Open Problems Discussion

March 17, 2019

Abstract

This talk will be more of a discussion on some open problems we have seen so far. It should be independent of the previous talks. We will focus on a few of the problems on class groups and isogenies referred to in the Altug-Chen paper discussed on 2/22/19. The preprint is available here: https://eprint.iacr.org/2018/926 and notes from the previous talk can be found https://www.math.uci.edu/~schollt/multilinear_map_seminar/scholl-02-22-19.pdf The problems we will focus on are finding an elliptic curve with a specified endomorphism ring, and finding l-isogenies over composite rings.

1 Introduction

The following problems are relevant to the cryptosystem proposed in [AC18].

2 Elliptic Curves With Specified Endomorphism Ring

This problem comes from [AC18 Sec. 4].

Problem 1. Given an order $\mathcal{O}$ in an imaginary quadratic field, find an elliptic curve $E$ over a finite field $\mathbb{F}_p$ with endomorphism ring $\mathcal{O}$.

This problem is easy if the discriminant $D$ of $\mathcal{O}$ is small. We can compute the Hilbert class polynomial $H_{\mathcal{O}}(x)$ of $\mathcal{O}$. For primes $p$ that split in $\mathcal{O}$, the roots of $H_{\mathcal{O}}(x) \mod p$ are $j$-invariants of ordinary elliptic curves over $\mathbb{F}_p$ with endomorphism ring $\mathcal{O}$.

Example 2. Suppose $\mathcal{O} = \mathbb{Z}[i]$. The Hilbert class polynomial of $\mathbb{Z}[i]$ is $x - 1728$. We can then write down a model (e.g. Weierstrass equation) of an elliptic curve $E$ over $\mathbb{Z}$ with endomorphism ring $\text{End}_{\mathbb{Z}}(E) = \mathbb{Z}[i]$, e.g. $Y^2 = X^3 + X$. Let $p$ be a prime of good reduction that splits in $\mathbb{Z}[i]$. Then $\text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[i]$.

If the discriminant $D$ of $\mathcal{O}$ is large, then computing $H_{\mathcal{O}}$ is infeasible. However, suppose that $\mathcal{O}$ has a large conductor, i.e. $D$ has a large square factor.
For example, $O = \mathbb{Z}[2^{100}i]$. Then we look for $\pi \in O$ with prime norm such that $\pi$ 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 $\text{End}_{\mathbb{F}_p}(E) = \mathbb{Z}[i]$. Now we compute vertical 2-isogenies descending down the isogeny volcano. That is, the first step takes us $E \rightarrow E_1$ and $\text{End}_{\mathbb{F}_p}(E_1) = \mathbb{Z}[2i]$. Then $E_1 \rightarrow E_2$ with $\text{End}_{\mathbb{F}_p}(E_2) = \mathbb{Z}[2^2i]$, and so on. The vertical isogenies can be computed using the algorithm of Ionica-Joux [IJ13].

During the discussion we talked about the following existence problem.

**Problem 3.** Given a prime $p$ and order $O$, does there exist an elliptic curve $E/\mathbb{F}_p$ with $\text{End} E \cong O$?

We came up with the following solution.

**Theorem 4.** Let $p$ be a prime and $O$ an order in a quadratic imaginary field. There exists an elliptic curve $E/\mathbb{F}_p$ with $\text{End} E \cong O$ if and only if there exists $\pi \in O$ such that $\pi \overline{\pi} = p$.

**Proof.** Suppose $E$ exists. Let $\pi \in O$ correspond to the Frobenius endomorphism on $E$. Then it is well known that $\pi \overline{\pi} = p$. The reverse direction is given by Honda-Tate theory which says there is a bijection between isogeny classes of simple ordinary abelian varieties over $\mathbb{F}_p$ and Weil $p$-numbers.

3 **The $(\ell, \ell^2)$-isogeny Problem**

This problem comes from [AC18 Sec. 5.2].

**Problem 5.** Let $j_0$ be the $j$-invariant of an elliptic curve over $\mathbb{Z}/NZ$ with endomorphism ring $O$. Let $I$ be an ideal of $O$ with prime norm $\ell$. Given $j_0$ and $j_1 = I \ast j_0$, find $j^{-1} = I \ast j_0$.

An easier version would be to ask for any root of $\gcd(\Phi_{\ell}(j_0, X), \Phi_{\ell^2}(j_1, X))$. The difference is that in this version, we are considering both horizontal and vertical $\ell$-isogenies.

A related problem is the following: Given an elliptic curve $E$ over $\mathbb{Z}/NZ$, find an elliptic curve $\ell$-isogeneous to $E$. A harder version of this is equivalent to factoring.

**Theorem 6** ([AC18 Thm. 3.3]). If we can find all $\ell$-isogeneous neighbors to $E$ in expected polynomial time, then we can factoring $N$ in expected polynomial time.

**Proof (sketch).** The $\ell$-isogeneous neighbors of $E$ are the roots of $\Phi_{\ell}(j, X) \mod N$. The roots of this polynomial are in bijection with the cartesian product of the roots in $\mathbb{F}_p$ and the roots in $\mathbb{F}_q$. Therefore, we should be able to find roots $j_1, j_2 \in \mathbb{Z}/NZ$ such that $j_1 \equiv j_2 \mod p$ and $j_1 \not\equiv j_2 \mod q$. Then $\gcd(j_1 - j_2, N)$ is a non-trivial divisor of $N$. 

2
Example 7. Let \( N = 109 \cdot 113 \). The roots of \( \Phi_5(7104, X) \) in \( \mathbb{Z}/N\mathbb{Z} \) are 9031 and 12192. The gcd of their difference with \( N \) is 109.

The main obstacle to adapting this proof to the original problem stated above, is an efficient method for sampling pairs \( j_0, j_1 \) with \( \Phi_\ell(j_0, j_1) \equiv 0 \mod N \).

3.1 Modular Curves

Suppose \( X_0(\ell) \) has genus \( \leq 1 \). Then we may be able to find many rational points on \( X_0(\ell) \). In particular, this gives us many pairs of \( j \)-invariants \( (j_1, j_2) \) which satisfy \( \Phi_\ell(X, Y) \). However, it is unclear how to use this to solve the previous problems. It may be possible to use this to reduce the \( (\ell, \ell^2) \)-isogeny problem to factoring in the case of small \( \ell \). That is, it may be possible to prove that finding a single \( \ell \)-isogeneous neighbor is equivalent to factoring if \( X_0(\ell) \) has genus 0 (or genus 1 with a known rational point over \( \mathbb{Z}/N\mathbb{Z} \) of large order). It may also be possible to provide some numerical experiments to conjecture such a result should hold for arbitrary \( \ell \).

4 Equivalence to Factoring

It was proved in [KK98] that counting \( \#E(\mathbb{Z}/N\mathbb{Z}) \) is equivalent to factoring \( N \). The proof is essentially Lenstra’s elliptic curve factorization algorithm.

A quick overview of [KK98 Sec. 3]: Suppose we have a black box to compute \( \#E(\mathbb{Z}/N\mathbb{Z}) \). We want 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 point addition formula we had to “divide by 0”, which corresponds to finding a factor of \( N \). Otherwise we repeat the process.

Problem 8. Adapt the Kunihiro-Koyama reduction theorem to the case where the endomorphism rings \( \text{End} E/F_p \) for prime factors \( p \) of \( N \) are all isomorphic.

A related problem is given an elliptic curve \( E \) over \( \mathbb{Z}/N\mathbb{Z} \), where \( N = pq \), determine whether \( \text{End} E/F_p \cong \text{End} E/F_q \). This should be done without factoring \( N \).

Remark 9. In the context of [AC18], we should focus only on the case where \( E/F_p \) is ordinary. But the question makes sense for arbitrary curves. Therefore it also makes sense to ask for \( \text{End} E/F_p \) to be isomorphic.
Example 10. Let $E$ be the elliptic curve given by $Y^2 = X^3 + X$. In this case,

$$\text{End}_{\mathbb{F}_p} E \cong \begin{cases} \mathbb{Z}[i] & p \equiv 1 \mod 4 \\ \mathbb{Z}[\sqrt{-p}] & p \equiv 3 \mod 4 \end{cases}$$

and

$$\text{End}_{\mathbb{F}_q} E \cong \begin{cases} \mathbb{Z}[i] & p \equiv 1 \mod 4 \\ \left(\frac{-p}{q}\right) & p \equiv 3 \mod 4 \end{cases}$$

Assume that $p, q > 2$. Then $p \equiv q \mod 4$ if and only if $N \equiv 1 \mod 4$. Therefore we can quickly test whether $E/\mathbb{F}_p$ and $E/\mathbb{F}_q$ have the same endomorphism ring. However, it is difficult to decide which case we are in. That is, given that $N \equiv 1 \mod 4$, we do not know how to efficiently test whether $p \equiv q \equiv 1 \mod 4$ or $p \equiv q \equiv 3 \mod 4$. This question is equivalent to asking whether $N$ is a sum of two squares.

References

