Commitment Schemes from Supersingular Elliptic Curve Isogeny Graphs

Valerio Ardizio, Eduarda Assunção, Parsa Tasbihgou

May 2024

Abstract

The paper *Commitment Schemes from Supersingular Elliptic Curve Isogeny Graphs* by Bruno Sterner presents the first provably secure isogeny-based commitment schemes. The first is based on the CGL hash function and the second is based on the SIDH framework, that can speedup the computation. Both of these commitment schemes require a trusted third party for the setup. The commitment scheme is built by going on random walks on a supersingular isogeny graph. The author conjectures an upper bound for the amount of steps required, a parameter that is linked to the security of the schemes.

1 Introduction

In recent years, post-quantum protocol design has been a huge topic in cryptography that aims at creating protocols that will not fail when faced against a quantum adversary. There are a few categories that have been particularly promising, one of which the isogeny-based cryptography that is used in this paper. These cryptosystems' security rely on the hardness of finding a path in the supersingular ℓ-isogeny graph, sometimes with auxiliary information.

Bruno Sterner's paper proposes the first provably secure commitment schemes on supersingular elliptic curve isogeny graphs. This schemes require the use of a hash function, which was chosen to be the one proposed by [CLG09]. Additionally, Sterner proposed the use of the SIDH framework to speedup the computation of the commitment.

2 Preliminaries

2.1 Supersingular Elliptic Curve Isogenies

An isogeny between two elliptic curves is a map that preserves geometric and algebraic structure. A (seprable) ℓ-isogeny has kernel size ℓ. An endomorphism is an isogeny from a curve onto itself. The set of endomorphisms create a ring with addition and composition, named $End(E)$. The dual isogeny of $\phi: E_{start} \longrightarrow E_{end}$ is the unique isogeny $\hat{\phi}: E_{end} \longrightarrow E_{start}$ such that $\hat{\phi} \circ \phi = [deg(\phi)]id_{E_{start}}$ and $\phi \circ \hat{\phi} = [deg(\phi)]id_{E_{end}}$, where $[\cdot]$ defines the scalar multiplication.

Given a small prime ℓ and a large prime p, the supersingular ℓ-isogeny graph is defined as the graph whose vertex set is the isomorphism classes of supersingular elliptic curves defined over $\mathbb{F}_{p^2}$. Two vertices are connected by a directed edge if there is an isogeny between the two curves of degree ℓ. Every isogeny has a dual isogeny so the graph is undirected. The graph is also connected, which means there exists a path between any two vertices. Finally, the graph is $(\ell+1)$-regular, which means every vertex has $\ell+1$ outgoing edges.

It is possible to freely walk this graph guided by a string $m \in \mathbb{Z}_{\ell+1} \times (\mathbb{Z}_\ell)^{k-1}$. We start at an elliptic curve E_0 and choose which edge (in this case, an isogeny) to take to the next vertex E_1 according to the entries of m. To decide which edge to follow, we define the irreducible factors of the ℓ-division polynomial of our current vertex. We take ℓ roots of these factors that generate different subgroups and avoid backtracking: $P_0, P_1, ...P_{\ell-1}$. Then, we compute the next vertex $E_{i+1} = E_i/\langle P_{m_i} \rangle$ and the corresponding isogeny. In the end, we get a sequence of steps:

$$E_0 \xrightarrow{\phi_{P_{m_0}}} E_1 \xrightarrow{\phi_{P_{m_1}}} ... \xrightarrow{\phi_{P_{m_{k-1}}}} E_k$$

The overall isogeny from E_0 to E_k is a ℓ^k-isogeny obtained by composing k ℓ-isogenies.

Alternatively, one can walk the graph by getting a ℓ^k-cyclic subgroup G and from there compute the corresponding isogeny whose kernel is G. This approach based on the SIDH framework has faster computation and will be discussed later.

2.2 Commitment Schemes

A commitment scheme consists of three algorithms:

- **KeyGen**: a probabilistic polynomial-time algorithm that generates the public parameters;
- **Commit**: a probabilistic polynomial-time algorithm that outputs a commitment c of a message m and a random value r.
- **Open**: a deterministic polynomial-time algorithm that, given m, r, and c, outputs a boolean of whether c is a valid commitment for m and r.

The security notions required for the cryptographic applications of a commitment scheme are the following:

- **Hiding**: the commitment c does not reveal anything about the message m
- **Binding**: it is hard to create the same commitment c from two different messages, i.e. $c(m_1, r_1) = c(m_2, r_2)$ where $m_1 \neq m_2$

The hiding property is obtained if an adversary with the commitment $c(m,r)$ cannot distinguish between m and another message m'. The binding property is obtained if an adversary cannot create a single commitment for two different messages. These properties are defined by games where the adversary's advantage has to be negligible for any probabilistic polynomial-time algorithm, i.e, there is no strategy that allows an adversary to win and break the commitment scheme with non-negligible probability.

2.3 Mixing Constant

In order to establish the hiding property of the isogeny-based commitment scheme presented, the author needed to quantify how related are the end point and starting point. What is stated in the paper is that, for a sufficient amount of steps, all the points in the graph are possible end-points. The minimum amount of steps is called the mixing constant k_G of the graph G.

In a more formal way, for a connected d-regular graph G (with $d \geq 3$), let k_G be the corresponding mixing constant. Then for all $k \geq k_G$ and every pair of vertices (i,j), there exists a non-backtracking path between i and j of length k.

3 A commitment scheme from isogeny assumptions

Within the present section, a provably secure commitment scheme based on isogeny assumptions is described, being designed with the intent of achieving information-theoretic hiding and computational binding.

The scheme will be firstly presented in the supersingular 2-isogeny graph and secondly generalised to the supersingular ℓ-isogeny graph, with ℓ being an odd prime.

Crucial assumptions for the security of the commitment scheme are the properties derived from having *non-backtracking* random walks on regular graphs. The security of the commitment scheme is determined by the mixing constant of the isogeny graph, for which is important to obtain a conjectured upper bound in order to estimate the performance of the scheme.

When compared to other post-quantum commitment schemes, the one proposed hereunder is found to have smaller commitment values.

3.1 The scheme

The main idea of the commitment scheme is to use the optimal mixing properties of Ramanujan graphs [Alo86], firstly used in a cryptographic context in [CLG09], where a hash function based on random walks on Ramanujan graphs was proposed. Indeed, Pizer [Piz90] proved that supersingular elliptic curve isogeny graphs are instances of Ramanujan graphs, leading to the possibility of proving the security of the commitment scheme at hand through graph theoretic results.

Let λ be the security parameter, we now describe the the key generation algorithm in Algorithm 1 as well as the algorithms to run in order to compute and open a commitment, presented respectively in Algorithm 3 and Algorithm 4.

Algorithm 1 KeyGen

Input: Security parameter λ
Output: The prime number p, a supersingular elliptic curve E over $\mathbb{F}_{p^2}$, the length of the messages k, two random isogenies ϕ_1,ϕ_2 that have E as domain.
1: Pick a 2λ bit prime.
2: $E \leftarrow \text{PickEllipticCurve}_{\mathcal{T}}(p)$
3: Let $k = k_{2,p}$
4: Pick 2 random edges incident to $j(E)$ in the isogeny graph, *i.e. pick 2 random isogenies ϕ_1,ϕ_2 that have E as domain.*

An execution of the key generation algorithm will return a prime prime p of 2λ bits, a supersingular elliptic curve E over the finite field $\mathbb{F}_{p^2}$ with *unknown* endomorphism ring, a positive integer k that will represent the length of the messages and two random isogenies that have E as domain. The choice of a supersingular elliptic curve that has *unknown* endomorphism ring is crucial for the security of the scheme and it is suggested that a trusted third party $\mathcal{T}$ generates such a curve E by going on a random walk that starts from a fixed node of the supersingular isogeny graph. The trusted third party $\mathcal{T}$ should then return the final curve of the random walk, that is E, without revealing the path they took to reach it, as described in Algorithm 2. Under these assumptions, the endomorphism ring of E should remain unknown. The overall procedure for generating a valid key is described in Algorithm 1.

Algorithm 2 $\text{PickEllipticCurve}_{\mathcal{T}}$

Input: The prime number p
Output: A supersingular elliptic curve E over $\mathbb{F}_{p^2}$.
1: Let E_{1728} be a known supersingular elliptic curve
2: Starting from E_{1728}, go on a random walk over the supersingular isogeny graph
3: Reach an elliptic curve E without revealing the path.

In order to commit to a given message $m \in \{0,1\}^k$, one should follow the procedure described in Algorithm 3. Within such algorithm, note that we denote by $\Phi_2(E,m)$ the supersingular elliptic curve obtained after going on a *non-backtracking* random walk over the supersingular 2-isogeny graph starting from E and guided by the string m, considering the sequence of steps:

$$E = E_0 \to E_1 \to \cdots \to E_k = \Phi_2(E,m).$$

Algorithm 3 Commit

Input: The message $m \in \{0,1\}^k$
Output: The commitment c of the message m.
1: Compute the curve $E_m \leftarrow \Phi_2(E,m)$, *making sure that the first step in the graph is one of the two edges chosen in* KeyGen
2: $r \in_{\$} \{0,1\}^k$
3: Compute the curve $E' := \Phi_2(E_m, r)$, *avoiding any backtracking in the isogeny graph*
4: Compute $c := j(E')$ as the commitment of the message m

It is possible to open the commitment with the knowledge of the message m, the randomness r and the value of the commitment c by following the procedure described in Algorithm 4.

Algorithm 4 OPEN

Input: The message m, randomness r, commitment c
Output: A boolean value to indicate if the commitment is valid or not.

1: Compute the curve $\Phi_2(\Phi_2(E,m),r)$
2: Compute the boolean $c==j(\Phi_2(\Phi_2(E,m),r))$

3.2 Hiding property

The results from graph theory presented in Section 2 and the following theorem on random walks on isogeny graphs will be used to show that the commitment scheme described in Section 3.1 is information-theoretically hiding.

Theorem 1. *Given a prime number p, let j_0 be a supersingular j-invariant in characteristic p, N_p be the number of supersingular j-invariants in characterstic p and $n=\prod_i \ell_i^{e_i}$ be an integer where ℓ_i are small primes. Let $\hat{j}$ be the j-invariant reached by a random walk of degree n starting at j_0. Then for every j-invariant $\tilde{j}$ we have*

$$\left|\mathbb{P}\left[\hat{j}=\tilde{j}\right]-\frac{1}{N_p}\right|\leq\prod_i\left(\frac{2\sqrt{\ell_i}}{\ell_i+1}\right)^{e_i}$$

Proof. See [GPS17, Theorem 1] □

Therefore, Theorem 1 ensures us that for any random walk of degree n, the probability of ending on any node of the supersingular isogeny graph is close to uniform for a sufficiently long walk. Moreover, Theorem 1 is crucial for proving the following theorem that shows the information-theoretical hiding property of the scheme described in Section 3.1.

Theorem 2 (information-theoretically hiding)**.** *Let $k_{2,p}$ be the mixing constant for the supersingular 2-isogeny graph in characteristic p. Then for any $k\geq k_{2,p}$, the commitment scheme described in Section 3.1 is information-theoretically hiding.*

Since our random walks happen on supersingular isogeny graphs, that are Ramanujan graphs, the mixing constant can be conjectured to be upper-bounded as follows[1].

Conjecture 1. *Let $k_{2,p}$ be as previously defined, the following upper bound holds:*

$$k_{2,p}\leq 4\lceil\log_2(p)\rceil-4$$

.

Conjecture 1 is the result of a general conjecture for connected d-regular graphs. Since isogeny graphs are optimal expanders we can hope to have a better upper bound.

[1]This upper bound seems to be accurate for supersingular 2-isogeny graphs as experimental results on this conjecture show that for every prime $p\leq 65600$ and also some primes between $123000\leq p\leq 131100$ and $234000\leq p\leq 2^{18}$, the associated mixing constant for the supersingular 2-isogeny graph is no more than $\log_2(p)+\log_2(\log_2(p))+\frac{3}{10}$.

Conjecture 2. *Let $k_{2,p}$ be as previously defined, the following upper bound holds:*

$$k_{2,p}\leq\log_2(p)+\log_2(\log_2(p))+O(1).$$

In particular, the constant in the big-O notation is at most 1.

If the conjecture holds true, then we can choose $k=\lceil\log_2(p)+\log_2(\log_2(p))+1\rceil$, ensuring information-theoretic hiding for the commitment scheme and obtaining decent performance for the protocol.

3.3 Binding property

The binding property of the scheme will be proved under the hardness assumption of the following problem.

Problem 1 (Supersingular Smooth 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[2] of E whose degree is a prime power ℓ^e.*

The following result ensures the computational binding property of the protocol.

Theorem 3 (computationally binding)**.** *The commitment scheme described in Section 3.1 is computationally binding under the Supersingular Smooth Endomorphism Problem on the curve E for the prime $\ell=2$.*

Remark. *Problem 1 trivially shows the necessity of the endomorphism ring of E remaining unknown during the execution of Algorithm 1 for generating a valid key. Moreover, the attack presented in [Eis+18] broke the second preimage resistance of the isogeny hash function under the assumption of known endomorphism ring of E.*

3.4 Generalisation

The scheme discussed in the previous sections can be easily generalised to work in the supersingular ℓ-isogeny graph for a small odd prime ℓ. Acknowledging that the key generation is the same as described in Algorithm 1, we describe the changes to the algorithms that allow to commit to a message and to open a commitment.

To commit to a message $m\in\{0,...,\ell-1\}^k$, every step of Algorithm 3 stays the same, except for the randomness being $r\in_\$\{0,...,\ell-1\}^k$ and the 2-isogenies now being ℓ-isogenies.

Given the knowledge of the message m, the randomness r and the value of the commitment c, in order to open the commitment one can follow Algorithm 4, but acknowledging that now we have ℓ-isogenies instead of 2-isogenies.

The security of the generalised commitment scheme can be proved by the following theorems, completely analogous to the case described in Section 3.1 both for the claim and for the proofs.

Theorem 4. *Let $k_{\ell,p}$ be the mixing constant for the supersingular ℓ-isogeny graph in characteristic p. Then for any $k\geq k_{\ell,p}$, the commitment scheme described above is information theoretically hiding.*

[2]An endomorphism is *non-trivial* if it is not a multiplication-by-m map, i.e. $[m]$ and *cyclic* if the endomorphism has a cyclic kernel.

Theorem 5. *The above commitment scheme is computationally binding under the Supersingular Smooth Endomorphism Problem on the curve E and the prime ℓ.*

Furthermore, we can make the following conjecture on an upper bound of the mixing constant in the supersingular ℓ-isogeny graphs.

Conjecture 3. *Let $k_{\ell,p}$ be as previously defined, the following upper bound holds:*

$$k_{\ell,p} \leq \log_\ell(p) + \log_\ell(\log_\ell(p)) + O(1).$$

In particular, the constant in the big-O notation is at most 1.

4 Commitment using the SIDH approach

We can use the SIDH framework to speedup the commitment algorithm. Instead of computing the isogeny walk step by step using the l-division polynomial, we can specify its kernel and use Velu-type formulas to compute the image curve.
Let $p = 2^n f - 1$ be a prime and E a supersingular elliptic curve such that $\#E(\mathbb{F}_{p^2}) = (2^n f)^2$ (equivalently, $tr(\pi) = -2p$). The 2^n-torsion subgroup $E[2^n]$ is defined over $\mathbb{F}_{p^2}$. A cyclic isogeny with 2-power degree can be specified with its kernel that is contained in $E[2^n]$.
We know $E[2^n] \simeq (\mathbb{Z}_{2^n})^2$, so it's a $\mathbb{Z}_{2^n}$-Module of rank 2. Let $\{P,Q\}$ be a basis and $m \in \mathbb{Z}_{2^n}$, then a separable isogeny ϕ_m of degree 2^n exists with kernel $\langle P + mQ \rangle$ and it can be computed in polynomial time. Therefore a random isogeny walk of length n can be specified with a single element in $\mathbb{Z}_{2^n}$. The longest isogeny walk that can be specified with its kernel has length n and $n \simeq log(p)$ however, we need a walk of length $4log(p)$ to achieve the hiding property. The solution is to repeat the isogeny walk 4 times, each time using a subgroup of the torsion points of the new curve as the kernel of the next isogeny. To do this we need to find a basis for the torsion points of each image curve. We already know $Q' = \phi_m(Q)$ has order 2^n, we need another full order element P' independent of Q' to form a basis. P' has to be deterministic so the commitment can be opened.
To generate P' we use the "Elligator 2" method from [Cos+]. A deterministic point $R \in E_m$ is generated, then check that R is not divisible by 2 and R is independent from Q'. Then $\{P' = fR, Q'\}$ is a deterministic basis for $E_m[2^n]$. Now we can specify a random isogeny walk of length $4log(p)$ from 4 random elements $m_0, m_1, m_2, m_3 \in \mathbb{Z}_{2^n}$ equivalently $m \in \mathbb{Z}_{2^{4n}}$.

5 Comparison

For a prime $p = 2^n f - 1$ computing the CGL hash function for a walk of length k in the supersingular 2-isogeny graph takes $kn(5.7n + 110)M$ and the same computation in the SIDH framework takes $kn(13.5log(n) + 42.4)M$ where M is the cost of multiplication in $\mathbb{F}_{p^2}$. Their ratio is $\frac{5.7n+110}{13.5log(n)+42.4} \simeq O(\frac{n}{log(n)})$ So the SIDH variant is exponentially faster than CGL.
Both schemes have a single field element in $\mathbb{F}_{p^2}$ as commitment.When viewed as a 2-dimensional extension over the prime field, each element in $\mathbb{F}_{p^2}$ is represented by two elements in $\mathbb{F}_p$. If λ is the security parameter, a prime of size 2λ should be used, in this case the commitment has size 4λ. For 128-bit security these schemes give a 64B commitment, whereas known lattice-based schemes have commitments of size 9kB for the same level of security.
Consistent with other isogeny-based crypto, these schemes are slower than lattice-based constructions.

6 Conclusion

We have seen a commitment scheme that is unconditionally information-theoretic hiding and computationally binding assuming hardness of the endomorphism ring problem.
There are some questions that are unanswered and are interesting for further discussion: The presented schemes are not homomorphic. A homomorphic isogeny-based commitment scheme will be a breakthrough in the field. In this article an upper-bound for the mixing parameter of the supersingular isogeny graph is used that is far from the conjectured optimum. An improvement on this upper-bound translates to lower computation time.

References

[Alo86] Noga Alon. "Eigenvalues and expanders". In: *Combinatorica* 6.2 (1986), pp. 83–96.

[Piz90] Arnold K Pizer. "Ramanujan graphs and Hecke operators". In: *Bulletin of the American Mathematical Society* 23.1 (1990), pp. 127–137.

[CLG09] Denis X Charles, Kristin E Lauter, and Eyal Z Goren. "Cryptographic hash functions from expander graphs". In: *Journal of CRYPTOLOGY* 22.1 (2009), pp. 93–113.

[GPS17] Steven D Galbraith, Christophe Petit, and Javier Silva. "Identification protocols and signature schemes based on supersingular isogeny problems". In: *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23*. Springer. 2017, pp. 3–33.

[Eis+18] Kirsten Eisenträger et al. "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*. Springer. 2018, pp. 329–368.

[Cos+] Craig Costello et al. "Efficient Compression of SIDH Public Keys". In: ().