B,\ |c| = 1,\ |d| = 5$ only. More precisely, there are eight solutions depending on the sign of c, d and A. One can find concrete solutions of the equations (4.3) in [24]. We conclude that, for SIKEp434, the answer of Question 1 is “no” and that of Question 2 is “Yes”, in fact there are two curves which have two distinct paths from the initial curve E_6. One can also find the j-invariants of these curves in [24].

Case: SIKEp503

SIKEp503 uses $e_A = 250$, $e_B = 159$ and then $p = 2^{250}3^{159} - 1$. We discuss solutions of the equation (4.3) in a similar way for SIKEp434. Our computation showed that no solution exists in this case. We therefore conclude that the answers of Question 1 and Question 2 mentioned earlier for SIKEp503 are both “no”.

Remark. SIKE has other two parameters, SIKEp610 and SIKEp751. In our computation as above, we require factorization for integers as large as the characteristic p of the base field in order to solve the equation (4.3) by using the Cornacchia-Smith algorithm [25, Algorithm 2.3.12]. However, our computational resource could not complete the factorizations for such large integers.

§ 5. Summary

In this paper we gave an introduction to isogeny-based cryptography, which is one of the candidates for post-quantum cryptography. Its security is based on the difficulty of computing an isogeny between two given elliptic curves and no classical and quantum algorithm which solves this problem efficiently is known so far.

In this research area, there are two standard Diffie-Hellman style key exchange protocols, SIDH by Jao and De Feo and CSIDH by Castryck et al. We have reviewed the construction of these schemes and mathematical tools which are necessary to construct them. SIDH is modeled as random walks in supersingular isogeny graphs of a low degree, typically 2 or 3. On the other hand, CSIDH is the first practical instantiation of HHS using the CM action on supersingular elliptic curves.

In the last section, we gave a résumé about our result of the existence of cycles in the isogeny graphs used in SIKE. We proved that there is no path to a public key whose length is shorter than a certain bound. By applying this result, we discussed the existence of cycles in isogeny graphs for SIKE parameters SIKEp434 and SIKEp503.

References

[1] National Institute of Standards and Technology (NIST) "NIST Post-Quantum Cryptography Standardization", https://csrc.nist.gov/projects/post-quantum-cryptography

[2] Castryck W., Lange T., Martindale C., Panny L., Renes J. (2018) CSIDH: An Efficient Post-Quantum Commutative Group Action. In: Peyrin T., Galbraith S. (eds) Advances in Cryptology – ASIACRYPT 2018. ASIACRYPT 2018. Lecture Notes in Computer Science, vol 11274. Springer, Cham. https://doi.org/10.1007/978-3-030-03332-3_15

[3] Charles, D.X., Lauter, K.E., Goren, E.Z., Cryptographic Hash Functions from Expander Graphs. J Cryptol 22, 93–113 (2009). https://doi.org/10.1007/s00145-007-9002-x

[4] Cohen, Henri and Frey, Gerhard and Avanzi, Roberto and Doche, Christophe and Lange, Tanja and Nguyen, Kim and Vercauteren, Frederik, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Second Edition, Chapman & Hall/CRC, 2nd, 2012.

[5] Andrew M. Childs, David Jao, and Vladimir Soukharev. Constructing elliptic curve isogenies in quantum subexponential time. *J. Math. Cryptol.*, 8(1):1–29, 2014.

[6] Costello C., Hisil H. (2017) A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies. In: Takagi T., Peyrin T. (eds) Advances in Cryptology – ASIACRYPT 2017. ASIACRYPT 2017. Lecture Notes in Computer Science, vol 10625. Springer, Cham.

[7] Costello, C., Smith, B. Montgomery curves and their arithmetic. J Cryptogr Eng 8, 227–240 (2018). https://doi.org/10.1007/s13389-017-0157-6

[8] J-M. Couveignes. Hard Homogeneous Spaces. IACR Cryptography ePrint Archive 2006/291. https://eprint.iacr.org/2006/291

[9] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 14 (1941), 197–272.

[10] W. Diffie, M. E. Hellman, New Directions in Cryptography. IEEE Transactions on Information Theory, vol.IT-22, No.6, pp.644-654, Nov, 1976.

[11] L. De Feo, D. Jao and J. Plût. Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *Journal of Mathematical Cryptology*, 8(3):209-247, 2014.

[12] De Feo L., Kieffer J., Smith B. (2018) Towards Practical Key Exchange from Ordinary Isogeny Graphs. In: Peyrin T., Galbraith S. (eds) Advances in Cryptology – ASIACRYPT 2018. ASIACRYPT 2018. Lecture Notes in Computer Science, vol 11274. Springer, Cham. https://doi.org/10.1007/978-3-030-03332-3_14

[13] Eisenträger K., Hallgren S., Lauter K., Morrison T., Petit C. (2018) Supersingular Isogeny Graphs and Endomorphism Rings: Reductions and Solutions. In: Nielsen J., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2018. EUROCRYPT 2018. Lecture Notes in Computer Science, vol 10822. Springer, Cham. https://doi.org/10.1007/978-3-319-78372-7_11

[14] S. D. Galbraith, Mathematics of Public Key Cryptography. Cambridge University Press, 2012.

[15] Oded Regev. A subexponential time algorithm for the dihedral hidden subgroup problem with polynomial space, arXiv, June 2004. URL: `https://arxiv.org/abs/quant-ph/0406151`.

[16] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. De Feo, B. Hess, A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, G. Pereira, J. Renes, V. Soukharev, and D. Urbanik. SIKE-Supersingular Isogeny Key Encapsulation, Submission to the NIST Post-Quantum Cryptography Standardization project; `https://sike.org`.

[17] Jao D., De Feo L. (2011) Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies. In: Yang BY. (eds) Post-Quantum Cryptography. PQCrypto 2011. Lecture Notes in Computer Science, vol 7071. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-25405-5_2

[18] J. Katz, Y.Lindell. Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series), Chapman and Hall/CRC, second edition, 2014.

[19] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48:203-209, 1987.

[20] Greg Kuperberg. A subexponential-time quantum algorithm for the dihedral hidden subgroup problem. *SIAM J. Comput.*, 35(1):170–188, 2005.

[21] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math.* (2) 126 (1987), no. 3, 649-673.

[22] Miller V.S. (1986) Use of Elliptic Curves in Cryptography. In: Williams H.C. (eds) Advances in Cryptology — CRYPTO '85 Proceedings. CRYPTO 1985. Lecture Notes in Computer Science, vol 218. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-39799-X_31

[23] P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of computation*, 48(177):243-264, 1987.

[24] H. Onuki, Y. Aikawa, T. Takagi. The Existence of Cycles in the Supersingular Isogeny Graphs Used in SIKE, In *ISITA 2020*. IEEE Xplore, 2020.

[25] R.C.C. Pomerance, R. Crandall and C. Pomerance. Prime Numbers: A Computational Perspective. Lecture notes in statics. Springer, 2005.

[26] A. Rostovtsev, A. Stolbunov. Public0key cryptosystem based on isogenies, 2006. IACR Cryptography ePrint Archive 2006/145. `https://eprint.iacr.org/2006/145`

[27] P. W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer *SIAM J. Comput.*, 26(5), 1484–1509, 1997.

[28] J. H. Silverman, The arithmetic of elliptic curves. Graduate Texts in Mathematics. Springer, 2nd edition, 2009.

[29] J. Vélu. Isogénies entre courbes elliptiques. *Comptes Rendus de l'Académie des Sciences de Paris*, 273:238-241, 1971.

[30] L. C. Washington, Elliptic Curves. Number Theory and Cryptography. Second Edition. Discrete Mathematics ans its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2008.

[31] W. C. Waterhouse, Abelian varieties over finite fields. *Annals scientifique de l'École Normale Supérieure*, 2:521-560, 1969.