SiGamal

Hiroshi Onuki*

July 22, 2021

SiGamal is an IND-CPA secure public-key encryption using the group action in CSIDH without hash function. The name comes from supersinguler isogeny encryption that is similar to the ElGamal encryption [5].

1 Background

1.1 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 $\mathbb{Z}[\pi_p]$, where π_p is the p-Frobenius endomorphism. $\mathbb{Z}[\pi_p]$ 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 [4]). For $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, we define $\mathcal{E}\ell\ell_p(\mathcal{O})$ as the set of $\mathbb{F}_p$-isomorphism classes of supersingular elliptic curves whose $\mathbb{F}_p$-endomorphism ring is isomorphic to $\mathcal{O}$. To ease notation, we use the same symbol for an $\mathbb{F}_p$-isomorphism class of curves and a curve in the class. We denote the ideal class group of $\mathcal{O}$ by $\mathcal{C}\ell(\mathcal{O})$. For an ideal $\mathfrak{a}$ of $\mathcal{O}$, we denote the class of $\mathfrak{a}$ by $[\mathfrak{a}]$.

Let $E \in \mathcal{E}\ell\ell_p(\mathcal{O})$ and $\mathfrak{a}$ be an integral ideal of $\mathcal{O}$. We define the $\mathfrak{a}$-torsion subgroup of E by

$$E[\mathfrak{a}] \coloneqq \{P \in E \mid \alpha(P) = O \text{ for all } \alpha \in \mathfrak{a}\}.$$

Then there exists an elliptic curve $E' \in \mathcal{E}\ell\ell_p(\mathcal{O})$ and an isogeny $\varphi : E \to E'$ with $\ker\varphi = E[\mathfrak{a}]$. The curve E' is determined by the class $[\mathfrak{a}]$ as the class in $\mathcal{E}\ell\ell_p(\mathcal{O})$. We denote the class of E' by $[\mathfrak{a}] * E$. From this, we can define an action of $\mathcal{C}\ell(\mathcal{O})$ on $\mathcal{E}\ell\ell_p(\mathcal{O})$. This action is free and transitive (Theorem 7 in [3]).

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

Proposition 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 $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$. A more general result for a relation between the coefficient of curves and endomorphism rings is summarized in Table 1 in [2].

1.2 Isogeny Image

SiGamal uses a ciphertext derived from the image of a point under a secret isogeny instead of a Montgomery coefficient. We show a property of images of points under isogenies corresponding to class group actions.

*Department of Mathematical Informatics, The University of Tokyo, Japan

Proposition 2. *Let $\mathcal{O} = \mathbb{Z}[\sqrt{-p}]$ or $\mathbb{Z}\left[\frac{1+\sqrt{-p}}{2}\right]$, $E \in \mathcal{E}\ell\ell_p(\mathcal{O})$, and $\mathfrak{a}$ be an invertible integral ideal of $\mathcal{O}$. Let $E' \in \mathcal{E}\ell\ell_p(\mathcal{O})$ and $\varphi, \psi : E \to E'$ 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 [7]. □

Consider the set $E'/\{\pm 1\}$, in which $Q \in E'$ and $-Q$ are equivalent. We denote the class of $\varphi(P)$ in the above proposition by $\mathfrak{a} * P$. If E' is a Montgomery curve, then elements in $E'/\{\pm 1\}$ are uniquely determined by the x-coordinates. Note that for ideals $\mathfrak{a}, \mathfrak{b}$ in the same class, $\mathfrak{a} * P$ may differ from $\mathfrak{b} * P$ in general.

1.3 Public Key Encryption

Public key encryption (PKE) consists of three algorithms, `KeyGen`, `Enc`, and `Dec`. `KeyGen` takes a security parameter λ as input and outputs a secret key $\mathbf{sk}$, a public key $\mathbf{pk}$, and a message space $\mathcal{M}$. `Enc` takes a plaintext $\mu \in \mathcal{M}$ and $\mathbf{pk}$ as input and outputs a ciphertext c. `Dec` takes c and $\mathbf{pk}$ as input and outputs a plaintext $\tilde{\mu}$. If $\mu = \tilde{\mu}$, then we call a PKE is *correct*.

We define three properties for the security of PKEs, OW-CPA (one-wayness for chosen-plaintext attacks), IND-CPA (indistinguishability for chosen-plaintext attacks), and IND-CCA (indistinguishability for chosen-ciphertext attacks).

Definition 1 (OW-CPA secure)**.** Let $\mathcal{P}$ be a PKE with a plaintext message space $\mathcal{M}$. We say that $\mathcal{P}$ is OW-CPA secure if, for any efficient adversary $\mathcal{A}$,

$$\Pr\left[\ \mu = \mu^* \ \middle|\ \begin{array}{l}(\mathbf{pk}, \mathbf{sk}) \leftarrow \mathsf{KeyGen}(\lambda),\ \mu \xleftarrow{\$} \mathcal{M},\\ c \leftarrow \mathsf{Enc}(\mathbf{pk}, \mu),\ \mu^* \leftarrow \mathcal{A}(\mathbf{pk}, c)\end{array}\ \right] < \mathrm{negl}(\lambda),$$

where $\mu \xleftarrow{\$} \mathcal{M}$ means that μ is uniformly and randomly sampled from $\mathcal{M}$.

Definition 2 (IND-CPA security)**.** Let $\mathcal{P}$ be a PKE with a plaintext message space $\mathcal{M}$. We say that $\mathcal{P}$ is IND-CPA security if, for any efficient adversary $\mathcal{A}$,

$$\left|\Pr\left[\ b = b^* \ \middle|\ \begin{array}{l}(\mathbf{pk}, \mathbf{sk}) \leftarrow \mathsf{KeyGen}(\lambda),\ \mu_0, \mu_1 \leftarrow \mathcal{A}(\mathbf{pk}),\\ b \xleftarrow{\$} \{0,1\},\ c \leftarrow \mathsf{Enc}(\mathbf{pk}, \mu_b),\\ b^* \leftarrow \mathcal{A}(\mathbf{pk}, c)\end{array}\ \right] - \frac{1}{2}\right| < \mathrm{negl}(\lambda).$$

Definition 3 (IND-CCA secure)**.** Let $\mathcal{P}$ be a PKE with a plaintext message space $\mathcal{M}$. We say that $\mathcal{P}$ is IND-CCA secure if, for any efficient adversary $\mathcal{A}$,

$$\left|\Pr\left[\ b = b^* \ \middle|\ \begin{array}{l}(\mathbf{pk}, \mathbf{sk}) \leftarrow \mathsf{KeyGen}(\lambda),\ \mu_0, \mu_1 \leftarrow \mathcal{A}^{O(\cdot)}(\mathbf{pk}),\\ b \xleftarrow{\$} \{0,1\},\ c \leftarrow \mathsf{Enc}(\mathbf{pk}, \mu_b),\\ b^* \leftarrow \mathcal{A}^{O(\cdot)}(\mathbf{pk}, c)\end{array}\ \right] - \frac{1}{2}\right| < \mathrm{negl}(\lambda),$$

where $O(\cdot)$ is a decryption oracle that outputs $\mathsf{Dec}(\mathbf{sk}, c^*)$ for all $c^* \neq c$.

1.4 PKE from CSIDH

We consider constructing a PKE from CSIDH. A natural way is as follows:

`KeyGen`(λ)**:** Take a prime p of form $p = 4 \cdot \ell_1 \cdots \ell_n - 1$ such that the size of p satisfies the λ security [1]. Let E_0 be the elliptic curve $y^2 = x^3 + x$. A secret key $\mathbf{sk}$ is an integer vector $(e_1, \ldots, e_n)$, where $(e_1, \ldots, e_n)$ in a subset of $\mathbb{Z}^n$ with cardinality about $2^{2\lambda}$. Take an ideal $\mathfrak{a} = \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$, where $\mathfrak{l}_i$ is the prime ideal generated by ℓ_i and $\pi_p - 1$ for $i = 1, \ldots n$. A public key $\mathbf{pk}$ is $[\mathfrak{a}] * E_0$. A message space $\mathcal{M}$ is $\mathbb{F}_p$.

[1] The original paper of CSIDH [3] takes $p \approx 2^{4\lambda}$. The quantum-secure size of p is now under discussion [1, 8].

$\texttt{Enc}(\mu, \mathbf{pk})$**:** Take a random integer vector $(e'_1, \ldots, e'_n)$, where $(e'_1, \ldots, e'_n)$ in the same set as $(e_1, \ldots, e_n)$. Let $\mathfrak{b} = \mathfrak{l}_1^{e'_1} \cdots \mathfrak{l}_n^{e'_n}$, S be the Montgomery coefficient of $[\mathfrak{a}][\mathfrak{b}] * E_0$, and $s = S + \mu$. The ciphertext c is a pair $([\mathfrak{b}] * E_0, s)$

$\texttt{Dec}(c, \mathbf{sk})$**:** Compute the Montgomery coefficient S of $[\mathfrak{a}\mathfrak{b}] * E_0 = [\mathfrak{a}] * ([\mathfrak{b}] * E_0)$. The output $\tilde{\mu}$ is $s - S$.

This PKE is not IND-CPA secure since a supersingularity test (it has a polynomial time in $\log p$. See [10]). For two candidates μ_0 and μ_1 of a plaintext μ, an adversary tests the supersingularity of the curves with Montgomery coefficients $c - \mu_0$ and $c - \mu_1$. If μ_0 is the plaintext, then the curve with coefficient $c - \mu_0$ is supersingular, and the other curve is ordinary with a probability of about $1 - 1/\sqrt{p}$. Therefore, the adversary can distinguish the plaintext.

To make this PKE IND-CPA secure, we need to use a cryptographic hash function. Let $H : \mathbb{F}_p \to \mathbb{F}_p$ be a cryptographic hash function. If we change the ciphertext c to $H(S) + \mu$ in $\texttt{Enc}$ of the above protocol, then the protocol is IND-CPA secure under the assumption that CSIDH and the hash function H are secure.

2 Basic Protocol

SiGamal achieves the IND-CPA security by taking hidden information from a point of a curve, not from a curve. The idea comes from the assumption that the image of a point of a specific order under a hidden isogeny cannot be distinguished from a random point of the same order.

2.1 Computational Assumption in SiGamal

First, we consider the following problem.

Problem 1. Given $E, E' \in \mathcal{E}\ell\ell_p(\mathcal{O})$ and $P \in E$, find $\mathfrak{a} * P$ such that $E' = [\mathfrak{a}] * E$.

This problem does not make sense since E and E' determine the ideal class $[\mathfrak{a}]$ but not the ideal $\mathfrak{a}$. As we mentioned in Section 1.2, the image of P depends on a representative of the ideal class.

To resolve this obstacle, we use a diagram in CSIDH and images under the isogenies,

$$\begin{array}{ll} E & [\mathfrak{a}] * E \\ \\ [\mathfrak{b}] * E & [\mathfrak{a}][\mathfrak{b}] * E, \end{array}$$

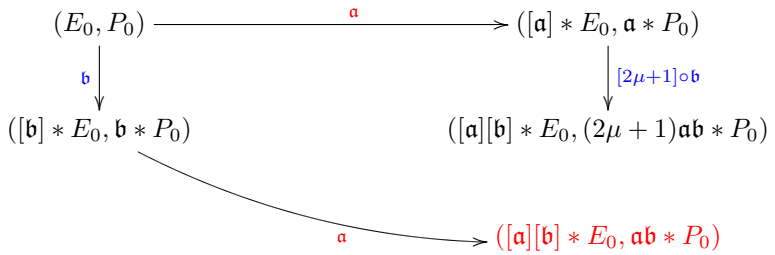

Figure 1: Diagram of SiGamal. The black symbols are public. The red symbols are privately computed by the sender, and the blue symbols by the receiver.

2.2 Protocol

SiGamal uses the characteristic p of form $2^r \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots, \ell_n$ are distinct small odd primes. As in CSIDH, secret keys of SiGamal are products of prime ideals above $\ell_1, \ldots \ell_n$. A secret key of SiGamal is an ideal $\mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$, where $e_1, \ldots, e_n$ are integers sampled from a certain subset of $\mathbb{Z}^n$. The factor 2^r of $p+1$ determines the message space of SiGamal. More precisely, the message space is the set of integers from 0 to $2^{r-2}-1$.

In the protocol of SiGamal, we use Montgomery curves and represent a curve by its Montgomery coefficient and a point by its x-coordinate, i.e., these are represented by elements in $\mathbb{F}_p$. The protocol is as follows (Figure 1 illustrates this protocol.):

`KeyGen`(λ)**:** Take a prime p of form $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$ whose size is as same as in CSIDH of the security level λ. Let E_0 be the elliptic curve $y^2 = x^3 + x$ and P_0 a point in $E_0(\mathbb{F}_p)$ of order 2^r. A secret key $\mathbf{sk}$ is an integer vector $(\alpha, e_1, \ldots, e_n)$, where α is an odd number in $[1, 2^r - 1]$ and $(e_1, \ldots, e_n)$ in a subset of $\mathbb{Z}^n$ with cardinality about $2^{2\lambda}$. Take an ideal $\mathfrak{a} = \alpha \mathfrak{l}_1^{e_1} \cdots \mathfrak{l}_n^{e_n}$. A public key $\mathbf{pk}$ is a pair $([\mathfrak{a}] * E_0, \mathfrak{a} * P_0)$. A message space $\mathcal{M}$ is $[0, 2^{r-2} - 1] \cap \mathbb{Z}$.

`Enc`$(\mu, \mathbf{pk})$**:** Take a random integer vector $(\beta, e'_1, \ldots, e'_n)$, where β is an odd number in $[1, 2^r - 1]$ and $(e'_1, \ldots, e'_n)$ in the same set as $(e_1, \ldots, e_n)$. Let $\mathfrak{b} = \beta \mathfrak{l}_1^{e'_1} \cdots \mathfrak{l}_n^{e'_n}$. The ciphertext c is a tuple $([\mathfrak{b}] * E_0, \mathfrak{b} * P_0, [\mathfrak{a}][\mathfrak{b}] * E_0, (2\mu+1)\mathfrak{a}\mathfrak{b} * P_0)$

`Dec`$(c, \mathbf{sk})$**:** Compute $\mathfrak{a}\mathfrak{b} * P_0 = \mathfrak{a} * (\mathfrak{b} * P_0)$. Solve a discrete logarithm for $\mathfrak{a}\mathfrak{b} * P_0$ and $(2\mu+1)\mathfrak{a}\mathfrak{b} * P_0$ by using Pohlig-Hellman algorithm [9]. Let M be the solution. We can take M in $[0, 2^r - 1]$. Because the points $\mathfrak{a}\mathfrak{b} * P_0$ and $(2\mu+1)\mathfrak{a}\mathfrak{b} * P_0$ have order 2^r, the integer M is odd. If $M < 2^{r-1}$ then the output $\tilde{\mu}$ is $(M-1)/2$. Otherwise, $\tilde{\mu}$ is $(2^r - M - 1)/2$.

2.3 Security

We define security assumption in SiGamal. P-CSSDDH assumption defined below says that the solution of Problem 2 cannot be distinguished from a random point of the same order.

Definition 4 (P-CSSDDH (Points-Commutative Supersingular Isogeny Decisional Diffie-Hellman) assumption)**.** Let p be a prime of form $p = 2^r \cdot \ell_1 \cdots \ell_n - 1$, where $\ell_1, \ldots \ell_n$ are small distinct odd primes. Let E_0 be the elliptic curve $y^2 = x^3 + x$, P_0 be a uniformly random point in $E_0(\mathbb{F}_p)$ of order 2^r, and $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in $\mathbb{Z}[\sqrt{-p}]$ whose norms are odd. Furthermore, let Q be a uniformly random point of order 2^r in $([\mathfrak{a}][\mathfrak{b}] * E_0)(\mathbb{F}_p)$. Set λ as the bit length of p.

The *P-CSSDDH assumption* holds if, for any efficient algorithm $\mathcal{A}$,

$$\left| \Pr\left[b = b^* \;\middle|\; \begin{array}{l} b \xleftarrow{\$} \{0,1\},\ R_0 \coloneqq \mathfrak{a}\mathfrak{b} * P_0,\ R_1 \coloneqq Q, \\ b^* \leftarrow \mathcal{A}(E_0, P_0, [\mathfrak{a}] * E_0, \mathfrak{a} * P_0, [\mathfrak{b}] * E_0, \mathfrak{b} * P_0, [\mathfrak{a}][\mathfrak{b}] * E_0, R_b) \end{array} \right] - \frac{1}{2} \right| < \mathrm{negl}(\lambda).$$

Assuming P-CSSDDH assumption, SiGamal is IND-CPA secure (Theorem 8 in [7]).

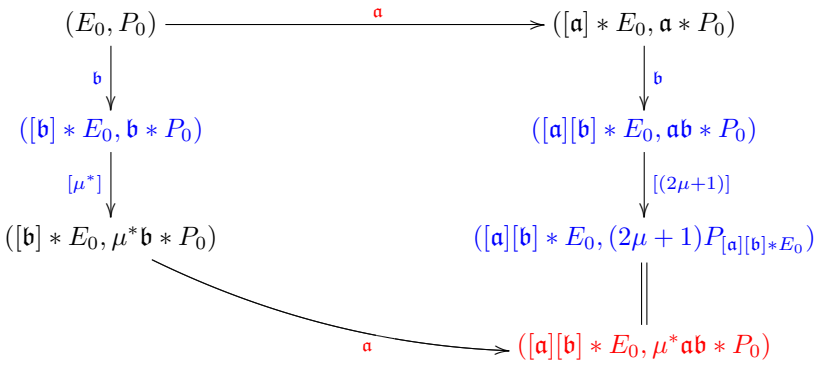

Figure 2: Diagram of C-SiGamal. The black symbols are public. The red symbols are privately computed by the sender, and the blue symbols by the receiver.

3 Compressed Version

We use the same symbols as in SiGamal in this section. A ciphertext of SiGamal is a tuple $([\mathfrak{b}] * E_0, \mathfrak{b} * P_0, [\mathfrak{a}][\mathfrak{b}] * E_0, \mathfrak{ab} * P_0)$. The receiver of this ciphertext does not need the curve $[\mathfrak{a}][\mathfrak{b}] * E_0$ because it can be computed from $[\mathfrak{b}] * E_0$ and the secret key $\mathfrak{a}$. So we have a tradeoff between the computational cost of the decryption and the size of ciphertext. This observation leads us to a compressed version of SiGamal, C-SiGamal.

In C-SiGamal, we use a distinguished point of order 2^r in a Montgomery curve. To do so, we prepare an efficient algorithm that takes a Montgomery curve E as input and outputs a point $P_E \in E(\mathbb{F}_p)$ of order 2^r. We discuss how to construct such an algorithm in Section 3.2.

3.1 Protocol

Using distinguished points, we can drop $[\mathfrak{a}][\mathfrak{b}] * E_0$ and $\mathfrak{ab} * P_0$ from a ciphertext. A concrete description of the protocol is as follows (Figure 2 illustrates this protocol):

$\mathtt{KeyGen}(\lambda)$**:** The same as the uncompressed SiGamal.

$\mathtt{Enc}(\mu, \mathbf{pk})$**:** Take a random ideal $\mathfrak{b}$ as same as in the uncompressed SiGamal. Find an integer μ^* such that $\mu^*\mathfrak{ab} * P_0 = (2\mu+1)P_{[\mathfrak{a}][\mathfrak{b}]*E_0}$ by Pohlig-Hellman algorithm. The ciphertext c is a pair $([\mathfrak{b}] * E_0, \mu^*\mathfrak{b} * P_0)$

$\mathtt{Dec}(c, \mathbf{sk})$**:** Compute $\mu^*\mathfrak{ab} * P_0 = \mathfrak{a} * (\mu^*\mathfrak{b} * P_0)$. Find an integer M such that $MP_{[\mathfrak{a}][\mathfrak{b}]*E_0} = \mu^*\mathfrak{ab} * P_0$ by Pohlig-Hellman algorithm. We can take M in $[0, 2^r - 1]$. Because the points $\mathfrak{ab} * P_0$ and $(2\mu+1)\mathfrak{ab} * P_0$ have order 2^r, the integer M is odd. If $M < 2^{r-1}$ then the output $\tilde{\mu}$ is $(M-1)/2$. Otherwise, $\tilde{\mu}$ is $(2^r - M - 1)/2$.

C-SiGamal is also IND-CPA secure under P-CSSCDH assumption (Theorem 11 in [7]).

3.2 Distinguished Points

We discuss how to determine distinguished points. A simple algorithm for a Montgomery curve E is as follows:

1. Set $\xi = 2$. [2]
2. Let P be a point on E of x-coordinate ξ, and check $P \in E(\mathbb{F}_p)$ and the order of P is divisible by 2^r.
3. If P satisfies the condition, then output $P_E = \ell_1 \cdots \ell_n P$.

[2] In a Montgomery curve, the point of x-coordinate 0 has order 2, and the points of x-coordinate 1 have order 4.

4. Otherwise, change ξ to $\xi + 1$ and go to Step 2.

This algorithm, however, is not efficient in the case that $\ell_1, \ldots, \ell_n$ contains all odd primes below a certain number and $r \geq 3$. The reason is that the smallest ξ satisfying the condition in Step 2 is relatively large, so one should check the condition many times. This comes from the following proposition.

Proposition 3 (Proposition 1 in [7]). *Let p be a prime such that $p \equiv 3 \pmod 4$, and E be a Montgomery curve in $\mathcal{E}\ell\ell_p(\mathbb{Z}[\sqrt{-p}])$. Then, for $P \in E(\mathbb{F}_p)\backslash E[2]$, the x-coordinate of P is in $\mathbb{F}_p^{\times 2}$ if and only if P is in $2E(\mathbb{F}_p)$.*

For a SiGamal prime $p = 2^r \ell_1 \cdots \ell_n - 1$, we have $\ell_i \equiv 1 \pmod p$ for $i = 1, \ldots, n$. Furthermore, if $r \geq 3$, then 2 is in $\mathbb{F}_p^{\times 2}$. Therefore, all numbers factored into a product of 2 and $\ell_1, \ldots, \ell_n$ are also in $\mathbb{F}_p^{\times 2}$. This is the reason that the above algorithm is not efficient.

This problem can be easily solved by taking ξ from negative integers. I.e., we modify Step 2 in the above algorithm to $\xi = -2$ and Step 4 to $\xi - 1$.

4 IND-CCA Security

Finally, we quickly look at the IND-CCA security of SiGamal and related recent progress.

As shown in [7], SiGamal is not IND-CCA secure. Consider the situation in Figure 1. A CCA adversary can compute $3(2\mu + 1)\mathfrak{b} * P_0$ from the given ciphertext. Then the adversary decrypt a ciphertext $([\mathfrak{b}] * E_0, \mathfrak{b} * P_0, [\mathfrak{a}][\mathfrak{b}] * E_0, 3(2\mu + 1)\mathfrak{b} * P_0)$ by using the oracle. The decrypted message is $3\mu + 1$ and the adversary obtain the message μ from this.

Remark 7 in [7] suggests that a variant of SiGamal that omits $[\mathfrak{a}][\mathfrak{b}] * E_0$ from the ciphertext could be IND-CCA secure. However, Fouotsa and Petit [6] proved that the variant is not IND-CCA secure (Corollary 1 in [6]). Roughly speaking, the reason is that an adversary can compute a scalar multiplication of $\mathfrak{b} * P$ and can imitate a ciphertext for the same secret random ideal $\mathfrak{b}$ and another plaintext. In addition, Foutosa and Petit [6] proposed a new scheme that resists the above attack, SimS (Simplified SiGamal), a PKE based on C-SiGamal. SimS is IND-CCA secure under some new assumptions.

References

[1] Xavier Bonnetain and André Schrottenloher. Quantum security analysis of csidh. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 493–522, Cham, 2020. Springer International Publishing.

[2] Wouter Castryck and Thomas Decru. CSIDH on the surface. In Jintai Ding and Jean-Pierre Tillich, editors, *Post-Quantum Cryptography*, pages 111–129, Cham, 2020. Springer International Publishing.

[3] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In Thomas Peyrin and Steven Galbraith, editors, *Advances in Cryptology – ASIACRYPT 2018*, pages 395–427, Cham, 2018. Springer International Publishing.

[4] Christina Delfs and Steven D. Galbraith. Computing isogenies between supersingular elliptic curves over $\mathbb{F}_p$. *Designs, Codes and Cryptography*, 78(2):425–440, 2016.

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

[6] Tako Boris Fouotsa and Christophe Petit. SimS: a simplification of SiGamal. Cryptology ePrint Archive, Report 2021/218, 2021. https://eprint.iacr.org/2021/218 (To appear at PQCrypto 2021).

[7] Tomoki Moriya, Hiroshi Onuki, and Tsuyoshi Takagi. SiGamal: A supersingular isogeny-based PKE and its application to a PRF. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology – ASIACRYPT 2020*, pages 551–580, Cham, 2020. Springer International Publishing.

[8] Chris Peikert. He gives c-sieves on the csidh. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology – EUROCRYPT 2020*, pages 463–492, Cham, 2020. Springer International Publishing.

[9] Stephen Pohlig and Martin Hellman. An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance. *IEEE Transactions on information Theory*, 24(1):106–110, 1978.

[10] Andrew V. Sutherland. Identifying supersingular elliptic curves. *LMS Journal of Computation and Mathematics*, 15:317–325, 2012.