Avoiding Trusted Setup in Isogeny-based Commitments

Gustave Tchoffo Saah[1], Tako Boris Fouotsa[2], Emmanuel Fouotsa[3], and Célestin Nkuimi-Jugnia[1]

[1] Département de Mathématiques, Université de Yaoundé 1, Cameroon; gustavesaah@gmail.com, nkuimi@yahoo.co.uk
[2] EPFL, Lausanne, Switzerland; tako.fouotsa@epfl.ch
[3] Centre for Cybersecurity and Mathematical Cryptology, The University of Bamenda, Cameroon; emmanuelfouotsa@yahoo.fr

Abstract. In 2021, Sterner proposed a commitment scheme based on supersingular isogenies. For this scheme to be binding, one relies on a trusted party to generate a starting supersingular elliptic curve of unknown endomorphism ring. In fact, the knowledge of the endomorphism ring allows one to compute an endomorphism of degree a power of a given small prime. Such an endomorphism can then be split into two to obtain two different messages with the same commitment. This is the reason why one needs a curve of unknown endomorphism ring, and the only known way to generate such supersingular curves is to rely on a trusted party or on some expensive multiparty computation. We observe that if the degree of the endomorphism in play is well chosen, then the knowledge of the endomorphism ring is not sufficient to efficiently compute such an endomorphism and in some particular cases, one can even prove that endomorphism of a certain degree do not exist. Leveraging these observations, we adapt Sterner's commitment scheme in such a way that the endomorphism ring of the starting curve can be known and public. This allows us to obtain isogeny-based commitment schemes which can be instantiated without trusted setup requirements.

Keywords: Supersingular isogenies, Post-Quantum Cryptography, Isogeny-Based Cryptography, commitment schemes.

1 Introduction

A commitment scheme allows to commit to a message while keeping its content hidden until a desired moment. Such schemes play an important role in Cryptography, namely in proofs of knowledge [17,14] and electronic vote [16,13]. The two security requirements for commitment schemes are the binding and the hiding property. The binding property ensures that a message can not be changed after it has been committed to. The hiding property ensures that it must be impossible to learn any information about the message from its commitment. The most currently used commitment scheme is the Pedersen commitment [28], whose binding property is due to the uniqueness of the discrete logarithm, and the hiding property is based on the discrete logarithm problem. The discret logarithm problem can be solved with a quantum computer by using Shor's quantum algorithm [31], which also solves the integer factorization problem. Hence, the Pedersen scheme is not quantum safe, as well as protocols whose security is based on the discrete logarithm problem and integer factorization problem. Some alternatives to protocols whose security is based on discrete logarithm problem and integer factorization problem are lattice-based protocols, code-based protocols, isogeny-based protocols etc. In this paper, we are interested in isogeny-based commitments. The existing isogeny-based commitment scheme is proposed by Sterner [33]. This commitment scheme is constructed from CGL hash function [9], a hash function constructed with supersingular isogeny graph.

In 2006, Charles, Goren and Lauter [9] introduced a new method for constructing hash functions (the CGL hash function), which uses expander graphs. The method consists of constructing a path defined by the message in a graph, from a public fixed starting vertex to a vertex whose label is the hash of the message. One concrete example of expander graph used for CGL hash function is the supersingular ℓ-isogeny graph [30], whose vertices are isomorphism classes of supersingular elliptic curves and edges are isogenies of degree ℓ up to composition by authomorphisms, where ℓ is a small prime. The collision resistance of CGL hash function is based on the problem of computing ℓ-power degree endomorphisms of the starting curve. The pre-image resistance is based on the hardness of the supersingular ℓ-isogeny path problem, which consists of computing an isogeny of degree a power of ℓ between two random supersingular elliptic curves. This problem is believed to be hard, even for a quantum computer. The best known algorithm for solving it has complexity $O(p^{\frac{1}{2}})$ for classical computers [21] and $O(p^{\frac{1}{4}})$ for quantum computers [5], where p is the characteristic the base field.

Sterner's commitment scheme [33] can be summarized as follows. The space of messages is $\mathcal{M} = \{0, 1, \ldots, \ell - 1\}^*$. For $m \in \mathcal{M}$, the commitment for m is $\mathsf{CGL}(m||r)$, where r is sampled at random from $\{0, 1, \ldots, \ell - 1\}^{k_r}$ for some integer k_r. The hiding property is based on the fact that k_r should be greater than the mixing constant of the supersingular ℓ-isogeny graph in play. For such value of k_r (say $k_r > 2 \log_\ell p$) and some message of length k_m, $\ell^{k_m + k_r} > 2 \log_\ell p$ is large enough so that we can efficiently compute an endomorphism of degree $\ell^{2(k_r + k_m)} > p^4$ when the endomorphism of the starting curve is known [20,25]. Such an endomorphism represents a collision in the ℓ-isogeny graph, which compromises the binding property of this scheme. In order to avoid this, one uses a curve with unknown endomorphism ring. Unfortunately, all existing methods for efficiently constructing supersingular elliptic curves [7,26] allow the person generating the curve to efficiently recover its endomorphism ring. To solve this issue, the author suggests to delegate the generation of the starting curve to a trusted third party. Basso et al. [3] introduced a multiparty computation method for implementing such a trusted party. Such method requires a lot of resources.

In this work, we propose two approaches to avoid the trusted setup. These two approaches share the same idea which can be summarized as follows. We modify Sterner's commitment scheme so that the message space consists of messages of fixed length k_m and the random string r used to compute the commitment to m is of length k_r where k_m and k_r are such that either endomorphisms of degree $\ell^{2(k_m+k_r)}$ do not exist, or they exist but finding them is hard.

- The first approach consists of using as starting curve, the curve $E_6 : y^2 = x^3 + 6x^2 + x$ for which we can easily avoid endomorphisms of small degree in the setting of this commitment scheme. In fact it was shown in [27] that in a specific setting, some relatively short isogenies never have the same co-domain, hence there are no collisions. With this approach, we obtain a perfect binding and computationally hiding commitment scheme.
- The second approach consists of using a uniformly random supersingular elliptic curve as starting curve. Such an elliptic curve can be generated by using the CGL hash function to hash a long nothing-up-my-sleeve string. We then take k_m and k_r so that existing algorithms to compute an endomorphism of given degree cannot be used to efficiently compute an endomorphism of degree $\ell^{2(k_m+k_r)}$. We obtain a computationally binding and computationally hiding commitment scheme.

We stress that going from messages of arbitrary size (as it is the case in [33]) to messages of bounded size does not have a significant impact on protocols using commitment schemes. In fact, even the Pedersen commitment [28] uses $\mathbb{Z}/q\mathbb{Z}$ as message space, for some prime q. This is also the case in bit-commitment[15] used in electronic vote [16] and coin flipping [6]. Moreover, the definition of commitment scheme given in [14] consider the message space to be a finite set.

The rest of the paper is structured as follows: In Section 2, we give some preliminaries on commitment schemes, isogenies and quaternion algebras; and we describe the CGL hash function. Sterner's commitment scheme is presented in Section 3. In Section 4, we present the first approach of our construction and in Section 5 we discuss the smallest ℓ-power degree endomorphism that can be efficiently computed, together with the second approach. We conclude the paper in Section 6.

2 Commitment Schemes, Isogenies and Quaternion Algebras

In this section, we recall some background about commitment schemes, elliptic curves and isogenies.

2.1 Commitment Schemes

A commitment scheme consists of two probabilistic polynomial-time algorithms **KeyGen** and **Commit** and a deterministic polynomial-time algorithm **Open** described as follows.

- **KeyGen**(1^λ) takes the security parameter as input and outputs the public parameters pp needed for the protocol, as well as the message space $\mathcal{M}$.
- **Commit**(pp, m, r) : Given the public parameters pp, a message $m \in \mathcal{M}$ and a uniformly random string r sampled from a space $\mathcal{R}$, outputs a value c which is the commitment to m.
- **Open**(pp, m, r, c): Given the public parameters pp, a message m, a string r and a value c, verifies if c is a valid commitment for m and r. It returns a boolean $b \in \{0, 1\}$.

The hiding and the binding properties are modeled by the following games.

```
Hidinggame_b(A)
$\mathsf{pp} \leftarrow \mathbf{KeyGen}(1^\lambda)$
$(\mathsf{m_0}, \mathsf{m_1}) \leftarrow \mathcal{A}(\mathsf{pp})$
$\mathsf{r} \xleftarrow{\$} \mathcal{R}$
$\mathsf{c} \leftarrow \mathbf{Commit}(\mathsf{pp}, \mathsf{m_b}, \mathsf{r})$
$b' \leftarrow \mathcal{A}(\mathsf{c})$
return $b'$
```

```
Bindinggame(A)
$\mathsf{pp} \leftarrow \mathbf{KeyGen}(1^\lambda)$
$(\mathsf{m}, \mathsf{r}, \mathsf{m}', \mathsf{r}', \mathsf{c}) \leftarrow \mathcal{A}(\mathsf{pp})$
return $(\mathsf{m} \neq \mathsf{m}')\&(\mathbf{Open}(\mathsf{pp}, \mathsf{m}, \mathsf{c}, \mathsf{r}) == (\mathsf{pp}, \mathsf{m}', \mathsf{c}, \mathsf{r}') == 1)$
```

The hiding game is modelled like an indistinguishability game. An adversary chooses two distinct messages m_0 and m_1 and submits to an oracle. In the $\mathsf{Hidinggame_0}$, one commits to m_0 while in the game $\mathsf{Hidinggame_1}$ one commits to m_1. The adversary wins the game if it can correctly guess in which game he is ($\mathsf{Hidinggame_0}$ or $\mathsf{Hidinggame_1}$). In the binding game, the adversary wins if it can find two distinct messages from the message space with the same commitment.

For the security analysis, we use the following definition of negligible function from [23].

Definition 1. *A function $\varepsilon : \mathbb{N} \to [0, 1]$ is negligible if for all $c \geq 0$, there exists $k_c \geq 0$ such that $\varepsilon(k) < \frac{1}{k^c}$ for all $k > k_c$.*

The security of a commitment scheme depends on the ability of an adversary to win the hiding game or the binding game. This ability is evaluated using its advantage against these games.

Definition 2. *Let $\mathcal{C}$ be a commitment scheme and λ a security parameter. The hiding advantage and the binding advantage for an adversary $\mathcal{A}$, are respectively defined by*

$$Adv_{\mathcal{C}}^{hid}(\mathcal{A}) = |\mathsf{Pr}\,(\mathsf{Hidinggame_1}\ \textit{returns}\ 1) - \mathsf{Pr}(\mathsf{Hidinggame_0}\ \textit{returns}\ 1)|$$

and

$$Adv_{\mathcal{C}}^{bind}(\mathcal{A}) = Pr[\mathcal{A}\ \textit{wins the binding game}].$$

We say that $\mathcal{C}$ is information-theoretically (resp. computationally) hiding *if for all adversary (resp. PPT adversary) $\mathcal{A}$, there is a negligible function negl, such that $Adv_{\mathcal{C}}^{hid}(\mathcal{A}) \leq negl(\lambda)$. Furthermore, $\mathcal{C}$ has* perfect hiding *if $Adv_{\mathcal{C}}^{hid}(\mathcal{A}) = 0$ for any adversary.*

The *information-theoretical binding*, the *computational binding* and the *perfect binding* are defined similarly, replacing $Adv_{\mathcal{C}}^{hid}(\mathcal{A})$ by $Adv_{\mathcal{C}}^{bind}(\mathcal{A})$.

A black box way to build a commitment scheme is to use a hash function as follows. Let $H : \{0,1\}^* \to \{0,1\}^t$ be a hash function. For a given message m, the algorithm **Commit** returns $c = H(m||r)$ where r is a random string. In the opening phase, the message m is reveled together with the string r. The algorithm **Open** consists to verify if $c = H(m||r)$ holds. The isogeny based construction [33] follows this idea, using the CGL hash function, an isogeny based hash function introduced by Charles, Goren and Lauter [9]. To understand the isogeny based commitment scheme, we give a little background on isogenies.

2.2 Elliptic Curves and Isogenies

In this section, we recall some useful notions on elliptic curves and isogenies. Any interested reader can refer to Silverman's book [32] or Washington's book [36] for more details.

Definition 3. *Let K be a field. An elliptic curve defined over K is a projective regular algebraic curve of genus one defined over K.*

Any elliptic curve defined over K has a Weierstrass affine equation $E : y^2+a_1xy+a_3y = x^3 + a_2x^2 + a_4x + a_6$. If the characteristic of K is different from 2 and 3, then this equation can be reduced to an equation of the form $y^2 = x^3 + b_4x + b_6$ with $\Delta(E) = 4b_4^3 + 27b_6^2 \neq 0$. The *$j$-invariant* of a curve $E : y^2 = x^3 + b_4x + b_6$ is defined by $j(E) = 1728\frac{4b_4^3}{4b_4^3+27b_6^2} = 1728\frac{4b_4^3}{\Delta(E)}$, and characterizes the isomorphism class of E. This means that any other elliptic curve isomorphic to E has the same j-invariant. Any elliptic curve has an abelian group structure. Any rational map which preserves the group structure of elliptic curves is called isogeny. More formally, we have the following definition.

Definition 4. *Let E and E' be two elliptic curves. An isogeny between E and E' is a rational map $\varphi : E \to E'$ such that $\varphi(O_E) = O_{E'}$.*

Any isogeny $\varphi : E \to E'$ is a group homomorphism and is defined by $\varphi(x, y) = \left(\frac{u_1(x)}{v_1(x)}, y\frac{u_2(x)}{v_2(x)}\right)$. This formulation allows us to define the degree of an isogeny.

Definition 5. *Let $\varphi : E \to E'$ be an isogeny defined by $\varphi(x, y) = \left(\frac{u_1(x)}{v_1(x)}, y\frac{u_2(x)}{v_2(x)}\right)$ where $u_1(x)$ and $v_1(x)$ are co-prime polynomials. The degree of φ is the integer $deg(\varphi) = \max\{deg(u_1), deg(v_1)\}$. If the derivative $\left(\frac{u_1}{v_1}\right)'(x)$ is not identically 0, we say that φ is* separable.

For any isogeny $\varphi : E \rightarrow E'$, there is a unique isogeny (up to isomorphism) $\bar{\varphi} : E' \rightarrow E$, the dual isogeny of φ, such that $\varphi \circ \bar{\varphi} = [deg(\varphi)]$ and $\bar{\varphi} \circ \varphi = [deg(\varphi)]$, where $[deg(\varphi)]$ denotes the multiplication by $deg(\varphi)$. When φ is a separable as it will be the case in this article, we have $deg(\varphi) = \#Ker\,\varphi$. The kernel of any isogeny $\varphi : E \rightarrow E'$ is a finite subgroup of E. Conversely, given a finite subgroup G of an elliptic curve E, there exists a unique isogeny (up to composition by an isomorphism) of kernel G. This isogeny can be computed and evaluated using Vélu's formulas [34]. We denote the codomain curve of this isogeny by E/G. Two isogenies with a same domain are said to be equivalent if they have the same kernel. This implies that they have isomorphic codomains. If an isogeny φ is decomposed as $\varphi = \varphi_1 \circ \varphi_2$, then we have $deg(\varphi) = deg(\varphi_1)deg(\varphi_2)$. Hence, for a prime ℓ, an isogeny of degree ℓ^e can be viewed as a sequence of e isogenies of degree ℓ. Such a sequence of is a path in the ℓ-isogeny graph.

Definition 6. *Let p an ℓ be two distinct primes. The ℓ-isogeny graphs in characteristic p is the graph whose vertices are isomorphism classes of elliptic curves defined over the algebraic closure $\bar{\mathbb{F}_p}$ of the field $\mathbb{F}_p$ and edges are equivalence classes of isogenies of degree ℓ defined over $\bar{\mathbb{F}_p}$.*

The vertices of the ℓ-isogeny graph are labeled by j-invariants of elliptic curves. Given a prime p, the ℓ-isogeny graph in characteristic p has two sub-graphs, the sub-graph of which vertices are isomorphism classes of supersingular elliptic curves and that of which vertices are isomorphism classes of ordinary elliptic curves. The first sub-graph is a component called the *supersingular ℓ-isogeny graph* and denoted by $G_\ell(p)$. In characteristic p, the j-invariant of any supersingular elliptic curve (supersingular j-invariant for short) is an element of $\mathbb{F}_{p^2}$. The nature of an elliptic curve (ordinary or supersingular) is given by the structure of its endomorphism ring.

Given an elliptic curve E, an endomorphism of E is an isogeny from E to E. Such isogenies form a ring $End(E)$, where multiplication is the natural maps composition. When E is defined over a field of characteristic p, E is said to be ordinary if $End(E)$ is isomorphic to an order in an imaginary quadratic field, and supersingular if $End(E)$ is isomorphic to a maximal order in the quaternion algebras $\mathcal{B}_{p,\infty}$ ramified at p and ∞.

2.3 Quaternion Algebra

In this section, we present a little background on quaternion algebras that will allow us to understand the computation of endomorphisms of supersingular elliptic curves in Section 5.1. For more details about this notion, the reader can refer to John Voight's book [35].

Definition 7. *A quaternion algebra over a field K is a K-algebra of which the underlying K-vector space is generated by $\{1, i, j, k\}$ where i, j and k satisfy $i^2 = a$; $j^2 = b$ and $k = ij = -ji$ for some $a, b \in K\backslash\{0\}$. Such quaternion algebra is noted by $\left(\frac{a,b}{K}\right)$.*

In this paper, we are interested in quaternion algebras over $\mathbb{Q}$. Let p be a prime. We denote by $\mathcal{B}_{p,\infty}$ the quaternion algebra ramified [4] only at p and ∞, which is defined by

$$\mathcal{B}_{p,\infty} = \left(\frac{-q, -p}{\mathbb{Q}}\right)$$

where q is in $\{1, 2\}$ or is a prime congruent to 3 modulo 4. One defines the norm and trace of a quaternion $x = x_1 + ix_2 + jx_3 + kx_4$ by $\mathrm{Nrd}(x) = x\bar{x}$ and $\mathrm{Trd}(x) = x + \bar{x}$ respectively, where $\bar{x} = x_1 - (ix_2 + jx_3 + kx_4)$ is the conjugate of x.

The principal link between supersingular elliptic curves and quaternion algebras is that the endomorphism ring of any supersingular elliptic curve defined over a field of characteristic p is isomorphic to a maximal order in $\mathcal{B}_{p,\infty}$. Conversely, any maximal order in $\mathcal{B}_{p,\infty}$ is isomorphic to the endomorphism ring of a supersingular elliptic curve.

Definition 8. *An order in $\mathcal{B}_{p,\infty}$ is a $\mathbb{Z}$-sub module $\mathcal{O}$ of $\mathcal{B}_{p,\infty}$ such that $\mathcal{O} \otimes \mathbb{Q} = \mathcal{B}_{p,\infty}$. $\mathcal{O}$ is said to be maximal if it is not contained in another order.*

Using the correspondence between maximal orders in $\mathcal{B}_{p,\infty}$ and endomorphism ring of supersingular elliptic curves, the degree of an endomorphism corresponds to the norm of the associated quaternion. Hence, finding an endomorphism of E of degree d is equivalent to finding a quaternion of norm d in the maximal order of $\mathcal{B}_{p,\infty}$ isomorphic to $End(E)$. Now we describe the CGL hash function.

2.4 Supersingular ℓ-isogeny Graph and CGL Hash Function

In characteristic p, the number of supersingular j-invariants is $N_p = \left[\frac{p}{12}\right] + \epsilon$, where $\epsilon \in \{0, 1, 2\}$.

Let $\ell \neq p$ be a prime. The graph $G_\ell(p)$ is a connected $(\ell + 1)$-regular graph, with the Ramanujan property[30]. It is an example of expander graph which can be used to build a hash function [9]. This hash function is constructed as follows.
Setup:

- Fix a prime p and a starting supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$;
- Fix a small prime $\ell \neq p$ and a point $P_0 \in E[\ell]$ of order ℓ, where $E[\ell]$ is the ℓ-torsion subgroup of E;
- Define a canonical order in the set of points of order ℓ in any supersingular elliptic curve;
- The message space is $\mathcal{M} = \{0, 1, \ldots, \ell - 1\}^*$.

Hashing:
Let $m = (m_1, \ldots, m_k) \in \mathcal{M}$.

1. Set $E_0 = E$;
2. for $i = 1, 2, \ldots, k$

[4] We refer the reader to [35, Chapter 13] for details about ramification place

(a) Avoiding the point P_{i-1}, order the ℓ remaining points of order ℓ and successively label them with the bits from 0 to $\ell - 1$;
(b) Set S_{i-1} to be the point corresponding to m_i and compute the isogeny $\varphi_i : E_{i-1} \to E_i$ of kernel $\langle S_{i-1} \rangle$;
(c) Set $P_i = \varphi_i(P_{i-1}) \in E_i$;

3. Return $j(E_k)$

We denote this algorithm by $\mathsf{CGL}(E, \ell, P_0, m)$. A more efficient algorithm can be found in [19].

We now describe the isogeny-based commitment scheme following Sterner's construction [33].

3 Sterner's Isogeny-based Commitment Scheme

Sterner's isogeny-based commitment scheme is described as follows.

KeyGen(1^λ) : Given a security parameter λ, fix a prime p of bit length depending on λ; a small prime ℓ; a positive integer k_r and a supersingular elliptic curve $E/\mathbb{F}_{p^2}$, together with a point $P_0 \in E[\ell]$ of order ℓ. The public parameters are $\mathsf{pp} := \{p, \ell, E, k_r, P_0\}$ and the message space is $\mathcal{M} = \{0, 1, \ldots, \ell - 1\}^*$.

Commit(pp, m, r) : Given the public parameters, a message $m \in \mathcal{M}$ and a random $r \in \{0, 1, \ldots, \ell - 1\}^{k_r}$, return $c = \mathsf{CGL}(E, \ell, P_0, m||r)$.

Open(pp, m, r, c) : Given the public parameters; a message $m \in \mathcal{M}$; a string $r \in \{0, 1, \ldots, \ell - 1\}^{k_r}$ and a commitment c, return 1 if $c = \mathsf{CGL}(E, \ell, P_0, m||r)$ and 0 otherwise.

Remark 9. In the original paper, to commit to a message m, one first computes $E_m = E(\mathsf{CGL}(E, \ell, m))$, followed by $c = \mathsf{CGL}(E_m, \ell, r)$. The paper says that the computations are done in such a way that there is no backtracking. It is not clear how these computations explicitly avoid backtracking. In fact, when one calls the CGL hash function on m, one gets E_m and nothing else. Explicitly avoiding backtracking when computing $c = \mathsf{CGL}(E_m, \ell, r)$ requires the knowledge of the last isogeny step in the computation of $E_m = E(\mathsf{CGL}(E, \ell, m))$. Hence the correct way to proceed is to concatenate the message m and the string r before giving them as inputs to the hash function.

Now we move to the security properties of Sterner's commitment scheme.

3.1 Hiding Property

In the context of the commitment scheme described above, the hiding game involves finding two isogenies $\varphi_0 : E \to E_0$ and $\varphi_1 : E \to E_1$ of ℓ-power degree and a distinguisher $\mathcal{D}$ such that, for a given curve E' computed from a (hidden) random cyclic isogeny $\psi : E_b \to E'$ of degree ℓ^{k_r} such that $\psi \circ \varphi_b$ is a cyclic isogeny for a random $b \in \{0, 1\}$, $\mathcal{D}$ can distinguish which curve has been used as domain of the isogeny ψ. When k_r is such that there exists an isogeny of degree ℓ^{k_r} between any pair of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$, the advantage of any distinguisher is less than $\left(\frac{\ell+1}{2\sqrt{\ell}}\right)^{-k_r}$ [33]. Such value of k_r is formally defined as follows.

Definition 10. *Let G be a d-regular connected graph. The* mixing constant *of G is the smallest value $k_G \in \mathbb{N}$ such that for all $k \geq k_G$, for all pair of vertices (j_1, j_2), there is a path of length k between j_1 and j_2.*

For the ℓ-isogeny graph in characteristic p, we denote the mixing constant by $k_{\ell,p}$. The hiding property of the above commitment scheme is given by the following theorem from [33, Theorem 4.2].

Theorem 11. *Let $\mathcal{C}$ be the isogeny based commitment scheme described above, and k_r the length of the random path used in $\mathcal{C}$. If $k_r \geq k_{\ell,p}$, then $\mathcal{C}$ is information-theoretically hiding.*

By [33, Lemma 3.5], $k_{\ell,p}$ is lower bounded by $\log_\ell\left(\frac{N_p}{\ell+1}\right) + 1$. Hence, we should take $k_r > \log_\ell(p)$ to expect $\mathcal{C}$ to be hiding.

3.2 Binding Property

In the context of the above isogeny based commitment scheme, the binding game involves finding two distinct cyclic isogenies $\varphi_0 : E \rightarrow E_0$ and $\varphi_1 : E \rightarrow E_1$ of ℓ-power degree and two other cyclic isogenies $\psi_0 : E_0 \rightarrow E'$ and $\psi_1 : E_1 \rightarrow E'$ of degree ℓ^{k_r} such that $\psi_0 \circ \varphi_0$ and $\psi_1 \circ \varphi_1$ are cyclic isogenies. This is exactly a collision in the supersingular ℓ-isogeny graph, and is equivalent to finding an endomorphism of E which has ℓ-power degree. This fact is formalized in [33, Theorem 4.6], where the author shows that the scheme $\mathcal{C}$ is computationally binding, assuming the hardness of the following Problem 12.

Problem 12 (Supersingular ℓ-power Endomorphism Problem). Given a prime p, a supersingular elliptic curve E over $\mathbb{F}_{p^2}$ and a small prime ℓ, compute a non-trivial cyclic endomorphism of E whose degree is ℓ^e, where e is a positive integer.

When the endomorphism ring of E is known, solving this problem consists of solving a norm equation in the maximal order $\mathcal{O} \cong End(E)$ of the quaternion algebra $\mathcal{B}_{p,\infty}$. This can be done by [20, Algorithm 13] and [25, Algorithm 8]. So for this commitment scheme to be binding, ideally, we need a starting curve with unknown endomorphism ring. Since all existing efficient methods for constructing a supersingular elliptic curve [8,10] allow the one constructing the curve to recover its endomorphism ring [7,26], one needs a trusted party to generate the starting curve. One method to implement such trusted party is given by [3]. This method involves a multiparty computation, and require a lot of resources to be performed. In this paper, we modify this commitment scheme in such a way that the trusted setup is avoided.

In the original version of the Sterner's scheme presented at the beginning of this Section, the message space is $\mathcal{M} = \{0, 1, \ldots, \ell - 1\}^*$, and the starting curve is required to have a hidden endomorphism ring. The first major modification we bring is that we allow a starting curve of known endomorphism ring. In this situation, we have a binding issue: Knowing the endomorphism ring, one can compute a cycle in $G_\ell(p)$ using [20, Algorithm 13] and [25, Algorithm 8]. In order to fix this issue, we modify the message space: we take $\mathcal{M} = \{0, 1, \ldots, \ell - 1\}^{k_m}$ where k_m is a fixed integer. We then need to take k_m and k_r (the length of the random string) so that an endomorphism of degree lower than $\ell^{2(k_m+k_r)}$ does not exists or is hard to compute. The first approach consists of using as starting curve, the curve $E_6 : y^2 = x^3 + 6x^2 + x$ where endomorphisms of small degree do not exist[5].

4 Committing from the Curve E_6

Here we use the curve $E_6 : y^2 = x^3 + 6x^2 + x$ defined over $\mathbb{F}_{p^2}$ where $p \equiv 15(\text{Mod } 16)$. Contributing to the security analysis of SIDH/SIKE, Onuki [27] investigated on the existence of endomorphism of degree $\ell^e < p$ on this curve.

Theorem 13 ([27]). *Let ℓ be a prime number that does not split in $\mathbb{Z}[\sqrt{-1}]$, $\phi = (\phi_1, \ldots, \phi_n)$ and $\psi = (\psi_1, \ldots, \psi_m)$ two distinct paths of respective lengths n and m from E_6 to the same curve E in $G_\ell(p)$ without backtracking. Then one of the following holds:*

- $\ell^{n+m} \geq \frac{p+1}{16}$;
- $\ell = 2$ *and either* ϕ *or* ψ *has a form* $\phi' \circ \phi_0$ *where* $\phi_0 : E_6 \to E(1728)$ *is of degree* 2 *and* $E(1728)$ *has* j*-invariant* 1728.

It follows that there does not exist a cycle of length less than $\frac{p+1}{16}$ in the ℓ-isogeny graph which begins with E_6 when $\ell \neq 2$. In the case where $\ell = 2$, the first edge of such a cycle is the 2-isogeny whose codomain is the curve of j-invariant 1728. The adjustment of k_m and k_r can then be done so that $\ell^{2(k_m+k_r)} < \frac{p+1}{16}$. We describe the protocol as follows.

4.1 Description of the Commitment Scheme

Our idea is to use the curve E_6 as starting curve, and take k_m and k_r such that $k_m + k_r < \frac{1}{2}\log_\ell(\frac{p+1}{16})$. We designate this scheme by $\mathcal{C}_{k_m,k_r}$ and described it as follows.

KeyGen(1^λ) : Given a security parameter λ, fix a prime $p \equiv 15 \pmod{16}$, two positive integers k_m and k_r (The size of p, k_m and k_r will be given later in Section 4.4). Let ℓ be a small prime equal to 2 or congruent to 3 modulo 4 and $P_0 \in E_6[\ell]$. When $\ell = 2$, the point P_0 is such that $j(E_6/\langle P_0\rangle) = 1728$. The public parameters are $\mathsf{pp} := \{p, \ell, k_m, k_r, E_6, P_0\}$ and the message space is $\mathcal{M} = \{0, 1, \ldots, \ell - 1\}^{k_m}$.

Commit(pp, m, r) : Given the public parameters, a message $m \in \mathcal{M}$ and a random $r \in \{0, 1, \ldots, \ell - 1\}^{k_r}$, return $c = \mathsf{CGL}(E_6, \ell, P_0, m||r)$.

[5] Such an endomorphism exists, but can be easily avoided in our setting

Open(pp, m, r, c) : Given the public parameters, a message $m \in \mathcal{M}$, $r \in \{0, 1, \ldots, \ell - 1\}^{k_r}$ and a commitment c, return $c == \mathsf{CGL}(E_6, \ell, P_0, m||r)$.

For the rest of this section, p is a prime congruent to 15 modulo 16 and ℓ is a small prime equal to 2 or congruent to 3 modulo 4. We now analyse the security properties of the new commitment scheme.

4.2 Binding Property

Our scheme is constructed to be perfectly binding. In fact, since $k_m + k_r < \frac{1}{2}\log_\ell(\frac{p+1}{16})$, Theorem 13 shows that the only cycles starting from E_6 and of length smaller than $\log_\ell(\frac{p+1}{16})$ have the isogeny $E_6 \to E(1728) = E_6/\langle P_0 \rangle$ as their first step. Since this isogeny is never the first step in the computation of the commitment $c = \mathsf{CGL}(E_6, \ell, P_0, m||r)$, then there exists no distinct messages $m_0, m_1 \in \mathcal{M}$, no random strings $r_0, r_1 \in \{0, 1, \ldots, \ell - 1\}^{k_r}$ such that $\mathsf{CGL}(E_6, \ell, P_0, m_0||r_0) = \mathsf{CGL}(E_6, \ell, P_0, m_1||r_1)$. Meaning that $\mathcal{C}_{k_m,k_r}$ is perfectly binding by design. In the next paragraph, we discuss the hiding property.

4.3 Hiding Property

Since the mixing constant of ℓ-isogeny graph is lower bounded by $\log_\ell(N_p) - \log_\ell(\ell + 1) + 1$ [33, Lemma 3.5], we have $k_r < k_{\ell,p}$, which does not satisfy the conditions of Theorem 11. Moreover, considering the context of the hiding game, if c is the commitment for a message m_b following the scheme in Section 4.1, the probability to be the commitment of m_{1-b} is 0. This is justified by Lemma 14, where we consider the following set for each tuple (d, E, ψ) where d is a positive integer and $\psi : E_6 \to E$ is a cyclic isogeny.

$$\mathsf{Isog}_d(E, \psi) = \left\{ \begin{array}{c} j(E'/\mathbb{F}_{p^2});\ \text{there exist a cyclic isogeny } \phi : E \to E' \text{ of degree } d \\ \text{such that } \phi \circ \psi \text{ is a cyclic isogeny} \end{array} \right\}.$$

Lemma 14. *Let $\varphi_0 : E_6 \to E_0$ and $\varphi_1 : E_6 \to E_1$ be two non equivalent cyclic isogenies of degree ℓ^{k_m} and let k_r be an integer such that $k_m + k_r < \frac{1}{2}\log_\ell(\frac{p+1}{16})$. Then $\mathsf{Isog}_{\ell^{k_r}}(E_0, \varphi_0) \cap \mathsf{Isog}_{\ell^{k_r}}(E_1, \varphi_1) = \emptyset$ in the following cases:*

1. $\ell \neq 2$
2. $\ell = 2$ *and neither φ_0 nor φ_1 is a path containing the curve of j-invariant* 1728*;*

Proof. Let us suppose that $\mathsf{Isog}_{\ell^{k_r}}(E_0, \varphi_0) \cap \mathsf{Isog}_{\ell^{k_r}}(E_1, \varphi_1) \neq \emptyset$, and let E such that $j(E) \in \mathsf{Isog}_{\ell^{k_r}}(E_0, \varphi_0) \cap \mathsf{Isog}_{\ell^{k_r}}(E_1, \varphi_1)$. Then there exists two cyclic isogenies $\psi_0 : E_0 \to E$ and $\psi_1 : E_1 \to E$ of degree ℓ^{k_r} such that $\psi_0 \circ \varphi_0$ and $\psi_1 \circ \varphi_1$ are cyclic isogenies. We then have two distinct paths $\psi_0 \circ \varphi_0 : E_6 \to E$ and $\psi_1 \circ \varphi_1 : E_6 \to E$ in the ℓ-isogeny graph, both of length $k_m + k_r$. This contradicts Theorem 13, since $\ell^{2(k_m+k_r)} < \frac{p+1}{16}$.

Hence our scheme is not information theoretically hiding. We prove that our scheme is computationally hiding assuming that Problem 15 is hard.

Problem 15. Let $k_m, k_r \in \mathbb{N}^*$ such that $k_m + k_r < \frac{1}{2}\log_\ell(\frac{p+1}{16})$. Find two cyclic isogenies $\varphi_0 : E_6 \to E_0$ and $\varphi_1 : E_6 \to E_1$ of degree ℓ^{k_m} and a PPT distinguisher which distinguishes between the following distributions:

1. $E' \in \mathsf{Isog}_{\ell^{k_r}}(E_0, \varphi_0)$;
2. $E' \in \mathsf{Isog}_{\ell^{k_r}}(E_1, \varphi_1)$.

Theorem 16. *The scheme $\mathcal{C}_{k_m,k_r}$ is computationally hiding under the hardness of Problem 15.*

Proof. Let $\mathcal{A} = (A_1, A_2)$ be a polynomial time adversary against the hiding game, described as follows: A_1 returns two massages m_0 and m_1. After a uniformly random one of the two messages has been committed to, A_2 takes the commitment and distinguishes which of them has been committed to.

We describe an adversary $\mathcal{A}'$ for Problem 15 as follows: $\mathcal{A}'$ queries $\mathcal{A}$ to obtain the two messages m_0, m_1 returned by A_1 and computes the corresponding isogenies $\varphi_0 : E_6 \to E_0$ and $\varphi_1 : E_6 \to E_1$. Afterward, uses the distinguisher A_2 to obtain b such that m_b has been committed to. $\mathcal{A}'$ returns the distribution $E' \in \mathsf{Isog}_{\ell^{k_r}}(E_b, \varphi_b)$. $\mathcal{A}'$ has the same success probability as $\mathcal{A}$.

Given two curves E_0 and E_1, to the best of our knowledge the best approach to distinguish among the distributions in Problem 15 is the strategy which consists of trying to compute an isogeny $E_b \to E'$ of degree ℓ^{k_r} using vOW algorithm [12], for each $b \in \{0, 1\}$. This approach has running time of $O(\frac{N^{3/2}}{w^{1/2}m})$, where w is the size of the memory, m is the number of processors and $N = (\ell+1)\ell^{k_r/2-1} \approx \ell^{k_r/2}$[1]. So for our scheme to be secured, we need to carefully choose k_r, according to ℓ and the security parameter λ. In the following section, we provide further details for the parameters selection.

4.4 Concrete Setup

The analysis of vOW [1] allows us to suggest some values for k_r, according to some security parameters λ. We summarize these values in Table 1. For any security level, the length k_m is such that $k_m + k_r = \lfloor \frac{1}{2}\log_\ell(\frac{p+1}{16})\rfloor$. For giving the size of p as function of λ, we consider the MIM attack [1] instead of vOW attack. Then we need $k_r = 2\lambda$. Taking $k_m \approx n\lambda$ for some rational n, we need a prime p such that $\log_\ell(p+1) \approx 2(n+2)\lambda + \log_\ell(16)$.

λ	128		160		192	
ℓ	2	3	2	3	2	3
k_r	216	137	273	172	305	192

Table 1. Some secure values for k_r

We hence get rid of the trusted setup, but at the cost of having a prime whose size is linear in the size of the messages. In the original scheme [33], the size of the prime is 2λ. The relatively large size of p in our variant is due to the smallness of the upper bound $\log_\ell(\frac{p+1}{16})$. In the next section, we suggest a more compact variant of our construction, which instead of aiming for perfectly binding commitment scheme, goes for computationally binding one by using a uniformly random supersingular curve (of non secret endomorphism ring) as starting curve.

5 Committing from a Uniformly Random Supersingular Curve

This approach is similar to that presented in Section 4.1. The difference is that we use a publicly generated uniformly random supersingular curve, and we exploit lower bounds on the degree of prime power degree endomorphisms that can be efficiently computed.

5.1 Computing short ℓ-power Degree Endomorphisms

In this section, our goal is to discuss the shortest ℓ-power degree endomorphism that can be efficiently computed using existing algorithms. Our motivation comes from the fact that the commitment scheme $\mathcal{C}_{k_m,k_r}$ in Section 4 requires k_m and k_r such that $k_m + k_r < \frac{1}{2}\log_\ell\left(\frac{p+1}{16}\right)$, in order to avoiding the existence of endomorphisms of degree $\ell^{2(k_m+k_r)}$ in the starting curve. The smallness of the upper bound $\frac{1}{2}\log_\ell\left(\frac{p+1}{16}\right)$ leads to a relatively large size of p. In order to increase this upper bound (and then reduce the size of p), we allow the existence of endomorphism of degree $\ell^{2(k_m+k_r)}$, but ensure that these endomorphisms are hard to compute.

We recall that computing an endomorphism of a curve E of degree d implies solving a norm equation in a maximal order which is isomorphic to the endomorphism ring of E. The method for solving the norm equation in maximal order depends on whether the order is a special extremal order [24] or not. A part of the following discussion about special extremal orders is already done in [2] for slightly different purpose.

Let $\mathcal{B}_{p,\infty} = \left(\frac{-q,-p}{\mathbb{Q}}\right) = \mathbb{Q} + i\mathbb{Q} + j\mathbb{Q} + k\mathbb{Q}$ be the quaternion algebra ramified at p and ∞, where $i^2 = -q,\ j^2 = -p$ and $ij = -ji = k$. A special p-extremal maximal order [24] is a maximal order containing j. Examples of p-extremal maximal orders are those containing $\mathbb{Z}\langle i,j\rangle = \mathbb{Z} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ as subring. For such a maximal order $\mathcal{O}$, if $R = \mathcal{O} \cap \mathbb{Q}[i] = \mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{Q}[i]$, then the restriction of the norm to $R + Rj$ is given by

$$\mathrm{Nrd}(x_1 + y_1\omega + (x_2 + y_2\omega)j) = f(x_1,y_1) + pf(x_2,y_2),$$

where f is a principal quadratic form of same discriminant as R [24]. We have

$$f(x,y) = x^2 + \mathrm{Trd}(\omega)xy + \mathrm{Nrd}(\omega)y^2.$$

In the following example, for several congruence classes of p, we exhibit the quaternion algebra $\mathcal{B}_{p,\infty}$, a special p-extremal order $\mathcal{O}$, the corresponding quadratic ring R and the form of $f(x, y)$.

Example 17. 1. For $p \equiv 3 \bmod 4$: $\mathcal{B}_{p,\infty} = \left(\frac{-1,-p}{\mathbb{Q}}\right)$; $\mathcal{O} = \langle 1, i, \frac{1+k}{2}, \frac{i+j}{2} \rangle$; $R = \mathbb{Z}[i]$;

$$f(x, y) = x^2 + y^2$$

.

2. For $p \equiv 5 \bmod 8$: $\mathcal{B}_{p,\infty} = \left(\frac{-2,-p}{\mathbb{Q}}\right)$; $\mathcal{O} = \langle 1, i, \frac{1+j+k}{2}, \frac{i+2j+k}{4} \rangle$; $R = \mathbb{Z}[i]$;

$$f(x, y) = x^2 + 2y^2$$

.

3. For $p \equiv 1 \bmod 4$: $\mathcal{B}_{p,\infty} = \left(\frac{-q,-p}{\mathbb{Q}}\right)$, where $q \equiv 3 \bmod 4$ is a prime such that $\left(\frac{-p}{q}\right) = 1$; $\mathcal{O} = \langle 1, \frac{1+i}{2}, j, \frac{ci+k}{q} \rangle$, where $c^2 \equiv -p \bmod q$; $R = \mathbb{Z}[\frac{1+i}{2}]$;

$$f(x, y) = x^2 - xy + \frac{1+q}{4}y^2$$

.

Any curve whose endomorphism ring is isomorphic to one of p-extremal maximal orders given in Example 17 is said to be special. For such a curve, the best method to find an endomorphism of ℓ-power degree consists of solving the equation

$$f(x, y) + pf(z, t) = \ell^e$$

for some e. Algorithm 13 in [20] consists of taking e large enough so that the quantity $\ell^e - pf(z, t)$ is positive for sufficiently many pairs (z, t) and the equation

$$f(x, y) = \ell^e - pf(z, t)$$

can be solved by Cornacchia's algorithm [11]. When ℓ is split in R, this equation may have a solution for $z = t = 0$ and[6]. When ℓ is not split in R, this equation does not have a solution for $\ell^e < p$. The solution returned by [20, Algorithm 13] is such that $\ell^e \approx p^2$.

For a random curve of known endomorphism ring isomorphic to $\mathcal{O}$, we don't have a nice norm form as in the above case. So it is not clear how to use the same approach to solve the norm equation. The method given by [25, Algotithm 8, Page 75] consists of solving the norm equation in the Einsler order $\mathcal{O}_0 \cap \mathcal{O}$, where $\mathcal{O}_0$ is one of extremal orders given in Example 17. From [18, Proposition 1], we have $\mathcal{O}_0 \cap \mathcal{O} = \mathbb{Z} + I$ where I is an ideal connecting $\mathcal{O}_0$ and $\mathcal{O}$. One can always choose the idea I such that its norm is prime [24]. Let $N = Nrd(I)$ be prime. One computes $\mu \in \mathbb{Z} + I$ of ℓ-power norm as follows:

[6] This may not be the case. The probability that this holds is $\frac{1}{h_{\Delta_\omega}}$, where h_{Δ_ω} is the class number of R.

1. Compute $(C : D) \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ such that $\mu_0 = (C + \omega D)j \in \mathbb{Z} + I$;
2. Compute $\lambda \in \mathbb{Z}/N\mathbb{Z}$ and $\mu_1 \in \mathcal{O}_0$ such that $\mu = \frac{1}{2}(\lambda\mu_0 + N\mu_1)$ is of norm ℓ^e for some $e \in \mathbb{N}$.

The existence of $(C : D)$ in Step 1 can be justified by [25, Proposition 3.3.1].

The idea in Step 2 is to find μ_1 of the form $\mu_1 = x + y\omega + (z + t\omega)j \in R + Rj$. We then have $\mu = \frac{1}{2}\left[N(x + y\omega) + (Nz + \lambda C + (Nt + \lambda D)\omega)j\right]$ and $Nrd(\mu) = \ell^e$ is equivalent to

$$\frac{1}{4}\left[N^2 f(x,y) + pf(Nz + \lambda C; Nt + \lambda D)\right] = \ell^e. \tag{1}$$

Modulo N, we have $p\lambda^2 f(C,D) = 4\ell^e$. Since ℓ is a quadratic non-residue modulo N, we can adjust the parity of e so that $\left(\frac{pf(C,D)}{N}\right) = \left(\frac{4\ell^e}{N}\right)$ and take

$$\lambda = \sqrt{\frac{4\ell^e}{pf(C,D)}} (\text{mod } N).$$

Equation 1 is equivalent to

$$f(x,y) = \frac{4\ell^e - pf(Nz + \lambda C; Nt + \lambda D)}{N^2} \tag{2}$$

Using the optimisation strategy presented in [29], this equation can be solved by choosing e such that $4\ell^e \approx pN^3\sqrt{\Delta_{\mathbb{Q}(\omega)}}$. Since N is slightly greater than $\sqrt{p}$, ℓ^e is slightly greater than $p^{\frac{5}{2}}$. If we could generate many pairs $(C : D)$, we could use the strategy in [2, Section 4.1] to have a superpolynomial time version of this algorithm where the lower bound $p^{\frac{5}{2}}$ is reduced to $p^{\frac{5}{2}-\epsilon}$ with running time in $O(N^\epsilon)$ where N^ϵ is the number of pairs $(C : D)$ generated. However, the pair (C, D) given by [25, Proposition 3.3.1] is unique up to scalar multiplication, according to [25, Proposition 2.3.12]. So $p^{\frac{5}{2}}$ (as found in [25]) is the lower bound on the degrees of endomorphisms that can be efficiently computed, assuming the supersingular curve in play was generated uniformly at random.

Recently, some improvements [4,22] have been made on algorithms to find isogenies of fixed degree between supersingular elliptic curves E_1 and E_2. The algorithm given in [22] improves that given in [4]. More precisely, given two maximal orders $\mathcal{O}_1$ and $\mathcal{O}_2$ in $\mathcal{B}_{p,\infty}$, Algorithm 5 in [22] allows to compute an ideal of any norm d connecting $\mathcal{O}_1$ and $\mathcal{O}_2$, assuming that such an ideal exists. This algorithm runs in time $O(\sqrt{Nrd(\beta_1)Nrd(\gamma_1)})$ where $\beta_1 \in \mathcal{O}_1$ and $\gamma_1 \in \mathcal{O}_2$ are the smallest (in terms of norm) non scalar endomorphisms of E_1 and E_2 respectively. For a generic maximal order $\mathcal{O}$, the norm of the smallest elements in $\mathcal{O}$ is upper-bounded by $O(p^{2/3})$ [22]. Hence the expected running time of this algorithm is $O(p^{2/3})$ when both maximal orders are generic, and $O(p^{1/3})$ when either $\mathcal{O}_1$ or $\mathcal{O}_2$ is one of the extremal maximal orders in Example 17. This algorithm could be used to find an endomorphisms of given degree d on a curve E of known endomorphism ring $\mathcal{O}$ by setting $\mathcal{O}_1 = \mathcal{O}_2 = \mathcal{O}$. We note that, if β is a non scalar endomorphism of smallest norm in $\mathcal{O}$, this algorithm cannot return a non scalar endomorphism if $d < Nrd(\beta)$. When $\mathcal{O}$ is one of the above extremal maximal orders, this method runs in polynomial time and can return an endomorphism of any degree when it exists.

A more efficient method could be to use Algorithm 3 in [22], which allows to compute an endomorphism of given trace and degree if such an endomorphism exists in $\mathcal{O}$. One could exploit this algorithm by picking a random trace t and finding an endomorphism of our given norm d and trace t. The resulting algorithm has expected running time $O(\sqrt{Nrd(\beta)}.polylog(dp))$.

Another way for computing a degree ℓ^e endomorphism of a curve E could be as follows, assuming that its endomorphism ring $End(E) \cong \mathcal{O}$ is known.

1. Compute an isogeny $\phi : E \to E'$ of degree $\ell^{e/2}$;
2. Compute the endomorphism ring $\mathcal{O}'$ of E';
3. Use Algorithm 5 in [22] to compute an ideal I of norm $\ell^{e/2}$ connecting $\mathcal{O}$ to $\mathcal{O}'$;
4. Compute the isogeny ϕ_I of kernel ideal I;
5. If ϕ_I is equivalent to ϕ then go back to 2 and consider a maximal order $\mathcal{O}''$ conjugated to $\mathcal{O}'$ that is not isomorphic to $End(E'^p)$;
6. Return $\alpha = \bar{\phi} \circ \phi_I$.

If E is a randomly generated curve, this approach has expected exponential running time as Algorithm 5 in [22] runs in expected time $O(p^{3/2})$. Furthermore, the loop in this algorithm might not stop. For example if $E = E_6$ as defined in Section 4 and $\ell^e < \frac{p+1}{16}$, there is no non equivalent isogeny to ϕ if ϕ corresponds to a path whose the first edge does not connect E_6 to $E(1728)$.

According to the above discussion, we can use a generic curve with no small endomorphism for our protocol. The obtained variant is described as follows.

5.2 Description of the Scheme

The scheme $\mathcal{C}_{k_m,k_r}$ described in Section 4 uses the curve $E_6 : y^2 = x^3+6x^2+x$ as starting curve. The message space is $\{0, 1, \ldots, \ell-1\}^{k_m}$ and the space of random messages is $\{0, 1, \ldots, \ell-1\}^{k_r}$, where $k_m + k_r = \lfloor \frac{1}{2} \log_\ell \left(\frac{p+1}{16}\right) \rfloor$. In this Section, we bring the following modification to this scheme.

- The starting curve E is a uniformly random supersingular elliptic curve with no endomorphism of small degree. Such an elliptic curve can be generated by using the CGL hash function to hash a long nothing-up-my-sleeve string. To verify that the curve E has no endomorphism of small degree, one can compute a Minkowski reduced basis of $End(E)$.
- The message space and the space of random strings are unchanged, but values of k_m and k_r are such that $2(k_m + k_r) = \lfloor 2\log_\ell(p) \rfloor$.

Apart form these modifications, everything else is unchanged (see Section 4.1). We designate this new variant by $\mathcal{C}_{k_m,k_r}(E)$. We now provide security arguments for this variant.

5.3 Binding Property

For the binding property of $\mathcal{C}_{k_m,k_r}(E)$, we have the following problem which is a variant of Problem 12.

Problem 18. Given a prime p, a uniformly random supersingular elliptic curve E defined over $\mathbb{F}_{p^2}$, a small prime ℓ and a positive fixed integer $e \leq 2\log_\ell(p)$, compute a cyclic endomorphism of E which has degree ℓ^e.

Theorem 19. *The commitment scheme $\mathcal{C}_{k_m,k_r}(E)$ is computationally binding, assuming the hardness of Problem 18.*

The proof of the above theorem is straightforward. Following the discussion in Section 5.1, existing efficient algorithms for computing an endomorphism of ℓ-power degree can not return an endomorphism whose degree is smaller than $p^{\frac{5}{2}}$. So to the best of our knowledge, there is no known efficient algorithm for solving Problem 18.

5.4 Hiding Property

For the hiding property, we introduce the following problem.

Problem 20. Let E be a random supersingular elliptic curve and $k_m, k_r \in \mathbb{N}^*$ such that $k_m + k_r = \lfloor \log p \rfloor$. Find two distinct cyclic isogenies $\varphi_0 : E \to E_0$ and $\varphi_1 : E \to E_1$ of degree ℓ^{k_m} and a distinguisher which distinguishes between the following distributions:

1. E' sampled uniformly at random from $\mathsf{Isog}_{\ell^{k_r}}(E_0, \varphi_0)$;
2. E' sampled uniformly at random from $E' \in \mathsf{Isog}_{\ell^{k_r}}(E_1, \varphi_1)$.

Theorem 21. *Let E be a supersingular elliptic curve. The scheme $\mathcal{C}_{k_m,k_r}(E)$ is computationally hiding under the hardness of Problem 20.*

Proof. The proof is similar to that of Theorem 16.

The best known strategy against Problem 20 is the same as that against Problem 15 which consists of trying to compute an isogeny $E_b \to E'$ of degree ℓ^{k_r} using vOW algorithm [12], for each $b \in \{0, 1\}$. We can hence use the values of k_r given in Table 1 to avoid such attacks. Furthermore, taking $k_r = 2\lambda$ and $k_m = n\lambda$ as in Section 4.4, we can use a prime p of size $\log_\ell(p) \approx (n+2)\lambda$, instead of $\log_\ell(p+1) \approx 2(n+2)\lambda + \log_\ell(16)$ as in the previews variant. .

6 Conclusion

In this work, we have investigated the problem of constructing an isogeny based commitment without trusted setup. We have suggested two approaches to solve this problem. These two approaches share the same idea that consists of modifying Sterner's commitment scheme by using a starting curve of known endomorphism ring and a finite set as message space. In the first approach, the starting curve is a curve that does not have endomorphisms of relatively small ℓ-power degree and the size of messages is bounded in such a way that associated isogenies never have the same co-domain, and hence never lead to endomorphisms on the starting curve. Doing so, we obtain a perfectly binding and computationally hiding commitment scheme. However, this approach requires a field of characteristic p significantly larger than that used for the initial scheme. In order to limit the efficiency loss in our first proposal, we suggest a second variant where instead of choosing the starting curve and the degree of the isogenies in such a way that certain endomorphisms do not exist, we choose them in such a way that these endomorphisms may exist but computing them is hard. This leads to a scheme where we half the size of the prime p, compared to our first proposal. We prove that the resulting scheme is computationally hiding and computationally binding.

Acknowledgments. We thank Antonin Leroux for useful discussions about computing an endomorphism of given degree.

References

1. Gora Adj, Daniel Cervantes-Vázquez, Jesús-Javier Chi-Domínguez, Alfred Menezes, and Francisco Rodríguez-Henríquez. On the cost of computing isogenies between supersingular elliptic curves. In Carlos Cid and Michael J. Jacobson Jr., editors, *Selected Areas in Cryptography – SAC 2018*, pages 322–343, Cham, 2019. Springer International Publishing.
2. Andrea Basso, Mingjie Chen, Tako Boris Fouotsa, Péter Kutas, Abel Laval, Laurane Marco, and Gustave Tchoffo Saah. Exploring sidh-based signature parameters. In *International Conference on Applied Cryptography and Network Security*, pages 432–456. Springer, 2024.
3. Andrea Basso, Giulio Codogni, Deirdre Connolly, Luca De Feo, Tako Boris Fouotsa, Guido Maria Lido, Travis Morrison, Lorenz Panny, Sikhar Patranabis, and Benjamin Wesolowski. Supersingular curves you can trust. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 405–437. Springer, 2023.
4. Benjamin Benčina, Péter Kutas, Simon-Philipp Merz, Christophe Petit, Miha Stopar, and Charlotte Weitkämper. Improved algorithms for finding fixed-degree isogenies between supersingular elliptic curves. Cryptology ePrint Archive, Paper 2023/1618, 2023. `https://eprint.iacr.org/2023/1618`.
5. Jean-François Biasse, David Jao, and Anirudh Sankar. A quantum algorithm for computing isogenies between supersingular elliptic curves. In *International Conference on Cryptology in India*, pages 428–442. Springer, 2014.
6. Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *ACM SIGACT News*, 15(1):23–27, 1983.
7. Jeremy Booher, Ross Bowden, Javad Doliskani, Tako Boris Fouotsa, Steven D Galbraith, Sabrina Kunzweiler, Simon-Philipp Merz, Christophe Petit, Benjamin Smith, Katherine E Stange, et al. Failing to hash into supersingular isogeny graphs. *arXiv preprint arXiv:2205.00135*, 2022.
8. Reinier Bröker. Constructing supersingular elliptic curves. *J. Comb. Number Theory*, 1(3):269–273, 2009.

9. Denis X Charles, Kristin E Lauter, and Eyal Z Goren. Cryptographic hash functions from expander graphs. *Journal of CRYPTOLOGY*, 22(1):93–113, 2009.
10. Ilya Chevyrev and Steven D Galbraith. Constructing supersingular elliptic curves with a given endomorphism ring. *LMS Journal of Computation and Mathematics*, 17(A):71–91, 2014.
11. Giuseppe Cornacchia. Su di un metodo per la risoluzione in numeri interi dell'equazione $\sum_{h=0}^{n} c_h x^{n-h} y^h = p$. *Giornale di Matematiche di Battaglini 46, 33–90*, 1908.
12. Craig Costello, Patrick Longa, Michael Naehrig, Joost Renes, and Fernando Virdia. Improved classical cryptanalysis of the computational supersingular isogeny problem. *IACR Cryptol. ePrint Arch.*, 2019:298, 2019.
13. Ronald Cramer, Matthew Franklin, Berry Schoenmakers, and Moti Yung. Multi-authority secret-ballot elections with linear work. In Ueli Maurer, editor, *Advances in Cryptology — EUROCRYPT '96*, pages 72–83, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.
14. Ivan Damgard. Commitment schemes and zero-knowledge protocols. *Lectures on Data Security: Modern Cryptology in Theory and Practice*, 1561:63, 1999.
15. Ivan Bjerre Damgård. On the existence of bit commitment schemes and zero-knowledge proofs. In *Advances in Cryptology—CRYPTO'89 Proceedings 9*, pages 17–27. Springer, 1990.
16. A Darwish and MM El-Gendy. A new cryptographic voting verifiable scheme for e-voting system based on bit commitment and blind signature. *Int J Swarm Intel Evol Comput*, 6(158):2, 2017.
17. Luca De Feo, Samuel Dobson, Steven D. Galbraith, and Lukas Zobernig. Sidh proof of knowledge. In Shweta Agrawal and Dongdai Lin, editors, *Advances in Cryptology – ASIACRYPT 2022*, pages 310–339, Cham, 2022. Springer Nature Switzerland.
18. Luca De Feo, David Kohel, Antonin Leroux, Christophe Petit, and Benjamin Wesolowski. Sqisign: compact post-quantum signatures from quaternions and isogenies. In *Advances in Cryptology–ASIACRYPT 2020: 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7–11, 2020, Proceedings, Part I 26*, pages 64–93. Springer, 2020.
19. Javad Doliskani, Geovandro CCF Pereira, and Paulo SLM Barreto. Faster cryptographic hash function from supersingular isogeny graphs. *Cryptology ePrint Archive*, 2017.
20. Kirsten Eisenträger, Sean Hallgren, Kristin Lauter, Travis Morrison, and Christophe Petit. Supersingular isogeny graphs and endomorphism rings: reductions and solutions. In *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part III 37*, pages 329–368. Springer, 2018.
21. Kirsten Eisenträger, Sean Hallgren, Chris Leonardi, Travis Morrison, and Jennifer Park. Computing endomorphism rings of supersingular elliptic curves and connections to path-finding in isogeny graphs. *Open Book Series*, 4(1):215–232, 2020.
22. Jonathan Komada Eriksen and Antonin Leroux. Computing orientations from the endomorphism ring of supersingular curves and applications. Cryptology ePrint Archive, Paper 2024/146, 2024. `https://eprint.iacr.org/2024/146`.
23. Jonathan Katz. *Digital signatures*, volume 1. Springer, -, 2010.

24. David Kohel, Kristin Lauter, Christophe Petit, and Jean-Pierre Tignol. On the quaternion-isogeny path problem. *LMS Journal of Computation and Mathematics*, 17(A):418–432, 2014.
25. Antonin Leroux. *Quaternion Algebra and isogeny-based cryptography.* PhD thesis, Ecole doctorale de l'Institut Polytechnique de Paris, 2022.
26. Marzio Mula, Nadir Murru, and Federico Pintore. On random sampling of supersingular elliptic curves. Cryptology ePrint Archive, Paper 2022/528, 2022. `https://eprint.iacr.org/2022/528`.
27. Hiroshi Onuki, Yusuke Aikawa, and Tsuyoshi Takagi. The existence of cycles in the supersingular isogeny graphs used in sike. In *2020 International Symposium on Information Theory and Its Applications (ISITA)*, pages 358–362. IEEE, 2020.
28. Torben Pryds Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In Joan Feigenbaum, editor, *Advances in Cryptology — CRYPTO '91*, pages 129–140, Berlin, Heidelberg, 1992. Springer Berlin Heidelberg.
29. C. Petit and S. Smith. An improvement to the quaternion analogue of the '-isogeny problem, 2018. `file:///C:/Users/HP/Downloads/08-50_3.pdf`.
30. Arnold Pizer. An algorithm for computing modular forms on $\gamma_0(n)^*$. *Journal of algebra, 64:340-390*, 1980.
31. P.W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.
32. Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, -, 2009.
33. Bruno Sterner. Commitment schemes from supersingular elliptic curve isogeny graphs. *Mathematical Cryptology*, 1(2):40–51, Mar. 2022.
34. J. Vélu. Isogenies entre courbes ellitiques. *C.R. Acard. Sc. Paris 273, 238-394*, 1935.
35. John Voight. *Quaternion algebras.* Springer Nature, 2021.
36. Lawrence C Washington. *Elliptic curves: number theory and cryptography.* Chapman and Hall/CRC, 2008.