Isogeny Graphs Over Composite Moduli

Travis Scholl

February 22, 2019

Abstract

Recently Altuğ and Chen proposed a cryptographic construction involving the isogeny graph of elliptic curves over $\mathbb{Z}/N\mathbb{Z}$ with composite N. In this talk, we will summarize their construction and mention some of the open problems related to the security of cryptosystems based on this construction.

1 Goal

The goal is to find a group G such that we can easily multiply, but not invert. We want to support the following functionality:

encode (private): Given $x \in G$, output an encoding $e(x)$.

compose (public): Given $e(x)$, $e(y)$, output $e(xy)$.

equivalence (public): Given $e(x)$, $e(y)$, determine if $x = y$.

We require the following to be computationally hard:

inversion (hard) Given $e(x)$, output $e\left(x^{-1}\right)$.

Remark 1.1. A related problem to inversion is cancellation: Given $e(x)$ and $e(xy)$, output $e(y)$. If you can solve one of cancellation or inversion for all inputs, then you can solve the other. However, in the construction below, the cancellation problem will sometimes be easy because the group operation will be represented by concatenation of encodings. This does not seem to affect the difficulty of the inversion problem.

2 Implementation with Isogenies

Choose two large primes p and q. Set $N = pq$. Choose two elliptic curves $E_{0,p}/\mathbb{F}_p$ and $E_{0,q}/\mathbb{F}_q$ such that

$$\operatorname{End}_{\overline{\mathbb{F}}_p}(E_{0,p}) \cong \operatorname{End}_{\overline{\mathbb{F}}_q}(E_{0,q}) \cong \mathcal{O},$$

where $\mathcal{O}$ is some pre-specified order in an imaginary quadratic field. Let $j_0 \in \mathbb{Z}/N\mathbb{Z}$ be the output of the Chinese remainder theorem applied to $j(E_{0,p})$ and $j(E_{0,q})$. Our group G will be the class group $G = Cl(\mathcal{O})$. The public information is (N, j_0). Some auxiliary data will also be made public to support composition (see below).

Remark 2.1. The order $\mathcal{O}$, its class group structure, class number, and the factorization of N are all private.

Our implementation is as follows:

encode (private): Given an ideal $\mathcal{I}$ of $\mathcal{O}$, we write $\mathcal{I}$ as a product of small ideals[1] $\mathfrak{a}_i$ with coprime norm and coprime to N (being small should automatically force them to be coprime to N, i.e. ideals whose norm is polynomial in the security parameter), so $\mathcal{I} = \prod_{i=1}^{t} \mathfrak{a}_i^{e_i}$. For each i, we have a ladder $(j_0 = j_{0,i}, j_{1,i}, \ldots, j_{e_i,i})$ where $j_{k,i} = \mathfrak{a}_i * j_{k-1,i}$. The action of the class group on j-invariants in $\mathbb{Z}/N\mathbb{Z}$ is computed as by the usual action over $\mathbb{Z}/p\mathbb{Z}$ and $\mathbb{Z}/q\mathbb{Z}$, and the results are combined via the Chinese remainder theorem. Let L_i denote the ladder $L_i = (j_{0,i}, \ldots, j_{e_i,i})$. The encoding $e(\mathcal{I})$ is given by a list of tuples

$$e(\mathcal{I}) = \{(\mathrm{Norm}(\mathfrak{a}_i), L_i)\}_{i=1,\ldots,t}$$

equivalence (public): Given the encodings $e(\mathcal{I})$ and $e(\mathcal{J})$, we want to determine whether $\mathcal{I} \equiv \mathcal{J}$ in $Cl(\mathcal{O})$. It is sufficient to show that, given $e(\mathcal{I})$, we can compute $\mathcal{I} * j_0$ using only public information.

Suppose $\mathfrak{a}_1, \mathfrak{a}_2$ are ideals with coprime norms n_1, n_2 respectively. Then $(\mathfrak{a}_1\mathfrak{a}_2) * j_0$ is the root of the linear polynomial $\gcd(\Phi_{n_2}(\mathfrak{a}_1 * j_0, x), \Phi_{n_1}(\mathfrak{a}_2 * j_0, x))$ in $\mathbb{Z}/N\mathbb{Z}$.[2] Here Φ_n is the usual modular polynomial. The computation can be done in $\mathbb{Z}/N\mathbb{Z}$ because $\Phi_n(x, y) \in \mathbb{Z}[x, y]$.

Recall that an encoding $e(\mathcal{I})$ is a list of tuples $(\mathrm{Norm}\,\mathfrak{a}_i, L_i)$ for $i = 1, \ldots, t$, where $\mathcal{I} = \prod_{i=1}^{t} \mathfrak{a}_i^{e_i}$. We also required that $\mathrm{Norm}\,\mathfrak{a}_i$ was small. Write $L_i = (j_{0,i}, \ldots, j_{e_i,i})$. Here $j_{k,i} = \mathfrak{a}_i^k * j_0$. Our goal is to compute $\mathcal{I} * j_0$.

Let $\mathfrak{b}_1, \mathfrak{b}_2$ be two ideals dividing $\mathcal{I}$. Suppose that there is some pair of distinct indices i, j such that $\mathfrak{b}_1\mathfrak{a}_i = \mathfrak{b}_2\mathfrak{a}_j$. The operation above says that if we know $\mathfrak{b}_1 * j_0$ and $\mathfrak{b}_2 * j_0$, then we can compute $\mathfrak{b}_1\mathfrak{a}_i * j_0 = \mathfrak{b}_2\mathfrak{a}_j * j_0$. Essentially we are just computing

$$\gcd\left(\Phi_{\mathrm{Norm}\,\mathfrak{a}_i}(\mathfrak{b}_1 * j_0, x), \Phi_{\mathrm{Norm}\,\mathfrak{a}_j}(\mathfrak{b}_2 * j_0, x)\right)$$

over $\mathbb{Z}/N\mathbb{Z}$. Since we know $\mathfrak{a}_i^k * j_0$ for all $0 \le k \le e_i$, it is possible to compute $\mathcal{I} * j_0$. This takes roughly $O(\prod e_i)$ gcd computations.

[1] We also require these ideals correspond to cyclic isogenies, i.e. the induced isogeny $j \to \dashv * j$ is cyclic.

[2] To see that the polynomial is linear, notice that there is a unique subgroup of $E_{0,p}$ of degree $n_1 n_2$ containing both the kernel of $E_{0,p} \to \mathfrak{a}_1 * E_{0,p}$ and the kernel of $E_{0,p} \to \mathfrak{a}_2 * E_{0,p}$. The same holds for $E_{0,q}$.

Example 2.2. Suppose $\mathcal{I} = \mathfrak{a}_1^3\mathfrak{a}_2^2$. Then we start with $\mathfrak{a}_1 * j_0, \mathfrak{a}_1^2 * j_0, \mathfrak{a}_1^3 * j_0$ and $\mathfrak{a}_2 * j_0, \mathfrak{a}_2^2 * j_0$. First we compute $\mathfrak{a}_1\mathfrak{a}_2 * j_0$ using $\mathfrak{a}_1 * j_0$ and $\mathfrak{a}_2 * j_0$. Then we can compute $\mathfrak{a}_1\mathfrak{a}_2^2 * j_0$ using $\mathfrak{a}_1\mathfrak{a}_2 * j_0$ and $\mathfrak{a}_2^2 * j_0$. We continue adding one $\mathfrak{a}_1$ or $\mathfrak{a}_2$ at a time until we have covered all ideals $\mathfrak{a}_1^i\mathfrak{a}_2^j$ for $0 \leq i \leq 3$ and $0 \leq j \leq 2$.

compose (public): Given encodings $e(\mathcal{I})$ and $e(\mathcal{J})$, we want to compute $e(\mathcal{I}\mathcal{J})$ using only public information. For this we cheat by not really doing it. Instead, we make public some encodings of small ideals $e(\mathfrak{a}_1^{k_1}), \ldots, e(\mathfrak{a}_t^{k_t})$. If $\{\mathfrak{a}_1, \ldots, \mathfrak{a}_t\}$ generate the class group, then we can assume all encodings are made using only products of these ideals. Suppose $e(\mathcal{I})$ is constructed using the equivalent ideal $\prod \mathfrak{a}_i^{r_i}$ and $e(\mathcal{J})$ is constructed using $\prod \mathfrak{a}_i^{s_i}$. Then, assuming that $r_i + s_i \leq k_i$ for all i, we can construct an encoding $e(\mathcal{I}\mathcal{J})$ by taking ladders $j_0, \mathfrak{a}_i * j_0, \ldots, \mathfrak{a}_i^{r_i+s_i} * j_0$. These are subsets of the encodings $e(\mathfrak{a}_i^{k_i})$, which we just made public.

Remark 2.3. Suppose that $e(\mathcal{I})$ and $e(\mathcal{J})$ have disjoint support, meaning that if $e(\mathcal{I})$ was constructed from the factorization $\mathcal{I} \equiv \prod \mathfrak{a}_i^{r_i}$ and $e(\mathcal{J})$ was constructed using $\mathcal{J} \equiv \prod \mathfrak{b}_j^{s_j}$, then $\mathfrak{a}_i$ and $\mathfrak{b}_j$ have pairwise coprime norms. Then a valid encoding $e(\mathcal{I}\mathcal{J})$ can be obtained by simply concatenating $e(\mathcal{I})$ and $e(\mathcal{J})$, without the need for any ladders.

inversion (hard): Given an encoding $e(\mathcal{I})$, we want to know how much work is required to find an encoding $e(\mathcal{I}^{-1})$. A related question is finding a "canonical encoding", i.e. given $e(\mathcal{I})$, find $\mathcal{I}^{-1} * j_0$ in $\mathbb{Z}/N\mathbb{Z}$.

Consider the case of an ideal $\mathfrak{l}$ with prime norm ℓ. This is called the (ℓ, ℓ^2)-*isogenous neighbor problem*. Since we are given $e(\mathfrak{l})$, we know j_0 and $j_1 = \ell * j_0$. Finding $e(\mathfrak{l}^{-1})$ is equivalent to finding a root of $\gcd(\Phi_\ell(j_0, x), \Phi_{\ell^2}(j_1, x))$ in $\mathbb{Z}/N\mathbb{Z}$. This polynomial has degree ℓ, so finding a root may be computationally difficult without the factorization of N. Note that it is important that we don't make public composition ladders as long as the order of $\mathfrak{l}$ in $Cl(\mathcal{O})$ (see the compose function).

Remark 2.4. The (ℓ, ℓ^2)-isogeneous neighbor problem is stated using only j-invariants. However, one could also phrase it as follows: Given elliptic curves E_1, E_2 over $\mathbb{Z}/N\mathbb{Z}$ and an explicit ℓ-isogeny $\varphi : E_1 \to E_2$, find E_3 such that E_3 admits an ℓ-isogeny to E_1 and cyclic ℓ^2 isogeny to E_2. To see why this version is equivalent, we need to show that given a pair $j_1, j_2 \in \mathbb{Z}/N\mathbb{Z}$ such that $\Phi_\ell(j_1, j_2) \equiv 0 \mod N$, we can write down elliptic curves E_1, E_2 and an explicit ℓ-isogeny $\varphi : E_1 \to E_2$ such that $j(E_i) = j_i$. Moreover, all calculations must be done over $\mathbb{Z}/N\mathbb{Z}$ without factoring N. Using the formulas in [MS16, Sec. 2], it is sufficient to find the kernel polynomial $h(x) = \prod(x - x_Q)$, where the product ranges over all $Q \in \ker \varphi$ and x_Q is the x-coordinate of the point Q. This can be done following the method laid out in [Sch95, Sec. 8].

3 Attacks

In this section we summarize several approaches to attacking the (ℓ, ℓ^2)-isogeneous neighbor problem.

Factoring N via E_0: Suppose E_0 is chosen such that $\#E_0(\mathbb{F}_p)$ and $\#E_0(\mathbb{F}_q)$ have polynomially small factors. Then we could factor N using Lenstra's elliptic curve factorization algorithm. The subtleties are that it is difficult to find a point $P \in E_0(\mathbb{Z}/N\mathbb{Z})$, as it may require taking a square root. However, we may be able to work with only the x-coordinate. To avoid this attack, we should choose E_0 such that $\#E_0(\mathbb{F}_p)$ and $\#E_0(\mathbb{F}_q)$ are not polynomially-smooth.

$\ell \leq 3$ case: If $\Phi_\ell(j_1, j_2) \equiv 0 \mod N$, $\ell \nmid N$, then we can compute a kernel polynomial $h(x)$ for an isogeny $E_1 \to E_2$ where $j(E_i) = j_i$. This does not require the factorization of N. If $\ell \leq 3$, then $h(x)$ is linear, which gives us an x-coordinate of a point P in $E_0(\mathbb{Z}/N\mathbb{Z})[\ell]$. This can not be used in Lenstra's factorization algorithm because $\ell P = 0$ in both $E_0(\mathbb{F}_p)$ and $E_0(\mathbb{F}_q)$. It is suggested to avoid this case and only consider $\ell \geq 5$ [AC18, Sec. 4.3].

Using the Hilbert class polynomial: Suppose we know the discriminant D of $\mathcal{O}$. Then

$$\gcd\left(\Phi_\ell(j_0, x), \Phi_{\ell^2}(j_1, x), H_D(x)\right)$$

is a linear function whose root is a solution to the (ℓ, ℓ^2)-isogeneous neighbor problem. To avoid this, we should choose D to be super-polynomial in the security parameter. This should make computing H_D (even modulo N) difficult.

Frobenius relations: Suppose that ℓ factors in $\mathcal{O}$ as $\mathfrak{l}\bar{\mathfrak{l}}$. Assume these are non-trivial in the class group. Let $j_1 = \mathfrak{l} * j_0$. Then a solution to the (ℓ, ℓ^2)-isogenous neighbor problem is $j_{-1} = \bar{\mathfrak{l}} * j_0$. To see why, note that $\mathfrak{l}^2 * j_{-1} = \mathfrak{l}^2 * (\bar{\mathfrak{l}} * j_0) = \ell\mathcal{O} * (\mathfrak{l} * j_0) = \ell\mathcal{O} * j_1 = j_1$. As mentioned in [AC18, Rem. 2.5], if we are working over a finite field, then the isogeny from $E_{-1} \to E_0$ is related to the one from $E_0 \to E_1$ by the Frobenius automorphism. It is unclear how to use this fact over $\mathbb{Z}/N\mathbb{Z}$.

4 Applications

The paper [AC18] described a broadcast encryption scheme.

5 Open Problems

5.1 Security

The following problems, or certain specializations of these problems, should be difficult in order for this system to be secure.

1. Given E over $\mathbb{Z}/N\mathbb{Z}$, find a single elliptic curve ℓ-isogenous to E.

2. Over $\mathbb{Z}/N$, given an ℓ-isogeny $\phi : E \to E'$ given as a rational map, solve the (ℓ, ℓ^2)-neighbor problem. One may additionally suppose that we have coordinates of a point generating the kernel, or that $\ell = 3$ (in which case the x-coordinate of a kernel point can be easily found).

3. Solve the generalized (ℓ, ℓ^2)-neighbor problem in the context of the start of [AC18, Sec. 5.2].

4. [AC18, Sec. 5.2.2] In the isogeny volcano mod N, determine if a given isogeny is horizontal, going up, or going down. Or better: find a horizontal isogeny. Specifically, can we adapt an algorithm of Ionica-Joux [IJ13] for this purpose?

   A quick overview of [IJ13] is as follows. Let $E/\mathbb{F}_q$ be an ordinary elliptic curve with endomorphism ring $\mathcal{O}$. Suppose ℓ splits in $\mathcal{O}$ as $\mathfrak{l}\bar{\mathfrak{l}}$. Then the natural maps $E \to \mathfrak{l} * E$ and $E \to \bar{\mathfrak{l}} * E$ are the horizontal isogenies. These can be found by looking for invariant subspaces of the Frobenius endomorphism (e.g. choose a basis of $E[\ell]$ and find the eigenspaces for the matrix of the Frobenius endomorphism). Every vertex not on the crater admits a unique ascending isogeny, the rest are descending. The ascending one can be determined by checking a certain pairing-based condition and using some points in $E[\ell^\infty]$ in $E[\mathbb{F}_{q^k}]$ for certain k, see [IJ13, Prop. 7].

5. [AC18, Sec. 5.2.3] When $\ell \in \{2, 3, 5, 7, 13\}$, $X_0(\ell)$ has genus zero and hence lots of rational points (see https://oeis.org/A001617). Can we use these to get many points on $X_0(\ell)$ over $\mathbb{Z}/N\mathbb{Z}$, and leverage this to solve any of the above problems?

6. Find a discriminant D and trapdoor τ so that solving DLP in the class group $\mathrm{Cl}(D)$ is hard, but easy with the trapdoor.

7. [AC18, Defn. 5.4] Given an integer N and a set of primes $\mathcal{P} = \{p_1, \ldots, p_m\}$, find an integer $D < 0$ such that $|D| \leq \sqrt{N}$ and $\left(\frac{D}{p}\right) = 1$ for all $p \in \mathcal{P}$.

8. [AC18, Defn. 5.5] [Dam90, Prob. P1] Given

$$\left(\frac{a}{p}\right), \left(\frac{a+1}{p}\right), \ldots, \left(\frac{a+\ell}{p}\right),$$

   determine $\left(\frac{a+\ell+1}{p}\right)$.

9. Given an encoding of an ideal class, is it possible to determine if the element has polynomial order? If we know that the order *is* polynomial, can we actually compute the order?

10. [AC18, Sec. 5.4] Decisional inversion: Given an encoding of $e(\mathcal{I})$ and j-invariant j, determine whether $j = \mathcal{I}^{-1} * j_0$. Essentially, determine if j is a "canonical encoding" of the "composable encoding" of $\mathcal{I}$.

5.2 Efficiency

Solving any of the following problems may lead to a more efficient cryptosystem or more general parameters.

1. [AC18, Sec. 4] Given an order $\mathcal{O}$ in an imaginary quadratic field, find an elliptic curve E over a finite field $\mathbb{F}_q$ with endomorphism ring $\mathcal{O}$.

   This problem is easy if the discriminant D of $\mathcal{O}$ is small. For example, suppose $\mathcal{O} = \mathbb{Z}[i]$. The Hilbert class polynomial of $\mathbb{Z}[i]$ is $H_D(x) = x - 1728$. We can then write down a model (e.g. Weierstrass equation) of an elliptic curve E over $\mathbb{Z}$ with endomorphism ring $\mathrm{End}_{\overline{\mathbb{Q}}}(E) = \mathbb{Z}[i]$. Let p be a prime of good reduction that splits in $\mathbb{Z}[i]$. Then $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) = \mathbb{Z}[i]$, so we output $E/\mathbb{F}_p$.

   If D is large, then computing H_D is infeasible. However, suppose that $\mathcal{O}$ has a large conductor, i.e. D has a large square factor. For example, $\mathcal{O} = \mathbb{Z}[2^{100}i]$. Then we look for $\pi \in \mathcal{O}$ with prime norm such that π does not exist in any larger order, e.g. $\pi = a + 2^{100}i$ for some integer a. This is equivalent to searching for integers a such that $p = a^2 + 2^{200}$ is prime. Given such a prime p, we proceed as before to find $E/\mathbb{F}_p$ with $\mathrm{End}_{\overline{\mathbb{F}}_p}(E) = \mathbb{Z}[i]$. Now we compute vertical 2-isogenies descending down the isogeny volcano. That is, the first step takes us $E \to E_1$ and $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_1) = \mathbb{Z}[2i]$. Then $E_1 \to E_2$ with $\mathrm{End}_{\overline{\mathbb{F}}_p}(E_2) = \mathbb{Z}[2^2 i]$, and so on. The vertical isogenies can be computed using the algorithm of Ionica-Joux [IJ13].

5.3 Theoretical

The following problems are helpful for either a security reduction or are independently interesting.

1. Adapt the Kunihiro-Koyama point-counting algorithm [KK98] to the case of E over $\mathbb{Z}/N$ where E_p and E_q have isomorphic endomorphism rings.

   A quick overview of [KK98, Sec. 3]: Suppose we have a black box to compute $\#E(\mathbb{Z}/N\mathbb{Z})$. We want to show how to use this to factor N. The algorithm is essentially the same as the standard elliptic curve factoring algorithm. Start by choosing a random point P and random elliptic curve E such that $P \in E(\mathbb{Z}/N\mathbb{Z})$. Then use the black box to compute $\#E(\mathbb{Z}/N\mathbb{Z})$. Let r be a prime roughly equal to $\log N$. Repeat the process until $\#E(\mathbb{Z}/N\mathbb{Z})$ is divisible by r (this includes $\approx \log N$ queries). Now attempt to compute $\left(\frac{\#E(\mathbb{Z}/N\mathbb{Z})}{r}\right) \cdot P$. If it fails, then it failed because at some point in the addition formula we had to "divide by 0", which corresponds to finding a factor of N. Otherwise we repeat the process.

2. [AC18, Sec. 3.3] Is the (ℓ, ℓ^2)-isogenous neighbor problem equivalent to factoring? See [AC18, Thm. 3.3]

References

[AC18] Salim Ali Altug and Yilei Chen. A candidate group with infeasible inversion. Cryptology ePrint Archive, Report 2018/926, 2018. https://eprint.iacr.org/2018/926.

[Dam90] Ivan Bjerre Damgård. On the randomness of Legendre and Jacobi sequences. In *Advances in cryptology—CRYPTO '88 (Santa Barbara, CA, 1988)*, volume 403 of *Lecture Notes in Comput. Sci.*, pages 163–172. Springer, Berlin, 1990.

[IJ13] Sorina Ionica and Antoine Joux. Pairing the volcano. *Math. Comp.*, 82(281):581–603, 2013.

[KK98] Noboru Kunihiro and Kenji Koyama. Equivalence of counting the number of points on elliptic curve over the ring Z_n and factoring n. In *Advances in cryptology—EUROCRYPT '98 (Espoo)*, volume 1403 of *Lecture Notes in Comput. Sci.*, pages 47–58. Springer, Berlin, 1998.

[MS16] Dustin Moody and Daniel Shumow. Analogues of Vélu's formulas for isogenies on alternate models of elliptic curves. *Math. Comp.*, 85(300):1929–1951, 2016.

[Sch95] René Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 7(1):219–254, 1995. Les Dix-huitièmes Journées Arithmétiques (Bordeaux, 1993).