Supersingular Isogeny Graphs and the Discrete Log Analogy

Hyungrok Jo

Institute of Advanced Sciences, Yokohama National University,
79-5 Tokiwadai, Hodogaya, Yokohama, Kanagawa, Japan
jo-hyungrok-xz@ynu.ac.jp

Abstract

This article is a survey report based on the author's presentation at the RIMS workshop *Research on Finite Groups, Algebraic Combinatorics, and Vertex Algebras* in 2025. The rapid development of quantum computing threatens classical public-key cryptosystems based on integer factorization and the discrete logarithm problem. This motivates the study of post-quantum cryptography, where new hardness assumptions are required. Among several post-quantum approaches, isogeny-based cryptography provides a mathematically rich framework built from elliptic curves, isogenies, and arithmetic group actions.

In this article, we survey supersingular isogeny graphs and explain how group actions on supersingular elliptic curves give rise to a natural analogy with the classical discrete logarithm problem. We begin with the discrete logarithm problem and its cryptographic applications such as Diffie–Hellman key exchange and ElGamal encryption, then discuss the quantum threat and the emergence of post-quantum cryptography. After reviewing elliptic curves, isogenies, and isogeny graphs, we introduce the framework of hard homogeneous spaces and its realization in CSIDH. From this perspective, the action of an ideal class group on a suitable family of supersingular elliptic curves may be viewed as a conceptual replacement for exponentiation in finite cyclic groups.

We further describe cryptographic applications built on this viewpoint, including ElGamal-type encryption and proxy re-encryption. The goal of this report is to present a coherent mathematical and cryptographic picture of the discrete-log-style analogy arising from supersingular isogeny graphs and to clarify its role in the design of post-quantum public-key primitives.

1 Introduction

The present article is a survey report based on the author's talk delivered at the RIMS workshop *Research on Finite Groups, Algebraic Combinatorics, and Vertex Algebras*.

Public-key cryptography is one of the core technologies supporting secure digital communication. Classical systems such as RSA and elliptic-curve cryptography rely on the hardness of integer factorization and the discrete logarithm problem, respectively. However, Shor's algorithm [12] shows that both problems can be solved efficiently on a sufficiently large quantum computer. This makes it necessary to develop public-key cryptography secure against quantum attacks.

Post-quantum cryptography studies such replacements. Among the main directions are lattice-based, code-based, multivariate, and isogeny-based cryptography. The isogeny-based approach is especially attractive from a mathematical point of view, since it combines arithmetic geometry, algebraic number theory, and graph-theoretic structures.

The main object of this report is the supersingular isogeny graph and its cryptographic interpretation. In the classical setting, exponentiation

$$x \longmapsto g^x$$

in a finite cyclic group leads to the discrete logarithm problem. In the isogeny setting, the role of exponentiation is replaced by a group action on elliptic curves. This does not literally define a discrete logarithm problem in a cyclic group, but it provides a closely related one-way structure that plays an analogous cryptographic role.

The aim of this article is therefore twofold:

- to review the mathematical structures underlying supersingular isogeny-based cryptography, including supersingular isogeny graphs and hard homogeneous spaces, and
- to explain how the CSIDH framework realizes a discrete log analogy by means of ideal class group actions, together with cryptographic applications such as ElGamal-type encryption and proxy re-encryption.

2 The Discrete Logarithm Problem

We begin with the classical discrete logarithm problem.

Definition 2.1 (Discrete Logarithm Problem)**.** *Let G be a finite cyclic group generated by an element g. Given an element $h \in G$, the* discrete logarithm problem *(DLP) is to determine an integer x such that*

$$g^x = h,$$

if such an integer exists.

The map $x \mapsto g^x$ is easy to compute, while its inversion is believed to be hard in suitable groups. This asymmetry underlies many public-key constructions.

2.1 Diffie–Hellman key exchange

The Diffie–Hellman protocol [7] is based on the observation that exponentiation in a cyclic group can be combined in a symmetric way. Let $G = \langle g \rangle$ be a finite cyclic group. Alice chooses a secret integer a, Bob chooses a secret integer b, and they exchange the public values g^a and g^b. Each side then computes

$$(g^b)^a = g^{ab}, \qquad (g^a)^b = g^{ab}.$$

The resulting common value g^{ab} serves as a shared secret. The security of this protocol is related to the computational difficulty of deriving the shared secret from the public transcript, formalized by computational Diffie–Hellman type assumptions.

2.2 ElGamal encryption

The ElGamal encryption scheme [8] is another direct application of the same algebraic structure. Let $G = \langle g \rangle$ be a finite cyclic group and let the secret key be an exponent x. The public key is then $h = g^x$.

To encrypt a message m encoded in the group, one samples a fresh random r and forms the ciphertext

$$(c_1, c_2) = (g^r, m \cdot h^r).$$

Using the secret key x, decryption computes

$$c_2 / c_1^x = m \cdot h^r / (g^r)^x = m.$$

Here again the crucial feature is the availability of an easy forward map combined with a hard inverse problem.

Figure 1 illustrates the basic structure of the ElGamal encryption scheme.

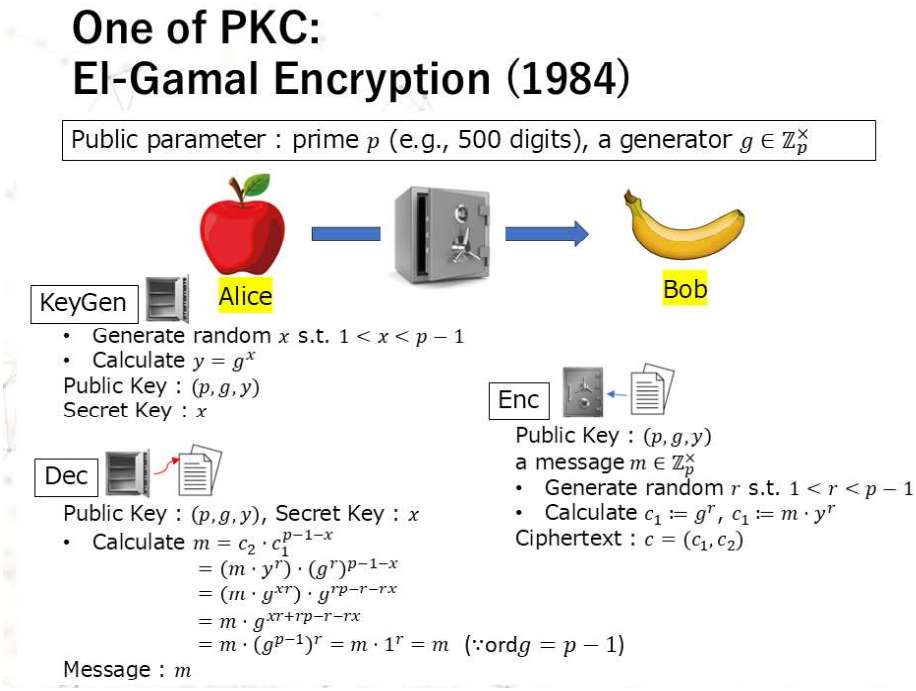

Figure 1: The ElGamal encryption scheme.

3 Quantum Threat and Post-Quantum Cryptography

Quantum computing changes the security assumptions underlying classical public-key cryptography. Shor's algorithm [12] implies that integer factorization and discrete logarithms can be solved in polynomial time on a quantum computer. Hence classical cryptosystems such as RSA, Diffie–Hellman, and elliptic-curve cryptography are not expected to remain secure in the long term.

This motivates the study of post-quantum cryptography, which aims to construct cryptographic systems secure against both classical and quantum adversaries. Current major families include:

- lattice-based cryptography,
- code-based cryptography,
- multivariate cryptography,
- isogeny-based cryptography.

Among these, isogeny-based cryptography stands out because of its compact keys and its strong connections with deep mathematical structures. It may be viewed as an attempt to retain the flavor of elliptic-curve cryptography while replacing the discrete logarithm problem by new computational assumptions involving elliptic curve isogenies.

4 Elliptic Curves and Isogenies

4.1 Elliptic curves over finite fields

Let k be a finite field. An elliptic curve E over k is a smooth projective curve of genus one together with a distinguished k-rational point. Over a field of characteristic different from 2 and

3, such a curve can be written in the affine form

$$E : y^2 = x^3 + ax + b$$

with discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. The set $E(k)$ of k-rational points forms a finite abelian group. Elliptic-curve cryptography is based on the scalar multiplication map

$$[n] : E \to E, \qquad P \mapsto nP.$$

The corresponding inverse problem is the elliptic-curve discrete logarithm problem.

4.2 Isogenies

Definition 4.1. *Let E_1 and E_2 be elliptic curves over a field k. An* isogeny $\varphi : E_1 \to E_2$ *is a non-constant morphism of algebraic groups.*

An isogeny is in particular a surjective homomorphism with finite kernel. Two elliptic curves are called *isogenous* if there exists an isogeny between them. For cryptographic purposes, it is important that if the kernel is known, then the isogeny can often be efficiently computed. This is made explicit by Vélu's formulas [14], which express the codomain and the rational map of an isogeny in terms of the finite subgroup defining its kernel.

4.3 One-way maps on elliptic curves

In the broadest sense, several natural maps on elliptic curves can be used as candidates for one-way functions:

- scalar multiplication, pairings, isogeny maps, or isogeny-induced group actions.

For scalar multiplication, the forward map is $P \mapsto [n]P$. For isogeny-based cryptography, the relevant forward map is not usually a single explicit isogeny of large degree, but rather a compactly represented composition of small-degree isogenies, or an action derived from such a composition.

5 Algorithms for Isogeny Problems

A central computational problem in isogeny-based cryptography is the following.

Definition 5.1 (Isogeny Problem)**.** *Given two isogenous elliptic curves E_1 and E_2, compute an isogeny $\varphi : E_1 \to E_2$, or at least a compact representation of such an isogeny.*

Here a compact representation often means a chain of small-degree isogenies, for example a sequence of ℓ-isogenies for small primes ℓ. The complexity of this problem depends strongly on whether the curves are ordinary or supersingular.

5.1 Ordinary case

For ordinary elliptic curves, the isogeny problem admits subexponential-time algorithms. This is closely related to the fact that the endomorphism ring is an order in an imaginary quadratic field, and ideal class group methods become available. The work of Childs, Jao, and Soukharev [4] also gives subexponential-time quantum algorithms in this setting.

5.2 Supersingular case

For supersingular elliptic curves, the structure is quite different. The endomorphism algebra is related to a quaternion algebra rather than an imaginary quadratic field, and the known attacks are of a different nature. This distinction is one of the reasons supersingular isogeny graphs became central objects in post-quantum cryptography. A useful graph-theoretic manifestation of this contrast is the following. In the ordinary case, the ℓ-isogeny graph has the structure of an ℓ-volcano, whose geometry is largely controlled by the endomorphism ring and its conductor. In the supersingular case, the corresponding graph is finite and highly connected, and is closely related to Hecke operators and Ramanujan-type expansion [11]. Thus the difference between ordinary and supersingular curves is reflected not only in algorithmic complexity but also in the global geometry of the associated isogeny graphs.

6 Supersingular and Ordinary Isogeny Graphs

To understand the graph-theoretic foundations of isogeny-based cryptography, it is useful to distinguish three related but different objects: ordinary ℓ-isogeny graphs, supersingular ℓ-isogeny graphs, and the restricted graph actually used in CSIDH. We survey each in turn, emphasizing the structural contrasts and their cryptographic relevance. We refer to [1, 9, 13].

6.1 Ordinary ℓ-isogeny graphs and volcanoes

Let p and ℓ be distinct primes, and let E be an ordinary elliptic curve over $\mathbb{F}_p$. Since $\ell \neq p$, one has

$$E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2,$$

so there are exactly $\ell + 1$ cyclic subgroups of order ℓ, each of which determines a separable ℓ-isogeny. Taking vertices to be ordinary elliptic curves over $\mathbb{F}_p$ up to isomorphism and edges to be ℓ-isogenies, one obtains the ordinary ℓ-isogeny graph.

A fundamental structural result is that each connected component of this graph has the structure of an *ℓ-volcano*. Roughly speaking, such a component consists of a distinguished cycle, called the *rim*, together with trees attached below it. Vertices are organized into levels according to their distance from the rim, and every non-rim vertex has a unique upward edge toward the rim [13]. This volcano structure plays an important role in the study of paths and random walks on ordinary isogeny graphs, but it is not the graph directly used by CSIDH.

6.2 Universal covering and tree structure

The graph-theoretic interpretation becomes clearer when one considers covering spaces. The universal covering of a connected k-regular graph is the k-regular infinite tree. Accordingly, the universal covering of an ordinary ℓ-isogeny volcano is the $(\ell + 1)$-regular tree. This viewpoint is useful for path counting and for the analysis of random walks, since paths on a volcano component may be lifted to paths on the regular tree. In particular, if one fixes a vertex v_0 and studies paths of length r, the corresponding counting problem can be interpreted in terms of repeated applications of the Hecke operator T_ℓ. Thus random walks on ordinary isogeny graphs naturally encode the action of Hecke correspondences on ordinary elliptic curves.

6.3 Supersingular ℓ-isogeny graphs

Fix distinct primes p and ℓ. In the standard supersingular setting, one considers supersingular elliptic curves over $\overline{\mathbb{F}}_p$, or equivalently supersingular j-invariants over $\mathbb{F}_{p^2}$, up to isomorphism,

with edges given by ℓ-isogenies.

Definition 6.1. *The* supersingular ℓ-isogeny graph $\Gamma_\ell(p)$ *has as its vertex set the supersingular elliptic curves over* $\overline{\mathbb{F}}_p$ *up to isomorphism, and as its edges the* ℓ*-isogenies between them, where in the undirected picture one identifies each isogeny with its dual.*

This graph is finite and highly connected. The number of supersingular j-invariants is

$$\left\lfloor \frac{p}{12} \right\rfloor + \varepsilon_p,$$

where $\varepsilon_p \in \{0, 1, 2\}$ is an explicit correction term depending on $p \bmod 12$. By contrast, the $\mathbb{F}_p$-rational subset relevant to CSIDH forms a more restrictive structure, which we discuss separately in Section 6.7.

Proposition 6.1. *Let* E *be a supersingular elliptic curve over a field of characteristic* p*, and let* $\ell \neq p$ *be prime. Then there are exactly* $\ell + 1$ *cyclic subgroups of* $E[\ell]$ *of order* ℓ*, and hence exactly* $\ell + 1$ *corresponding* ℓ*-isogenies from* E*.*

Sketch. Since $\ell \neq p$, the ℓ-torsion subgroup satisfies

$$E[\ell] \cong (\mathbb{Z}/\ell\mathbb{Z})^2.$$

Thus $E[\ell]$ is a two-dimensional vector space over $\mathbb{F}_\ell$. Cyclic subgroups of order ℓ correspond exactly to one-dimensional subspaces of this vector space, and the number of such subspaces is

$$\frac{\ell^2 - 1}{\ell - 1} = \ell + 1.$$

Each cyclic subgroup of order ℓ determines an ℓ-isogeny via Vélu's formulas [14]. □

Accordingly, in the standard supersingular model, one obtains an $(\ell+1)$-regular graph, up to the usual conventions concerning dual edges and possible automorphism-related multiplicities. Its adjacency operator is closely related to the Hecke operator T_ℓ acting on suitable spaces of modular forms. This connection goes back to Eichler, Shimura, and Pizer, and is one of the reasons supersingular isogeny graphs exhibit Ramanujan-type expansion properties [11].

6.4 Ramanujan-type expansion and random walks

The Hecke-theoretic description implies strong expansion properties for supersingular isogeny graphs. Informally, this means that random walks on such graphs mix rapidly, which helps explain why these graphs are useful in cryptographic constructions such as the hash function of Charles, Goren, and Lauter [2].

In cryptographic constructions, one often works not with a single large-degree isogeny, but with a compactly represented composition of small-degree isogenies. For example, composing e successive ℓ-isogenies without trivial backtracking yields an isogeny of degree ℓ^e. This compact representation is both efficient in practice and naturally compatible with the random-walk viewpoint.

6.5 Level N structure

A useful refinement is obtained by equipping each vertex with full level N structure. For an integer N prime to ℓ, one associates to a vertex not only an elliptic curve E but also an isomorphism

$$\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{\sim} E[N].$$

Thus a vertex is represented by a pair (E, α). An ℓ-isogeny $f : E \to E'$ then induces an edge

$$(E, \alpha) \longrightarrow (E',\ f \circ \alpha).$$

This enriched graph keeps track not only of the curve itself but also of the transport of level structure along the isogeny, and is useful when studying finer connectivity properties and path problems.

6.6 Connected components with level structure

When full level N structure is added, the graph may split into several connected components. More precisely, if one fixes a supersingular elliptic curve E whose endomorphism ring is identified with a maximal order in a definite quaternion algebra, then the connectedness of two vertices (E, α) and (E, β) is controlled by the determinant of the transition map

$$\alpha^{-1} \circ \beta \ \in\ \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

By strong approximation, the set of connected components may be identified with

$$(\mathbb{Z}/N\mathbb{Z})^\times / \langle \ell \rangle.$$

This provides a concrete arithmetic invariant controlling the decomposition of supersingular isogeny graphs with level structure. From the cryptographic point of view, such refinements may be relevant when one wishes to enrich the state space or impose additional structure on the public objects arising from isogeny-based constructions.

6.7 The CSIDH graph: a restricted $\mathbb{F}_p$-rational picture

The graph actually used in CSIDH [5] is more restrictive than the full supersingular ℓ-isogeny graph. One fixes a prime of the form

$$p = 4\ell_1 \cdots \ell_n - 1$$

with small odd primes $\ell_1, \ldots, \ell_n$, and considers the set

$$X = \left\{ E_A : y^2 = x^3 + Ax^2 + x \text{ is supersingular over } \mathbb{F}_p,\ A \in \mathbb{F}_p \right\}.$$

The relevant transitions are given by certain $\mathbb{F}_p$-rational isogenies of degrees $\ell_1, \ldots, \ell_n$.

From an intuitive point of view, one may think of the CSIDH action as being generated by moves associated with these small primes. What is important cryptographically is that these moves combine compatibly and yield a commutative group action. Thus the CSIDH setting should be viewed not as the full supersingular isogeny graph, but rather as a structured $\mathbb{F}_p$-rational family on which an ideal class group acts efficiently.

7 Hard Homogeneous Spaces

The framework of hard homogeneous spaces (HHS) [6] gives an abstract model for group-action-based cryptography.

Definition 7.1. *A* hard homogeneous space *consists of:*

- *a finite commutative group G,*

- *a finite set X,*
- *an action $G \curvearrowright X$ that is free and transitive,*

such that the following tasks are efficient:

- *group operations in G,*
- *sampling nearly uniform elements of G,*
- *testing validity and equality of representations in X,*
- *evaluating the action $g \cdot x$ for $g \in G$ and $x \in X$.*

At the same time, inverting the action is assumed to be hard.

Definition 7.2. *An action of G on X is* free *if $g \cdot x = x \implies g = e$ for all $x \in X$. It is* transitive *if for any $x, y \in X$ there exists $g \in G$ such that $g \cdot x = y$. Equivalently, the action is free and transitive if for every pair $x, y \in X$ there exists a unique $g \in G$ such that $g \cdot x = y$.*

This framework can be seen as a conceptual generalization of the discrete logarithm setting. In the classical case, exponentiation in a cyclic group is essentially an action of the additive group of exponents. In the HHS framework, one works directly with a group action on a set of objects.

8 CSIDH and the Discrete Log Analogy

8.1 The CSIDH action

CSIDH, introduced by Castryck, Lange, Martindale, Panny, and Renes [5], is a commutative group-action-based key exchange protocol defined on a suitable set of $\mathbb{F}_p$-rational supersingular elliptic curves. Its algebraic structure is described in terms of an ideal class group $\mathrm{Cl}(\mathcal{O})$ of a suitable imaginary quadratic order $\mathcal{O}$, which acts on this set. If $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O})$ and E is a curve in the corresponding CSIDH set, we write the action as

$$\mathfrak{a} * E.$$

A secret key is represented by an ideal class, typically encoded through exponents of small prime ideals,

$$\mathfrak{a} = \prod_i \mathfrak{l}_i^{e_i}.$$

The public key is then the curve obtained by applying this action to a fixed base curve.

8.2 Analogy with exponentiation

The analogy with the discrete logarithm problem becomes visible when one compares the maps

$$x \mapsto g^x \qquad \text{and} \qquad \mathfrak{a} \mapsto \mathfrak{a} * E.$$

In the classical setting:

- the secret is an exponent x,
- the public image is g^x,

- inversion means recovering x from g^x.

In the CSIDH setting:

- the secret is an ideal class $\mathfrak{a}$,
- the public image is $\mathfrak{a} * E$,
- inversion means recovering the hidden action from its effect on a curve.

This is not literally a discrete logarithm problem in a cyclic group. Nevertheless, it plays the same cryptographic role: a compact secret parameter determines an efficiently computable public object, while recovering the hidden parameter from the public object is believed to be hard.

Remark 8.1. *One may view this as a* discrete log analogy *rather than a literal generalization. The underlying object is a group action on a set, rather than a power map in a cyclic group. Nevertheless, the analogy is strong enough to support counterparts of Diffie–Hellman and ElGamal-type constructions.*

A practically important difference is that, in CSIDH-style systems, the secret action is evaluated through a carefully scheduled composition of many small-prime isogeny steps, rather than through a single straight-line exponentiation. Hence the computation differs from the classical setting not only algebraically but also algorithmically: the order and balance of the small-degree isogeny steps can significantly influence efficiency and implementation behavior.

9 Cryptographic Applications

9.1 HHS-based Diffie–Hellman

The hard homogeneous space framework naturally gives rise to a Diffie–Hellman-type key exchange. Let $G \curvearrowright X$ be a hard homogeneous space and fix a public base point $x \in X$. Alice chooses $a \in G$, Bob chooses $b \in G$, and they publish $a \cdot x$ and $b \cdot x$. The shared secret is then

$$a \cdot (b \cdot x) = b \cdot (a \cdot x).$$

This is exactly the paradigm realized by CSIDH [5].

9.2 ElGamal-type encryption

The same principle leads to ElGamal-type public-key encryption schemes [8]. In the classical setting, ElGamal uses exponentiation and multiplicative masking. In the group-action setting, the role of exponentiation is played by the action of a random group element on the public base object.

A representative example is SiGamal [10]. At a high level, one has:

- a public key given by a curve obtained from a secret action,
- an ephemeral random action used during encryption,
- a ciphertext containing an ephemeral public component together with a masked message component.

The secret action allows decryption of the masked message. This construction demonstrates that the DLP analogy is strong enough to support not only key exchange but also public-key encryption.

9.3 Proxy re-encryption

Proxy re-encryption (PRE) is a public-key primitive that allows a semi-trusted proxy to transform a ciphertext encrypted for one recipient into a ciphertext for another recipient, without learning the underlying plaintext. This functionality is useful in delegated access control, encrypted e-mail forwarding, cloud storage, and secure data sharing. Formally, suppose that Alice encrypts a message for Bob under Bob's public key. A proxy re-encryption scheme provides a re-encryption key $\mathsf{rk}_{B\to C}$ that enables a proxy to convert Bob's ciphertext into one decryptable by Charlie, while the proxy itself should not recover the message. Depending on the directionality and composability of this transformation, one distinguishes between unidirectional/bidirectional and single-hop/multi-hop proxy re-encryption. From the viewpoint of group-action-based cryptography, PRE is particularly interesting because it requires some controlled composability of hidden actions. In a CSIDH-like setting, public keys are represented by curves obtained via ideal class group actions, and one may hope to encode the relation between two secret actions into a re-encryption key. At a conceptual level, if Bob's public key is $E_B = \mathfrak{b} * E_0$ and Charlie's public key is $E_C = \mathfrak{c} * E_0$, then a re-encryption key should capture a suitable relation between $\mathfrak{b}$ and $\mathfrak{c}$ without revealing either secret class itself. This idea is not entirely straightforward, since naive exposure of such a relation may leak key information. Therefore, the design of PRE in the isogeny setting must carefully balance correctness, transformability, and secrecy of the underlying group action. As one concrete example, recent work [3] has explored how such functionality can be realized by adapting hashed ElGamal-type constructions over CSIDH and by exploiting divisible or composable action structures. In particular, bidirectional proxy re-encryption schemes have been proposed in the isogeny setting, showing that the discrete-log-style group-action viewpoint can support more advanced functionalities beyond key exchange. These examples suggest that the discrete-log-style group-action viewpoint may extend beyond key exchange to more advanced delegation-oriented primitives in the post-quantum setting.

9.4 Perspective toward advanced cryptography

The applications above suggest that supersingular isogeny graphs may support a broader family of advanced public-key primitives. Possible future directions include:

- identity-based encryption, identity-based signatures, broadcast encryption, aggregate signatures, and more general re-encryption and delegation mechanisms.

The main challenge is to retain the structural elegance of the group action while obtaining sufficiently strong and well-understood security notions.

10 Comparison with Classical DLP-Based Cryptography

It is instructive to compare the classical DLP setting and the isogeny-based group-action setting.

	Classical DLP	CSIDH / group action analogy
Secret object	exponent x	ideal class $\mathfrak{a}$
Public image	g^x	$\mathfrak{a} * E$
Underlying structure	cyclic group	set with a free transitive action
Forward map	exponentiation	action evaluation
Inverse problem	recover x	recover hidden action
Quantum attacks	polynomial-time via Shor	subexponential quantum algorithms known [4]

This comparison clarifies why the phrase "discrete log analogy" is useful. It emphasizes the continuity of cryptographic design ideas while acknowledging the essential mathematical differences.

11 Conclusion

In this report, we reviewed the discrete logarithm problem and its role in classical public-key cryptography, described the quantum threat that motivates post-quantum cryptography, and surveyed the mathematical foundations of isogeny-based cryptography. We then focused on supersingular isogeny graphs and explained how group actions on supersingular elliptic curves yield a natural analogue of the classical discrete logarithm problem. Through the framework of hard homogeneous spaces and its concrete realization in CSIDH, one obtains a replacement for exponentiation that supports post-quantum analogues of classical public-key constructions. Finally, we outlined cryptographic applications of this viewpoint, including ElGamal-type encryption and proxy re-encryption. These examples show that supersingular isogeny graphs are not only mathematically rich objects, but also a promising foundation for post-quantum cryptographic design.

References

[1] S. Arpin, Adding level structure to supersingular elliptic curve isogeny graphs, *Journal de théorie des nombres de Bordeaux*, 36(2):405–443, 2024.

[2] D. X. Charles, E. Z. Goren and K. E. Lauter, Cryptographic hash functions from expander graphs, *Journal of Cryptology*, 22(1):93–113, 2009.

[3] J. Chen, H. Jo, S. Sato and J. Shikata, Bidirectional Proxy Re-encryption Based on Isogenies, In: H. Jo, S. Shin, A. Merlo, I. You (eds) *Mobile Internet Security. MobiSec 2024*, Communications in Computer and Information Science, vol. 2597, pp. 133–148, Springer, Singapore, 2026.

[4] A. M. Childs, D. Jao and V. Soukharev, Constructing elliptic curve isogenies in quantum subexponential time, *Journal of Mathematical Cryptology*, 8(1):1–29, 2014.

[5] W. Castryck, T. Lange, C. Martindale, L. Panny and J. Renes, CSIDH: An efficient post-quantum commutative group action, In *Advances in Cryptology – ASIACRYPT 2018*, Lecture Notes in Computer Science, vol. 11274, pp. 395–427, Springer, 2018.

[6] J.-M. Couveignes, Hard homogeneous spaces, Cryptology ePrint Archive, Report 2006/291, originally circulated in 1997.

[7] W. Diffie and M. E. Hellman, New directions in cryptography, *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[8] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[9] D. R. Kohel, Endomorphism rings of elliptic curves over finite fields, *Ph.D. Thesis, University of California, Berkeley*, 1996.

[10] T. Moriya, H. Onuki and T. Takagi, SiGamal: A supersingular isogeny-based PKE and its application to a PRF, In *Advances in Cryptology – ASIACRYPT 2020*, Lecture Notes in Computer Science, vol. 12492, pp. 551–580, Springer, 2020.

[11] A. K. Pizer, Ramanujan graphs and Hecke operators, *Bulletin of the American Mathematical Society (N.S.)*, 23(1):127–137, 1990.

[12] P. W. Shor, Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer, *SIAM Review*, 41(2):303–332, 1999.

[13] A. V. Sutherland, Isogeny volcanoes, In *ANTS X – Proceedings of the Tenth Algorithmic Number Theory Symposium*, Open Book Series, vol. 1, pp. 507–530, Mathematical Sciences Publishers, 2013.

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

Institute of Advanced Sciences
Yokohama National University
Yokohama, Japan
E-mail address: `jo-hyungrok-xz@ynu.ac.jp`