RIMS Kôkyûroku Bessatsu
B90 (2022), 117–129

OSIDH and SiGamal: cryptosystems from supersingular elliptic curves

By

Hiroshi Onuki*

Abstract

We introduce two cryptosystems, OSIDH and SiGamal, which use isogenies between supersingular elliptic curves over a finite field. And we consider computational problems on which these cryptosystems are based. In particular, we discuss a relation between these problems and problems to find the image of a point under a secret isogeny.

§ 1. Introduction

To find an isogeny between given two isogenous elliptic curves is considered to be a computationally hard problem. We call this an *isogeny problem*. Isogeny-based cryptography is based on the hardness of the isogeny problem. This is one of the candidates of post-quantum cryptography since the isogeny problem is considered to be hard even by using a quantum computer.

The first isogeny-based cryptosystem was proposed by Couveignes [6] in 1997. But his work was not published and posted on a preprint server in 2006. The same result was rediscovered by Rostovtsev and Stolbunov [16, 17]. Their cryptosystem uses isogenies between ordinary elliptic curves. On the other hand, Charles, Goren, and Lauter [4] proposed a cryptographic hash function using isogenies between supersingular elliptic curves. This is the first appearance of isogenies between supersingular elliptic curves in cryptography. Subsequently, several cryptosystems using isogenies between supersingular isogenies are proposed, e.g., SIDH by Jao and De Feo [11], CSIDH by Castryck,

Received December 31, 2020. Revised April 4, 2021.
2020 Mathematics Subject Classification(s): 11T71
Key Words: *Post-quantum cryptography, supersingular ellitptic curves, isogeny graphs.*
Supported by JST CREST Grant Number JPMJCR14D6, Japan.
*Department of Mathematical Informatics, The University of Tokyo, Tokyo 113-8656, Japan.
e-mail: onuki@mist.i.u-tokyo.ac.jp

Lange, Martindale, Panny, and Renes [3], SÉTA by Guilhem, Kutas, Petit, and Silva [10], OSIDH by Colò and Kohel [5], and SiGamal by Moriya, Onuki, and Takagi [13].

In this paper, we introduce the latter two cryptosystems, OSIDH and SiGamal, and discuss their security. In particular, we consider problems to find the image of a point under a secret isogeny and a relation between these problems and the two cryptosystems.

§ 2. OSIDH

OSIDH stands for Oriented Supersingular Isogeny Diffie-Hellman protocol. It is a key-exchange protocol using oriented supersingular isogenies and actions of the ideal class group of an imaginary quadratic order on these curves.

§ 2.1. Orientations

We recall definitions about orientations on elliptic curves. See [5, 14] for more details. Let K be an imaginary quadratic field and $\mathcal{O}$ an order of K. We fix an algebraic closure $\overline{\mathbb{F}}_p$ of a prime field $\mathbb{F}_p$ of characteristic p. For an isogeny φ, we denote the dual isogeny of φ by $\hat{\varphi}$.

Definition 2.1. Let E be an elliptic curve over $\overline{\mathbb{F}}_p$. A *K-orientation* on an elliptic curve E is a ring homomorphism

$$\iota : K \hookrightarrow \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

A K-orientation on E is an *$\mathcal{O}$-orientation* if $\iota(\mathcal{O}) \subseteq \mathrm{End}(E)$. An $\mathcal{O}$-orientation is *primitive* if $\iota(\mathcal{O}) = \mathrm{End}(E) \cap \iota(K)$. If ι is a K-orientation on E (resp. primitive $\mathcal{O}$-orientation), a pair (E, ι) is called a *K-oriented* (resp. *primitive $\mathcal{O}$-oriented*) *elliptic curve*.

We denote the j-invariant of a K-orientated elliptic curve (E, ι) by $j(E)$ or $j((E, \iota))$. Let $\varphi : E \to F$ be an isogeny of degree ℓ. We define a K-orientation $\varphi_*(\iota)$ on F by

$$\varphi_*(\iota)(\alpha) = \frac{1}{\ell}\varphi \circ \iota(\alpha) \circ \hat{\varphi} \quad \text{for } \alpha \in K.$$

Definition 2.2. Let (E, ι_E) and (F, ι_F) be K-oriented elliptic curves. An isogeny $\varphi : E \to F$ is *K-oriented* if $\varphi_*(\iota_E) = \iota_F$. We denote this by $\varphi : (E, \iota_E) \to (F, \iota_F)$. We say that φ is *K-isomorphism* if there exists a K-oriented isogeny $(F, \iota_F) \to (E, \iota_E)$ that is the inverse of φ. In this case, we say that (E, ι_E) and (F, ι_F) are *K-isomorphic* and write $(E, \iota_E) \cong (F, \iota_F)$.

Let (E, ι_E) be a primitive $\mathcal{O}$-oriented elliptic curve and $\varphi : (E, \iota_E) \to (F, \iota_F)$ a K-oriented isogeny. Define $\mathcal{O}' := \mathrm{End}(F) \cap \iota_F(K)$. We say that φ is *horizontal* if $\mathcal{O} = \mathcal{O}'$, *ascending* if $\mathcal{O} \subsetneq \mathcal{O}'$, and *descending* if $\mathcal{O} \supsetneq \mathcal{O}'$.

For a K-oriented elliptic curve (E, ι), we denote its Frobenius conjugate by $(E^{(p)}, \iota^{(p)})$. I.e., $E^{(p)}$ is the elliptic curve obtained from E by raising each coefficient of E to the p-th power, and $\iota^{(p)} = (\phi_p)_*(\iota)$, where ϕ_p is the p-Frobenius map: $E \to E^{(p)}$.

We denote the set of K-isomorphism classes of primitive $\mathcal{O}$-oriented supersingular elliptic curves by $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$. We write a class of $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$ by the same symbol as one of its representatives for brevity. $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$ is nonempty if and only if p does not split in K and does not divide the conductor of $\mathcal{O}$ (Proposition 3.2 in [14]). In this case, by CM (complex multiplication) theory, all classes in $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$ are obtained by reductions of elliptic curves over number fields. Let $\mathcal{Ell}(\mathcal{O})$ be the set of isomorphism classes of elliptic curves over number fields with CM by $\mathcal{O}$. Then there exists a reduction map

$$\rho : \mathcal{Ell}(\mathcal{O}) \to \mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p),$$

and this map is surjective up to the Frobenius conjugate. I.e., we have the following.

Proposition 2.3 (Proposition 3.3 in [14]). *For all $(E, \iota) \in \mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$, we have*

$$(E, \iota) \text{ or } (E^{(p)}, \iota^{(p)}) \in \rho(\mathcal{Ell}(\mathcal{O})).$$

§ 2.2. Group Actions

The ideal class group $\mathcal{Cl}(\mathcal{O})$ of $\mathcal{O}$ acts freely and transitively on $\rho(\mathcal{Ell}(\mathcal{O}))$ if $\mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p)$ is nonempty (Theorem 3.4 in [14]). The action is defined as follows. Let $(E, \iota) \in \rho(\mathcal{Ell}(\mathcal{O}))$ and $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$ coprime to p. The $\mathfrak{a}$-torsion subgroup $E[\mathfrak{a}]$ of (E, ι) is defined by

$$E[\mathfrak{a}] = \bigcap_{\alpha \in \mathfrak{a}} \ker \iota(\alpha).$$

Then there are an elliptic curve F and a separable isogeny $\varphi : E \to F$ with $\ker \varphi = E[\mathfrak{a}]$. We denote the class of $\mathfrak{a}$ by $[\mathfrak{a}]$. We define the action of $[\mathfrak{a}]$ on (E, ι) by $(F, \varphi_*(\iota))$ and write it as $[\mathfrak{a}] * (E, \iota)$. This correspondence defines an action of $\mathcal{Cl}(\mathcal{O})$ on $\rho(\mathcal{Ell}(\mathcal{O}))$ (Proposition 3.6 in [14]).

Colò and Kohel [5] proposed a method to calculate these group actions for some imaginary quadratic fields and these orders.

We assume the class number of K is one and denote the maximal order of K by $\mathcal{O}_K$. Let $\ell \neq p$ be a prime and define

$$\mathcal{O}_\ell^{(n)} \coloneqq \mathbb{Z} + \ell^n \mathcal{O}_K \text{ for } n \in \mathbb{Z}_{\geq 0}.$$

Then there exists a chain of descending K-oriented isogenies of degree ℓ:

$$(E_0, \iota_0) \xrightarrow{\varphi_0} (E_1, \iota_1) \xrightarrow{\varphi_1} (E_2, \iota_2) \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} (E_n, \iota_n),$$

where $(E_i, \iota_i) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_\ell^{(i)}))$ for $i = 0, 1, \ldots, n$. Let $q \neq \ell$ be a prime splitting in $K$and $\mathfrak{q}$ a prime ideal in $\mathcal{O}_K$ lying above q. For brevity, we use the same symbol $\mathfrak{q}$ for the prime ideals $\mathfrak{q} \cap \mathcal{O}_\ell^{(i)}$ for $i = 0, 1, \ldots, n$. Let $(F_i, \tau_i) = [\mathfrak{q}] * (E_i, \iota_i)$ and $\psi_i : (E_i, \iota_i) \to (F_i, \tau_i)$ be an isogeny corresponding to the action of $[\mathfrak{q}]$. Then there exists a descending K-oriented ℓ-isogeny $\varphi_i' : (F_i, \tau_i) \to (F_{i+1}, \tau_{i+1})$ with $\ker \varphi_i' = \psi_i(\ker \varphi_i)$. We obtain the following commutative diagram of K-oriented isogenies:

$$\begin{array}{ccccccccc}
(E_0, \iota_0) & \xrightarrow{\varphi_0} & (E_1, \iota_1) & \xrightarrow{\varphi_1} & (E_2, \iota_2) & \xrightarrow{\varphi_2} & \cdots & \xrightarrow{\varphi_{n-1}} & (E_n, \iota_n) \\
\downarrow{\scriptstyle \psi_0} & & \downarrow{\scriptstyle \psi_1} & & \downarrow{\scriptstyle \psi_2} & & & & \downarrow{\scriptstyle \psi_n} \\
(F_0, \tau_0) & \xrightarrow{\varphi_0'} & (F_1, \tau_1) & \xrightarrow{\varphi_1'} & (F_2, \tau_2) & \xrightarrow{\varphi_2'} & \cdots & \xrightarrow{\varphi_{n-1}'} & (F_n, \tau_n).
\end{array}$$

For an integer m, let $\Phi_m(X, Y) \in \mathbb{Z}[X, Y]$ be the m-th modular polynomial. Then $j(F_i)$ is a common root of $\Phi_q(X, j(E_i))$ and $\Phi_\ell(X, j(F_{i-1}))$ for $i \geq 1$. If $j(F_i)$ is the only one common root of these polynomials then we can obtain $j(F_i)$ from $j(E_i)$ and $j(F_{i-1})$ by computing the gcd. Since we assume the class number of K is one, we have $j(F_0) = j(E_0)$. Therefore, we can compute the sequence $(j(F_0), \ldots, j(F_n))$ from $(j(E_0), \ldots, j(E_n))$. In general, the assumption that a common root of the modular polynomials is unique does not hold (§6.1 in [14]). However, if we take a sufficiently large p, all common roots of the modular polynomials are the j-invariants of elliptic curves determined by the action of $\mathcal{C}\ell(\mathcal{O}_\ell^{(i)})$. More precisely, we have the following.

Theorem 2.4. *In the above setting, we denote the discriminant of K by D. If $p > q\ell^{2i}D$ then a common root of $\Phi_q(X, j(E_i))$ and $\Phi_\ell(X, j(F_{i-1}))$ is $j(F_i)$ or $j([\mathfrak{q}^{-1}] * (E_i, \iota_i))$. Furthermore, if $j(F_{i-1}) \neq j([\mathfrak{q}^{-1}] * (E_{i-1}, \iota_{i-1}))$ then the gcd of $\Phi_q(X, j(E_i))$ and $\Phi_\ell(X, j(F_{i-1}))$ has degree one, and its root is $j(F_i)$.*

Proof. See §5.1 and Theorem 6.2 in [14]. □

In addition, if p is larger than the bound in the above theorem then the j-invariants that appear in the diagram are distinct. I.e., the following theorem holds.

Theorem 2.5 (Theorem 6.3 in [14])**.** *We use the same notation as in Theorem 2.4, and assume that $p > \ell^{2n}D$. Let $n_1, n_2 \leq n$ nonnegative integers, $(E_1, \iota_1) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_\ell^{(n_1)}))$, and $(E_2, \iota_2) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_\ell^{(n_2)}))$. Then $j(E_1) = j(E_2)$ if and only if $(E_1, \iota_1) \cong (E_2, \iota_2)$.*

As in Theorem 2.4, we assume $p > q\ell^{2n}D$. We further assume that $\mathfrak{q} \neq \mathfrak{q}^{-1} \in \mathcal{C}\ell(\mathcal{O}_\ell^{(1)})$ for simplicity (see §5 in [5] for discussion on this assumption). The method to calculate the group action of $\mathfrak{q}$ on the sequence (E_i, ι_i) is as follows: We first determine the j-invariant of $[\mathfrak{q}] * (E_1, \iota_1)$ (e.g., by using Vélu's formula [18]), and calculate the

j-invariants of $[\mathfrak{q}] * (E_i, \iota_i)$ for $i \geq 2$ by the gcds of modular polynomials. Then we can calculate the j-invariants of $[\mathfrak{q}^2] * (E_i, \iota_i)$ by the gcds of modular polynomials since we know the j-invariant of $[\mathfrak{q}^{-1}][\mathfrak{q}] * (E_1, \iota_1) = (E_1, \iota_1)$. By repeating this method, we obtain the j-invariants of the sequence $[\mathfrak{q}^e] * (E_i, \iota_i)$ for $i = 0, \ldots, n$ and any integer e.

Let $q_1, q_2 \neq \ell$ be distinct primes splitting in K, and $\mathfrak{q}_1, \mathfrak{q}_2$ prime ideals in $\mathcal{O}_K$ above q_1, q_2, respectively. (As in the above, we use the same symbols for prime ideals in $\mathcal{O}_\ell^{(i)}$ corresponding to these ideals.) For integers e_1, e_2, the j-invariant of $[\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}] * (E_n, \iota_n)$ is a common root of $\Phi_{q_1}(X, j([\mathfrak{q}_1^{e_1-1}\mathfrak{q}_2^{e_2}] * (E_n, \iota_n)))$ and $\Phi_{q_2}(X, j([\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2-1}] * (E_n, \iota_n)))$. Furthermore, if $p > \max\{q_1, q_2\}\ell^{2n}D$ then $j([\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}] * (E_n, \iota_n))$ is only one common root of these polynomials. Therefore, we can compute $j([\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}] * (E_n, \iota_n))$ from sequences of the j-invariants of $[\mathfrak{q}_1] * (E_n, \iota_n), \ldots, [\mathfrak{q}_1^{e_1}] * (E_n, \iota_n)$ and $[\mathfrak{q}_2] * (E_n, \iota_n), \ldots, [\mathfrak{q}_2^{e_2}] * (E_n, \iota_n)$. The following diagram illustrates this method. In the diagram, horizontal arrows are isogenies corresponding to the actions of $\mathfrak{q}_1$, and vertical arrows are corresponding to those of $\mathfrak{q}_2$.

$$
\begin{array}{ccccccc}
(E_n, \iota_n) & \longrightarrow & [\mathfrak{q}_1] * (E_n, \iota_n) & \longrightarrow & [\mathfrak{q}_1^2] * (E_n, \iota_n) & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1^{e_1}] * (E_n, \iota_n) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
[\mathfrak{q}_2] * (E_n, \iota_n) & \longrightarrow & [\mathfrak{q}_1\mathfrak{q}_2] * (E_n, \iota_n) & \longrightarrow & [\mathfrak{q}_1^2\mathfrak{q}_2] * (E_n, \iota_n) & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1^{e_1}\mathfrak{q}_2] * (E_n, \iota_n) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\vdots & & \vdots & & \vdots & & \vdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
[\mathfrak{q}_2^{e_2}] * (E_n, \iota_n) & \longrightarrow & [\mathfrak{q}_1\mathfrak{q}_2^{e_2}] * (E_n, \iota_n) & \longrightarrow & [\mathfrak{q}_1^2\mathfrak{q}_2^{e_2}] * (E_n, \iota_n) & \longrightarrow \cdots \longrightarrow & [\mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}] * (E_n, \iota_n)
\end{array}
$$

§ 2.3. Protocol

The protocol of OSIDH is similar to that of CSIDH. A rough sketch of the protocol is as follows: We consider a key exchange between Alice and Bob. First, Alice and Bob publicly share a chain of descending isogenies $(E_0, \iota) \to \cdots \to (E_n, \iota_n)$, which is defined in §2.2. Next, Alice computes $j([\mathfrak{a}] * (E_n, \iota_n))$, and Bob computes $j([\mathfrak{b}] * (E_n, \iota_n))$, where $[\mathfrak{a}], [\mathfrak{b}] \in \mathcal{C}\ell(\mathcal{O}_\ell^{(n)})$ are secret keys. Then Alice sends $j([\mathfrak{a}] * (E_n, \iota_n))$ and some additional information that allows Bob to compute the ideal action on $[\mathfrak{a}] * (E_n, \iota_n)$, and Bob do the same for $j([\mathfrak{b}] * (E_n, \iota_n))$. Finally, they compute the actions of their secret keys on the received curves and share the j-invariants of $[\mathfrak{ab}] * (E_n, \iota_n)$ as their shared secret.

More precisely, the data used in the protocol are the below.

Public parameters:

- K: an imaginary quadratic field whose class number is one.
- (E_0, ι_0): a primitive $\mathcal{O}_K$-oriented supersingular elliptic curve.
- $\ell \neq p$: a prime number.

- The j-invariants of a chain of descending K-oriented isogenies of degree ℓ

$$(E_0, \iota_0) \xrightarrow{\varphi_0} (E_1, \iota_1) \xrightarrow{\varphi_1} (E_2, \iota_2) \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} (E_n, \iota_n).$$

- $q_1, \ldots, q_t$: prime numbers distinct from ℓ and splitting in K,
  and $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$: prime ideals of $\mathcal{O}_K$ (and $\mathcal{O}_\ell^{(i)}$ for $i = 1, \ldots, n$) above $q_1, \ldots, q_t$.
- The j-invariants of $[\mathfrak{q}_1]*(E_{i_1}, \iota_{i_1}), \ldots, [\mathfrak{q}_t]*(E_{i_t}, \iota_{i_t})$, where i_k is the smallest positive integer such that $\mathfrak{q}_k \neq \mathfrak{q}_k^{-1}$ in $\mathcal{O}_\ell^{(i_k)}$ for $k = 1, \ldots, t$.

Secret key: An integer vector in $[-B, B]^t$, where B is a positive integer.
Public key: The public key corresponding to a secret key $(e_1, \ldots, e_t)$ is a set of the j-invariants of the following curves:

- $[\prod_{k=1}^t \mathfrak{q}_k^{e_k}] * (E_n, \iota_n)$, we denote this curve by (F, τ),
- (F, τ), $[\mathfrak{q}_k] * (F, \tau)$, $[\mathfrak{q}_k^2] * (F, \tau)$, $\ldots$, $[\mathfrak{q}_k^B] * (F, \tau)$,
- (F, τ), $[\mathfrak{q}_k^{-1}] * (F, \tau)$, $[\mathfrak{q}_k^{-2}] * (F, \tau)$, $\ldots$, $[\mathfrak{q}_k^{-B}] * (F, \tau)$.

Note that the later two sequences in the public key allow to compute the action of $\prod_{k=1}^t \mathfrak{q}_k^{d_k}$ for any integer vector $(d_1, \ldots, d_t)$ in $[-B, B]^t$. We call these sequences *auxiliary sequences* of the oriented elliptic curve (F, τ).

§ 2.4. Security

The security of OSIDH depends on two problems, which we call *horizontal isogeny problem* and *descending isogeny problem*.

The horizontal isogeny problem is as follows. This requires to find a secret key in OSIDH from public information.

Problem 2.6 (horizontal isogeny problem)**.** Given an imaginary quadratic field K with class number one, a prime $\ell \neq p$, a positive integer n, a chain of descending K-oriented isogenies of degree ℓ

$$(E_0, \iota_0) \xrightarrow{\varphi_0} (E_1, \iota_1) \xrightarrow{\varphi_1} (E_2, \iota_2) \xrightarrow{\varphi_2} \cdots \xrightarrow{\varphi_{n-1}} (E_n, \iota_n),$$

where $(E_i, \iota_i) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_\ell^{(i)}))$ for $i = 0, \ldots, n$, an oriented curve $(F, \tau) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_\ell^{(n)}))$, and auxiliary sequences of (F, τ), find an ideal class $[\mathfrak{a}]$ such that $(F, \tau) = [\mathfrak{a}] * (E_n, \iota_n)$.

The descending isogeny problem requires to find a chain of descending isogenies from the public curve (E_0, ι_0) to a public key (F, τ).

Problem 2.7 (descending isogeny problem)**.** Given an imaginary quadratic field K with class number one, a prime $\ell \neq p$, a positive integer n, oriented supersingular elliptic curves $(E, \iota) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_K))$, $(F, \tau) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_\ell^{(n)}))$, and auxiliary sequences of (F, τ), find a descending isogeny $(E, \iota) \to (F, \tau)$.

If this problem could be solved then one could solve the problem to find a secret ideal class in $\mathcal{Cl}(\mathcal{O}_\ell^{(n)})$ by successively searching connecting ideal classes in $\mathcal{Cl}(\mathcal{O}_\ell^{(i)})$ for $i = 0, \ldots, n-1$. See §5.1 in [5] for the details. Note that a solution to this problem always exists. Furthermore, it is unique up to equivalence of isogenies if the condition of Theorem 2.5 is satisfied (see §4 in [14]).

§6.3 in [14] gives a condition on the parameter set of OSIDH that satisfies a certain security level by assuming that the best way to solve these problems is the meet-in-the-middle attack [9]. In particular, this assumption means that one does not use the auxiliary sequences for an attack to Problem 2.7. We discuss the impact of the auxiliary sequences on these problems in §4.

§ 3. SiGamal

SiGamal is a public-key encryption using supersingular elliptic curves defined over a finite prime field $\mathbb{F}_p$. The name comes from the fact that the scheme is similar to the ElGamal encryption [8].

§ 3.1. Group Actions in CSIDH

First we recall the group actions used in CSIDH since these are also used in SiGamal.

Let $p > 3$, and E be a supersingular elliptic curve over $\mathbb{F}_p$. We denote the $\mathbb{F}_p$-endomorphism ring of E by $\mathrm{End}_{\mathbb{F}_p}(E)$. This ring has a subring $\mathbb{Z}[\phi_p]$, where ϕ_p is the p-Frobenius endomorphism. $\mathbb{Z}[\phi_p]$ is isomorphic to $\mathbb{Z}[\sqrt{-p}]$ since E is supersingular. $\mathrm{End}_{\mathbb{F}_p}(E)$ is isomorphic to $\mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$ (§2 in [7]). For $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, we define $\mathrm{Ell}_p(\mathcal{O})$ as the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves whose $\mathbb{F}_p$-endomorphism ring is isomorphic to $\mathcal{O}$. Then the ideal class group $\mathcal{Cl}(\mathcal{O})$ acts freely and transitively on $\mathrm{Ell}_p(\mathcal{O})$ (Theorem 7 in [3]).

This group action can be seen as the group action on primitive $\mathcal{O}$-oriented elliptic curves. The orientation is given by $\sqrt{-p} \mapsto \phi_p$. For two supersingular elliptic curves defined over $\mathbb{F}_p$, these are $\mathbb{F}_p$-isomorphic to each other if and only if $\mathbb{Q}(\sqrt{-p})$-isomorphic to each other. Therefore, we have $\mathrm{Ell}_p(\mathcal{O}) = \mathrm{SS}^{\mathrm{pr}}_{\mathcal{O}}(p) = \rho(\mathcal{E}\ell\ell(\mathcal{O}))$ (in this case ρ is surjective since $(E, \iota) = (E^{(P)}, \iota^{(p)})$ for $E/\mathbb{F}_p$ and $\iota : \sqrt{-p} \mapsto \phi_p$).

In the case that $p \equiv 3 \pmod 4$, an $\mathbb{F}_p$-isomorphism class in $\mathrm{Ell}_p(\mathbb{Z}[\sqrt{-p}])$ can be determined by an expression in the Montgomery form. More precisely, we have the following.

Proposition 3.1 (Proposition 3 in [2]). *Let $p > 3$ be a prime number such that $p \equiv 3 \pmod 4$ and E a supersingular elliptic curve over $\mathbb{F}_p$. If $\mathrm{End}_{\mathbb{F}_p}(E) \cong \mathbb{Z}[\sqrt{-p}]$*

then there exists a coefficient $a \in \mathbb{F}_p$ for which E is $\mathbb{F}_p$-isomorphic to the curve $E : y^2 = x^3 + ax^2 + x$. Furthermore, the coefficient a is unique.

This proposition allows us to use the Montgomery coefficient a as an identifier of a class in $\mathrm{Ell}_p(\mathbb{Z}[\sqrt{-p}])$. A more general result for a relation between the coefficient of curves and endomorphism rings is summarized in Table 1 in [2].

In the following, we omit the orientation defined above, i.e., we simply write an oriented elliptic curve (E, ι) as E if ι is defined by $\sqrt{-p} \to \phi_p$.

The protocol of CSIDH is almost as same as that of OSIDH. The difference is that CSIDH does not need auxiliary sequences since the orientation is obvious and that CSIDH uses the Montgomery coefficients instead of j-invariants as identifiers of classes of curves.

§ 3.2. Indistinguishability

To explain the motivation for SiGamal, we recall ciphertext indistinguishability. In this paper, we do not give a formal definition of indistinguishability. Here, we roughly explain it. A certain cryptosystem has *indistinguishability* if any PPT (probabilistic polynomial-time) adversary cannot distinguish ciphertexts of two given plain texts. This means that any information of plain text does not leak in the cryptosystem.

A naive public-key encryption scheme derived from CSIDH does not have indistinguishability since a shared secret in CSIDH is a Montgomery coefficient, which can be distinguished from an element uniformly sampled from $\mathbb{F}_p$ by a supersingularity test. To achieve indistinguishability, CSIDH needs a cryptographic hash function that maps Montgomery coefficients to uniform elements in $\mathbb{F}_p$. For a detailed discussion, see §2.5 in [13].

§ 3.3. Protocol

SiGamal uses a ciphertext derived from the image of a point under a secret isogeny instead of a Montgomery coefficient. Therefore, a supersingularity test does not break the indistinguishability of SiGamal.

First we recall a property of images of points under isogenies corresponding to class group actions.

Proposition 3.2. *Let $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, $E \in \mathrm{Ell}_p(\mathcal{O})$, and $\mathfrak{a}$ be an invertible integral ideal of $\mathcal{O}$. Let φ and ψ be separable isogenies defined over $\mathbb{F}_p$ with kernel $E[\mathfrak{a}]$. Then we have $\varphi(P) = \psi(P)$ or $\varphi(P) = -\psi(P)$ for all $P \in E$.*

Proof. See Theorem 4 and Lemma 1 in [13]. □

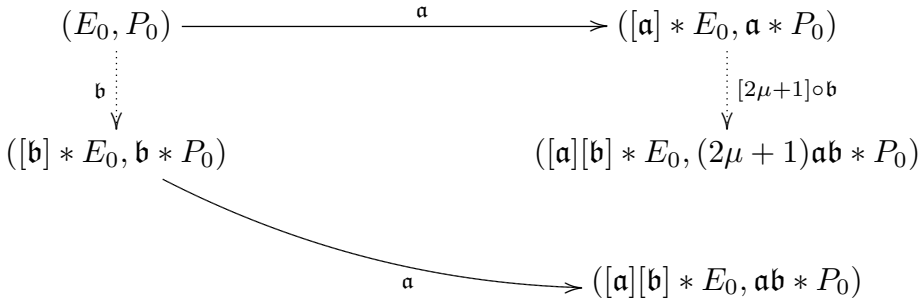

Figure 1. Diagram of SiGamal. Continuous lines are computed by the receiver, and dotted lines are by the sender

We denote the image $\varphi(P)$ in the above proposition by $\mathfrak{a} * P$. This point is determined up to sign. Note that for ideals $\mathfrak{a}, \mathfrak{b}$ in the same class, $\mathfrak{a} * P$ may differ from $\mathfrak{b} * P$ in general.

The protocol of SiGamal is as follows: (Figure 1 illustrates this protocol.)

Public parameter: Let p be a prime of form $2^r \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are small distinct odd primes. Let $\mathfrak{l}_i$ is a prime ideal of $\mathbb{Z}[\sqrt{-p}]$ above ℓ_i for $i = 1, \ldots, n$. The actions of $\mathfrak{l}_i$ can be efficiently computed by Vélu's formulae [18]. Let $E_0 \in \mathrm{Ell}_p(\mathbb{Z}[\sqrt{-p}])$, and P_0 be a point in $E_0(\mathbb{F}_p)$ of order 2^r.

Secret key: A secret key is an invertible integral ideal $\mathfrak{a}$ of form $\alpha \ell_1^{e_1} \cdots \ell_n^{e_n}$, where α is an integer in $[0, 2^r - 1]$ and $e_1, \ldots, e_n$ are integers in a certain range (this range is determined by the size of $\mathcal{C}\ell(\mathbb{Z}[\sqrt{-p}])$).

Public key: The public key corresponding to a secret key $\mathfrak{a}$ is a pair $(E_1, P_1) \coloneqq ([\mathfrak{a}] * E_0, \mathfrak{a} * P_0)$.

Encryption: Let μ be a $(r-2)$-bit message. We regard μ as an integer in $[0, 2^{r-2} - 1]$. The sender takes a random invertible integral ideal $\mathfrak{b}$ of form $\beta \ell_1^{e'_1} \cdots \ell_n^{e'_n}$, where β is an integer in $[0, 2^r - 1]$ and $e'_1, \ldots, e'_n$ are integers in the same range as $e_1, \ldots, e_n$. The ciphertext corresponding to the message μ, a public key (E_1, P_1), and β is a tuple $(E_3, P_3, E_4, P_4) \coloneqq ([\mathfrak{b}] * E_0, \mathfrak{b} * P_0, [\mathfrak{b}] * E_1, (2\mu + 1)\mathfrak{b} * P_1)$.

Decryption: The receiver calculates $\mathfrak{a} * P_3$ from the ciphertext and the secret key and solves the discrete logarithm problem between $\mathfrak{a} * P_3$ and P_4. (This discrete logarithm problem can be easily solved since the order of $\mathfrak{a} * P_3$ is a power of 2.) Let m be the solution, i.e., $P_4 = m\mathfrak{a} * P_3$. The decrypted message is $(m-1)/2$ if $m < 2^{r-1}$ and $(2^r - m - 1)/2$ otherwise.

Note that, in the above protocol, the curves are represented by Montgomery coefficients and the points by x-coordinates. These representations uniquely determine the $\mathbb{F}_p$-isomorphism classes of the curves and the points up to sign.

Remark. In the above protocol, the sender does not need to send E_4 since the receiver can calculate this curve by $[\mathfrak{a}] * E_3$. Furthermore, there is a trick to remove P_4 from a ciphertext. The scheme that uses this trick is named C-SiGamal, which is also proposed in [13]. See §4 in [13] for the details.

§ 3.4. Security

SiGamal depends on the hardness of the following problem, which requires to distinguish the image of a point under a secret isogeny from a random point of the same order.

Problem 3.3. We use the same notation as in §3.3. Given $E_0, [\mathfrak{a}] * E_0, P_0$, and a point Q, where Q is randomly chosen from $\mathfrak{a} * P_0$ and a random element of $[\mathfrak{a}] * E_0$ of order 2^r, determine $Q = \mathfrak{a} * P_0$ or not.

This problem seems to be hard (even for quantum algorithms) since calculating the image of a point under a secret isogeny is considered to be as hard as calculating the isogeny itself. We discuss this hardness in §4.

SiGamal achieves a certain type of indistinguishability by assuming the hardness of a "DDH variant" of Problem 3.3 (Theorem 8 in [13]).

§ 4. Isogeny Problems

In this section, we discuss the hardness of some problems related to OSIDH and SiGamal. First, we explain the hardness of calculating the image of a point under a secret isogeny. Next, we show a relation between this and the hardness of the problems given in the previous sections.

§ 4.1. Image Point Under Isogeny

Let E_0, E_1 be supersingular elliptic curves over $\mathbb{F}_{p^2}$, and $\varphi : E_0 \to E_1$ an isogeny of degree d. Let m be a positive integer prime to p and d, and P, Q generators of $E[m]$. We assume that these data can be represented by the size of a polynomial in $\log p$. In particular, all the prime factors of d are bounded by a polynomial in $\log p$, and $E[m]$ is defined over an extension field of $\mathbb{F}_{p^2}$ of a small degree. In addition, we also assume that all the prime factors of m are bounded by a polynomial in $\log p$. In this setting, we consider the following problem.

Problem 4.1. Given $E_0, E_1, d, m, P, Q, \varphi(P)$, and $\varphi(Q)$, find φ.

We say $P, Q, \varphi(P), \varphi(Q)$ *auxiliary points*. SIDH is based on the hardness of this problem for a certain tuple (p, d, m).

In addition, we assume that the structure of the endomorphism ring of E_0 is known. At the moment, Bröker's method [1] is the only efficient way to construct a supersingular elliptic curve for large p. This method uses CM theory, and consequently, the endomorphism ring of a constructed curve is known (in particular, it has an orientation of an imaginary quadratic field with a small discriminant). Therefore, it is natural to assume that the structure of the endomorphism ring of the starting curve E_0 is known in the setting of SIDH (and other cryptosystems).

In this setting, Petit [15] proposed an algorithm that solves Problem 4.1. The complexity of Petit's algorithm is polynomial in $\log p$ for some tuples (p, d, m) (of course, SIDH does not use such tuples). In particular, Petit showed that if $p < d$ and $d^4 < m$ then the complexity is $\log p$ under some heuristics. Kutas, Martindale, Panny, Petit, and Stange [12] improved Petit's algorithm. Their refined algorithm has polynomial-time complexity in the case that $p < d^2$ and $d^3 < m$, or $p < d$ and $d^2 < m$.

Petit's algorithm tells us that if one could find the image of an arbitrary point in E_0 under φ then s/he could find φ itself.

§ 4.2. Isogeny Problem in SiGamal

As we mentioned in §3.4, SiGamal depends on the hardness of calculating the image of a point under a secret isogeny. However, the setting in SiGamal is different from that we consider in §4.1. In SiGamal,

- the degree of the isogeny is hidden,
- the isogeny is defined over $\mathbb{F}_p$,
- and we take one point in the torsion subgroup, not generators.

As far as the author knows, there is no algorithm to find the secret isogeny in SiGamal (the isogeny corresponding to $\mathfrak{a}$) by using a pair of a point and its image $(P_0, \mathfrak{a} * P_0)$. In particular, Petit's algorithm cannot be applied in a straightforward way.

§ 4.3. Isogeny Problem in OSIDH

We show that the descending isogeny problem (Problem 2.7) is at least as hard as Problem 4.1 for some parameters. To do this, it is sufficient to show that one can calculate auxiliary sequences from auxiliary points.

Let K be an imaginary quadratic field with a small discriminant, and θ an algebraic integer in K such that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Let $\ell \neq p$ be a prime, n a positive integer, and m a positive integer of form $\prod_{k=1}^{t} q_k^{e_k}$, where $q_k \neq \ell$ is prime splitting in K and the size of q_k is bounded by a polynomial in $\log p$. We consider two orientated supersingular elliptic curves $(E, \iota) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_K))$ and $(F, \tau) \in \rho(\mathcal{E}\ell\ell(\mathcal{O}_\ell^{(n)}))$, and a descending isogeny $\varphi : (E, \iota) \to (F, \tau)$. Let P, Q be generators of $E[m]$, and assume that these points can

be represented by the size of a polynomial in $\log p$. Furthermore, we assume that the endomorphism $\iota(\theta)$ can be calculated in time of polynomials in $\log p$ (by the assumption on K, the degree of $\iota(\theta)$ is small). Then we have the following.

Theorem 4.2. *There exists an algorithm whose complexity is polynomial in* $\log p$ *to calculate auxiliary sequences*

$$(F,\tau),\ [\mathfrak{q}_k]*(F,\tau),\ [\mathfrak{q}_k^2]*(F,\tau),\ \ldots,\ [\mathfrak{q}_k^{e_k}]*(F,\tau),$$
$$(F,\tau),\ [\mathfrak{q}_k^{-1}]*(F,\tau),\ [\mathfrak{q}_k^{-2}]*(F,\tau),\ \ldots,\ [\mathfrak{q}_k^{-e_k}]*(F,\tau),$$

from $\ell, n, m, (E,\iota), (F,\tau), P, Q, \varphi(P)$, *and* $\varphi(Q)$.

Proof. (This proof is based on an idea in Petit's algorithm [15].)

It suffices to show the case that m has only one prime factor. Let $m = q^e$. Since φ is K-oriented, we have $\tau(\ell^n\theta) = \varphi \circ \iota(\theta) \circ \hat{\varphi}$. Therefore, we have

$$\tau(\ell^n\theta)(\varphi(P)) = \varphi(\ell^n\iota(\theta)(P)).$$

We can represent $\ell^n\iota(\theta)(P)$ as a linear combination of P and Q since $\ell^n\iota(\theta)(P) \in E[q^e]$, and $\tau(\ell^n\theta)$ can also be represented as a linear combination of $\varphi(P)$ and $\varphi(Q)$. Consequently, we can calculate the images of $\varphi(P)$ and $\varphi(Q)$ under the endomorphism $\tau(\ell^n\theta)$.

A prime ideal $\mathfrak{q}$ of $\mathcal{O}_\ell^{(n)}$ above q is generated by q and $a+b\ell^n\theta$, where a, b are integer such that the norm of $a + b\ell^n\theta$ is divisible by q but not by q^2. We can find such a, b by a brute-force search (note that q is less than a polynomial in $\log p$). By calculating ideal products, we obtain $\alpha \in \mathcal{O}_\ell^{(n)}$ such that q^e and α generate $\mathfrak{q}^e$ in $\mathcal{O}_\ell^{(n)}$.

Now, we can calculate $\alpha(\varphi(P))$ and $\alpha(\varphi(Q))$ since $\alpha \in \mathcal{O}_\ell^{(n)} = \mathbb{Z}[\ell^n\theta]$. So we know a generator of $F[q^e] \cap \ker\alpha = F[\mathfrak{q}]$. By using Vélu's formula for isogenies of degree q repeatedly, we can calculate the sequence

$$(F,\tau),\ [\mathfrak{q}_k]*(F,\tau),\ [\mathfrak{q}_k^2]*(F,\tau),\ \ldots,\ [\mathfrak{q}_k^{e_k}]*(F,\tau).$$

Similarly, we can calculate the sequence for $\mathfrak{q}^{-1}$. □

As a result, the descending isogeny problem seems to be hard if we use auxiliary sequences such that Problem 4.1 of the corresponding parameter is considered to be hard.

§ 5. Conclusion

We introduced two isogeny-based cryptosystems, OSIDH and SiGamal, and discussed the security of these cryptosystems. In particular, we showed that the descending isogeny problem is as hard as a well-known isogeny problem in SIDH for a certain parameter setting.

Constructing a computational reduction from the isogeny problem in SiGamal or the horizontal isogeny problem (Problem 2.6) to other known problems is an open problem.

References

[1] R. Bröker, Constructing supersingular elliptic curves. Journal of Combinatorics and Number Theory **1(3)** 269–273, 2009.

[2] W. Castryck, and T. Decru, CSIDH on the surface. *PQCrypto 2020*, LNCS **12100**, pp. 111–129.

[3] W. Castryck, T. Lange, C. Martindale, L. Panny, and J. Renes, CSIDH: An efficient post-quantum commutative group action. *ASIACRYPT 2018*, LNCS **11274**, pp. 395–427.

[4] D. Charles, E. Goren, and K. Lauter, Cryptographic hash functions from expander graphs. Cryptology ePrint Archive, Report 2006/021. `https://eprint.iacr.org/2006/021`.

[5] L. Colò and D. Kohel, Orienting supersingular isogeny graphs. *Number-Theoretic Methods in Cryptology 2019*.

[6] J.-M. Couveignes, Hard homogeneous spaces. IACR Cryptology ePrint Archive 2006/291. `https://eprint.iacr.org/2006/291`.

[7] C. Delfs and S. D. Galbraith, Computing Isogenies between Supersingular Elliptic Curves over $\mathbb{F}_p$. *Des. Codes Cryptography*, **78(2)**, pp. 425—440, 2016.

[8] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, **31(4)**, pp. 469–472, 1985.

[9] S. D. Galbraith, Constructing Isogenies between Elliptic Curves Over Finite Fields. *LMS Journal of Computation and Mathematics*, **2**, pp. 118–138, 1999.

[10] C. D. Guilhem, P. Kutas, C. Petit, and J. Silva, SÉTA: Supersingular Encryption from Torsion Attacks. Cryptology ePrint Archive, Report 2019/1291. `https://eprint.iacr.org/2019/1291`

[11] D. Jao and L. De Feo, Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. *PQCrypto 2011*, LNCS **7071**, pp. 19–34.

[12] P. Kutas, C. Martindale, L. Panny, C. Petit, K. E. Stange, Weak instances of SIDH variants under improved torsion-point attacks. Cryptology ePrint Archive, Report 2020/633. `https://eprint.iacr.org/2020/633`

[13] T. Moriya, H. Onuki, and T. Takagi SiGamal: A supersingular isogeny-based PKE and its application to a PRF. *ASISACRYPT 2020*, LNCS **12492**, pp. 551–580.

[14] H. Onuki, On oriented supersingular elliptic curves, *Finite Fields and Their Applications*, **69**, article 101777, 2021.

[15] C. Petit, Faster algorithms for isogeny problems using torsion point images. *ASIACRYPT 2017*, LNCS **10625**, pp. 330–353.

[16] A. Rostovtsev and A. Stolbunov, Public-key cryptosystem based on isogenies. Cryptology ePrint Archive, Report 2006/145. `https://eprint.iacr.org/2006/145`.

[17] A. Stolbunov, Constructing public-key cryptographic schemes based on class group action on a set of isogenous elliptic curves. *Advances in Mathematics of Communications*, **4(2)**:215, 2010.

[18] J. Vélu, Isogénies entre courbes elliptiques. *Comptes-Rendues de l'Académie des Sciences*, **273** pp. 238–241, 1971.