Research Article

Travis Scholl*

Isolated elliptic curves and the MOV attack

DOI: 10.1515/jmc-2016-0053
Received September 13, 2016; revised April 28, 2017; accepted May 1, 2017

Abstract: We present a variation on the CM method that produces elliptic curves over prime fields with nearly prime order that do not admit many efficiently computable isogenies. Assuming the Bateman–Horn conjecture, we prove that elliptic curves produced this way almost always have a large embedding degree, and thus are resistant to the MOV attack on the ECDLP.

Keywords: Elliptic curves, isogenies, isolated curves, embedding degree, cryptography, distribution of primes

MSC 2010: 11G20, 94A60, 14H52, 14K02

Communicated by: Hugh Williams

1 Introduction

The security of elliptic curve cryptosystems is based on the difficulty of the elliptic curve discrete logarithm problem (ECDLP). For an elliptic curve E over a prime field $\mathbb{F}_p$, the best known generic attack on the ECDLP takes roughly $\sqrt{p}$ operations. Suppose that a new algorithm $\mathcal{X}$ was found that could solve the ECDLP on a subset W of elliptic curves over $\mathbb{F}_p$ faster than all previously known algorithms. Given an instance of the ECDLP on E, if an attacker could construct an isogeny $\varphi : E \to E'$ with $E' \in W$, then they could transfer the instance to E' where they could use $\mathcal{X}$. The total time for this attack is bounded below by the time m that it takes to compute φ. If $m \geq \sqrt{p}$, then this attack is no faster than generic algorithms, no matter how fast $\mathcal{X}$ is. Let $\mathcal{T}$ denote the set of curves E' such that an isogeny $\varphi : E \to E'$ can be computed in less than $\sqrt{p}$ time. We will assume that the probability that a random curve in $\mathcal{T}$ lies in W, is roughly the ratio ϵ of $|W|$ to the number of elliptic curves over $\mathbb{F}_p$. For a random E, we expect that $|\mathcal{T}| \approx \sqrt{p}$, which in practice is $\approx 2^{128}$. However, it is possible for $|\mathcal{T}|$ to be much smaller, so that E is resistant to this attack. For example, if $\epsilon \approx 2^{-50}$ and $|\mathcal{T}| \leq 1000$, then the probability that the ECDLP on E can be efficiently transferred to some $E' \in W$ is about 2^{-40}. In this case, we call E isolated (a precise definition is given below). In this paper, we give an algorithm based on the complex multiplication (CM) method to generate isolated elliptic curves that are suitable for cryptography.

Remark 1.1. The hypothetical attack outlined above is motivated by the case of elliptic curves over composite degree extensions of prime fields (usually $\mathbb{F}_2$). In that case, Weil descent can sometimes be used to solve the ECDLP significantly faster than generic methods on a small but non-negligible proportion of curves [26, 27].

The *conductor gap* (see Definition 3.1) between two elliptic curves measures the difficulty of constructing an isogeny between them. If the conductor gap between E and E' is L, then the fastest known algorithm for computing an isogeny between E and E' takes roughly L^3 time. We say an elliptic curve E is (L, T)-*isolated* if

***Corresponding author: Travis Scholl:** Department of Mathematics, University of Washington, Seattle WA 98195, USA, e-mail: tscholl2@uw.edu. http://orcid.org/0000-0003-3039-4824

there are at most T curves whose conductor gap with E is at most L. For example, if E is $(p^{1/6}, 1000)$-isolated, then there are at most 1000 curves E' for which it would be feasible to construct an isogeny $E \to E'$. Thus E is most likely resistant to the hypothetical attack described above.

In addition to being resistant to the hypothetical attack above, isolated curves should be resistant to known attacks on the ECDLP, such as the MOV attack, named after the authors of [25]. The MOV attack reduces the ECDLP on an elliptic curve $E/\mathbb{F}_p$ to $\mathbb{F}_{p^k}^\times$. The smallest possible k is called the *embedding degree*. This reduction is only practical if k is $< \log^2 p$. Our main theorem shows that, under the Bateman–Horn conjecture, curves produced by our algorithm almost always have embedding degree larger than $\log^2 p$.

Theorem 1.2. *Assume the Bateman–Horn conjecture. There is an algorithm that takes as input a bound M, and returns an elliptic curve E over a prime field $\mathbb{F}_p$ such that the following hold:*
(i) $M/2 \le p \le M$,
(ii) $\#E(\mathbb{F}_p) = rf$, *where r is prime and $f \mid 24$,*
(iii) *E is $(\sqrt{p/50 - 100}, 8)$-isolated.*
The expected running time of the algorithm is $O(\log^3 M)$ multiplied by the time required to test if an integer of size M is prime. If M is sufficiently large, then the probability that the returned curve has an embedding degree less than $\log^2 p$, is bounded above by

$$C\frac{\log^8 M}{\sqrt{M}}$$

for some effectively computable constant C.

Remark 1.3. The Bateman–Horn conjecture is used to estimate how often several polynomials are simultaneously prime. While the conjecture gives an asymptotic formula for any collection of polynomials, we only require a big-Ω statement for how often three particular polynomials are simultaneously prime (see Problem 6.2).

Remark 1.4. Experimentally, our algorithm works well when $M \approx 2^{256}$. After several thousand iterations, it never produced a curve with embedding degree $> \log^2 p$ and finished within the expected time (see Section 6.4). However, we are unable prove an explicit lower bound for what "sufficiently large" is, nor can we give a computable upper bound for the implicit constant in the big-O notation for the run time. In Section 6, we discuss these points as well as provide a reasonable assumption to solves these issues.

Theorem 1.2 should be compared with the generic probability that a curve with prime order has embedding degree $< \log^2 p$.

Theorem 1.5 (Balasubramanian and Koblitz [1, Theorem 2]). *Let p be a uniformly random prime in the interval $[M/2, M]$, and E a random elliptic curve over $\mathbb{F}_p$ of prime order. The probability that the embedding degree of E is less than $\log^2 p$, is bounded above by*

$$C\frac{\log^9 M(\log\log M)^2}{M},$$

for some effectively computable constant C.

Remark 1.6. When giving a conditional theorem in cryptography, it is important to avoid contrived conjectures that are custom built to fill gaps in security proofs [21], [19, Section 1.4.2]. The Bateman–Horn conjecture is of independent interest. It predates elliptic curve cryptography, and is a generalization of the well-known hypothesis H from Schinzel [31]. It is supported by substantial theoretical and numerical evidence. For this reason we feel that the use of the conjecture is justified.

The rest of the paper is organized as follows. In Section 2 we briefly review background material as well as set notation for the rest of the paper. In Section 3 we define isolated curves, and in Section 4 we outline a method for generating them. In Section 5 we show that our algorithm has a high probability of producing curves that are resistant to the MOV attack, and prove Theorem 1.2. In Section 6, we explain some limitations of our results and give some heuristics suggesting that these limitations do not appear in practice.

2 Background and notation

Let E be an elliptic curve over a prime field $\mathbb{F}_p$. We will primarily consider primes on the order of 2^{256}. Let $N = |E(\mathbb{F}_p)|$ be the number of points, and $t = p + 1 - N$. If $t \equiv 0 \bmod p$ then E is vulnerable to the MOV attack [25], so we will only consider the case when $t \not\equiv 0 \bmod p$. In this case E is called *ordinary*.

An *isogeny* is a surjective morphism of elliptic curves with finite kernel. The set of isogenies $E \to E$ defined over the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$, together with the 0 map form the *endomorphism ring* $\operatorname{End} E = \operatorname{End}_{\overline{\mathbb{F}}_p} E$. If E is ordinary then $\operatorname{End} E$ is isomorphic to an order in an imaginary quadratic field K.

Let $\pi \in \operatorname{End} E$ denote the Frobenius endomorphism, which on the level of points takes $(x, y) \mapsto (x^p, y^p)$. We identify π with an element of K. Then $\operatorname{Tr} \pi = t$ and $\operatorname{Norm}(\pi) = p$ [34, Chapter V]. This means that we can identify $\pi = \frac{t+c\sqrt{-d}}{2}$, where $-d = \operatorname{Disc} K$ and $c > 0$. Notice that $\mathbb{Z}[\pi]$ is the order in K of conductor c, and that

$$4p = t^2 + dc^2. \tag{2.1}$$

Given an elliptic curve E, there is an associated number $j(E)$ which determines the isomorphism type of E over $\overline{\mathbb{F}}_p$. $j(E)$ is called the *j-invariant of E*. Throughout the rest of the paper, unless otherwise noted, E will represent an ordinary elliptic curve over the prime field $\mathbb{F}_p$.

2.1 Isogeny classes

Definition 2.1. The *isogeny class* I of E is the set of isomorphism classes (over $\mathbb{F}_p$) of elliptic curves that are isogenous (over $\mathbb{F}_p$) to E.

The isogeny class of E is uniquely determined by $N = \#E(\mathbb{F}_p)$. This follows from Tate's isogeny theorem, which says that two elliptic curves over $\mathbb{F}_p$ are isogenous if and only if they have the same number of points [34, Exercise. 5.4]. For every integer N in the Hasse interval $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$, there is an elliptic curve with N points. Thus by Tate's thereof, there are about $4\sqrt{p}$ isogeny classes. One can show using the j-invariant that there are roughly $2p$ isomorphism classes of elliptic curves over $\mathbb{F}_p$. This means that on average, each isogeny class has about $\sqrt{p}/2$ curves.

An *ℓ-isogeny* is an isogeny of degree ℓ. We will only consider ℓ-isogenies with ℓ a prime other than p. Such isogenies are separable and have a kernel of size ℓ. Any separable isogeny between elliptic curves factors into a composition of isogenies of prime degree.

2.2 Endomorphism classes

The isogeny class I of E can be partitioned into endomorphism classes. Let $I_{\mathcal{O}}$ denote the set of curves in I whose endomorphism ring is isomorphic to $\mathcal{O}$, an order in an imaginary quadratic field. We call $I_{\mathcal{O}}$ the *endomorphism class of $\mathcal{O}$ in I*.

Proposition 2.2. *The endomorphism classes in I are precisely those associated to orders in the quadratic imaginary field $\mathbb{Q}(\pi)$ that contain $\mathbb{Z}[\pi]$. For any $\mathcal{O} \supseteq \mathbb{Z}[\pi]$, the size of $I_{\mathcal{O}}$ is equal to the class number $h(\mathcal{O})$.*

Proof. See Theorems 4.3 and 4.5 from [32]. □

Endomorphism classes have $O(\sqrt{p} \log d)$ curves. To see this, let c' be the conductor of an order appearing in I. Recall that the class number of an order of conductor c' is approximately hc' (see [9, Theorem 7.24] for a precise formula). The class number h is bounded above by $\frac{1}{\pi}\sqrt{d} \log d$ [6, Excercise 5.27 b]. We also know that c' divides c because every order appearing in I contains the Frobenius ring $\mathbb{Z}[\pi]$. It follows from (2.1) that $hc' \le hc \le \frac{c}{\pi}\sqrt{d} \log d < \frac{2}{\pi}\sqrt{p} \log d$.

For a random curve E over $\mathbb{F}_p$ for a random prime p, we expect that c is close to 1 [16, Sec. 6]. Because the endomorphism classes in I correspond to divisors of c, we do not expect to find many endomorphism classes. Thus on average, we should expect that $I_{\operatorname{End} E}$ usually has roughly $\sqrt{p}$ curves.

2.3 Bateman–Horn conjecture

We will be interested in how often several polynomials are simultaneously prime. For a single polynomial of degree one, we have the prime number theorem and Dirichlet's theorem on primes in arithmetic progressions. Bateman and Horn made the following conjecture based on heuristics derived from the prime number theorem.

Definition 2.3. We say that a polynomial $f \in \mathbb{Z}[x]$ satisfies *Bunyakovsky's property* if $\gcd_{a\in\mathbb{Z}} f(a) = 1$.

Warning 1. In order for f to satisfy Bunyakovsky's property, it is necessary that the coefficients of f are relatively prime. This condition is not sufficient, for example $\gcd_{a\in\mathbb{Z}}(a^2 + a) = 2$.

Conjecture 2.4 (Bateman–Horn Conjecture [2]). Let $f_1, \dots, f_k \in \mathbb{Z}[x]$ be distinct irreducible polynomials such that their product $\prod f_i$ satisfies Bunyakovsky's property. Let

$$P_{f_1,\dots,f_k}(N) = \{a \in \mathbb{Z} : 1 \le a \le N \text{ and } f_i(a) \text{ is prime for all } i = 1, \dots, k\}.$$

Then

$$|P_{f_1,\dots,f_k}(N)| \sim \frac{C}{D}\frac{N}{\log^k N}. \tag{2.2}$$

Here $D = \prod \deg f_i$, $C = \prod_{\ell \text{ prime}} \frac{1-\omega(\ell)/\ell}{(1-1/\ell)^k}$, and $\omega(\ell)$ denotes the number of roots of $\prod f_i$ in $\mathbb{F}_\ell$.

Remark 2.5. There is a large amount of theoretical and numerical evidence for the Bateman–Horn conjecture. It reduces to Dirichlet's theorem on primes in arithmetic progressions for a single polynomial of degree 1. It also agrees with the twin prime conjecture and the Sophie Germain prime conjecture [33, Section 5.5]. More recently, an analog of the conjecture has been proven for function fields [10].

2.4 The MOV attack

The MOV attack transfers a discrete log from $E(\mathbb{F}_p)$ to $\mathbb{F}_{p^k}^\times$ for some positive integer k. The idea is to leverage sub-exponential time algorithms for solving discrete logs in the multiplicative group of a finite field. A necessary condition for this transfer is that $|E(\mathbb{F}_p)|$ divides $p^k - 1$. The smallest possible k is called the *embedding degree*[1] of E. This is the same as the multiplicative order of p in $(\mathbb{Z}/N\mathbb{Z})^\times$, where $N = |E(\mathbb{F}_p)|$. For more on the MOV attack see [25][2] or [34, Section XI.6].

If $k > \log^2 p$, then the MOV attack will not be faster than trying to solve the discrete log on E directly [1]. Therefore we are primarily interested in curves with embedding degree $> \log^2 p$.

3 Isolated curves

Definition 3.1. The *conductor gap* of two orders in a fixed quadratic imaginary field is the largest prime dividing the conductor of one and not the other. The conductor gap between two isogenous elliptic curves is defined to be the conductor gap of their endomorphism rings. If the curves are not isogenous, then their conductor gap is ∞. The *L-conductor-gap class* of a curve E is the set of all curves E' such that the conductor gap between E and E' is less than L.

---

1 The embedding degree may also refer to the multiplicative order of p in $(\mathbb{Z}/r\mathbb{Z})^\times$, where r is the largest prime factor of N. This is because cryptosystems are usually constructed using the largest prime order subgroup of the elliptic curve group, rather than the entire group. We will only be interested in curves with nearly prime order, so the difference between using N or r is not important. Also implicitly we are avoiding anomalous curves where $N = p$, i.e. $t = 1$. Anomalous curves are extremely rare but should be avoided as there are known attacks against them [35].

2 Technically, the attack of [25] requires that N be relatively prime to $p - 1$. But, if this is not the case, then there is an attack described by Frey and Rück [12] which also transfers the ECDLP to $\mathbb{F}_{p^k}^\times$. We will not differentiate between the two since both attacks require a small embedding degree.

Proposition 3.2. *Let $\varphi : E \to E'$ be an ℓ-isogeny for some prime ℓ. If $\mathcal{O}$ and $\mathcal{O}'$ are the endomorphism rings of E and E', respectively, then one of the following holds:*

$$[\mathcal{O} : \mathcal{O}'] = \ell, \quad [\mathcal{O}' : \mathcal{O}] = \ell, \quad \mathcal{O} = \mathcal{O}'.$$

Proof. See [22, Proposition 21]. □

In the first two cases of Proposition 3.2, we say that φ is *vertical*; otherwise φ is *horizontal*. Horizontal isogenies stay inside the same endomorphism class while vertical ones move to a new class. The main implication of Proposition 3.2 is that if two endomorphism classes have conductor gap a prime ℓ, then any isogeny between them factors through an ℓ-isogeny. Unless otherwise noted, throughout the rest of the paper ℓ will denote a prime not equal to p.

Definition 3.3. Let E be an elliptic curve over $\mathbb{F}_p$. We will say E is *isolated with gap L and set-size T*, or (L, T)-isolated, if the L-conductor-gap class of E has at most T curves.

Remark 3.4. The observation that isolated curves are resistant to isogeny based attacks has been noted before in the literature. This idea is discussed in [20, Section 11.2], [17, Section 7.1], and [26, Remark 6]. This idea has also been applied to Jacobians of curves of genus 2, cf. [37].

3.1 Computational complexity of isogenies

The computational complexity of an isogeny depends on its degree, but the complexity is different for horizontal and vertical isogenies. The fastest known method [22] for constructing a vertical isogeny from E involves constructing the modular polynomial Φ_ℓ. Finding $\Phi_\ell \bmod p$ is the most expensive step and the best known methods take $\widetilde{O}(\ell^3)$ time and $\widetilde{O}(\ell^2)$ space [4] (recall that $\widetilde{O}(f)$ means $O(f \log^k f)$ for some integer k); Φ_ℓ is a polynomial of degree $\ell + 1$ in two variables, so any method which involves computing Φ_ℓ must take $\Omega(\ell)$ time and space. Moreover, because we represent ℓ-isogenies using either polynomials of degree ℓ, or a list of points in the kernel; any algorithm which computes an ℓ-isogeny will need at least $\Omega(\ell)$ space.

For horizontal isogenies where the endomorphism ring has a small discriminant, there are much faster algorithms which are polynomial in $\log \ell$, cf. [3, 18]. These methods do not extend to vertical isogenies crossing a large conductor gap. Therefore we can only effectively transport the ECDLP to another endomorphism class when the conductor gap is less than $p^{1/6}$.

The best algorithm known for solving the ECDLP on a general elliptic curve takes $\widetilde{O}(\sqrt{p})$ time [28]. If $\ell \geq p^{1/6}$, then computing a vertical ℓ-isogeny takes similar time to solving the ECDLP. If two endomorphism classes have a conductor gap of at least $p^{1/6}$, then there is no significant benefit in transferring the ECDLP across the gap.

3.2 Examples

Example 3.5. Let E be the elliptic curve $y^2 = x^3 + 6x$ over $\mathbb{F}_p$, where $p = 12475737285765000161 \approx 2^{63.4}$. Note that $\operatorname{End} E \cong \mathbb{Z}[i]$ has class number 1, so E is the only curve in its endomorphism class. The Frobenius endomorphism π generates an order $\mathbb{Z}[\pi]$ with prime conductor $c = 2559154831 \approx 2^{31.2}$. This means that the isogeny class of E has two endomorphism classes: one which contains only E, and another which contains $h(\mathbb{Z}[\pi]) = 1279577416 \approx 2^{30.2}$ curves. Because the conductor gap between the classes is $c \approx \sqrt{p}$, this shows that E is isolated with gap 2^{31} and set-size 1.

Example 3.6. Let E be the elliptic curve $y^2 = x^3 + 350x$ over $\mathbb{F}_p$, where $p = 122501$. As in the previous example, the endomorphism class of E has only one curve. However, in this case $\mathbb{Z}[\pi]$ has conductor 1, so the isogeny class of E contains only E, and E is $(\infty, 1)$-isolated. This example is highly atypical because the trace $t = 700 = \lfloor 2\sqrt{p} \rfloor$ is at the extreme end of the Hasse bound.

4 Generating isolated curves

In this section we give an algorithm to generate isolated elliptic curves. We will apply some slight modifications to the algorithm presented here in order to prove Theorem 1.2. For use in cryptography, we would like to generate prime ordered curves. However there are some basic obstructions to a curve having prime order. For example, consider equation (2.1). In order for p to be an odd prime, if d is even then t must be even. It follows that $N = p + 1 - t$ is also even. In this case, the choice of d forced a factor of 2 to divide N. Fortunately, the only obstructions to N being prime are a few factors of 2 and 3.

For any integer $a \equiv 0, 3, 4 \bmod 8$, define[3] the *cofactor* to be

$$\mathrm{cof}_a = 2^{v_2} \cdot 3^{v_3}, \tag{4.1}$$

where

$$v_2 = \begin{cases} 0 & \text{if } a \equiv 3, 11, 19, 27 \bmod 32, \\ 1 & \text{if } a \equiv 4, 8, 20, 24 \bmod 32, \\ 2 & \text{if } a \equiv 0, 12, 16 \bmod 32, \\ 3 & \text{if } a \equiv 28 \bmod 32, \end{cases}$$

$$v_3 = \begin{cases} 0 & \text{if } a \not\equiv 2 \bmod 3, \\ 1 & \text{if } a \equiv 2 \bmod 3. \end{cases}$$

The algorithm proceeds as follows.

Algorithm 1. Isolated curve.

Input: a positive integer M and fundamental discriminant $-d < 0$.
Output: an elliptic curve defined over $\mathbb{F}_p$, where $\frac{dM}{16} < p < \frac{dM}{4}$.

1: **repeat** Steps 2–5
2: $t \leftarrow$ random integer in $[-\sqrt{M}, \sqrt{M}] \setminus \{0, 1, 2\}$
3: $c \leftarrow$ random integer in $[\frac{\sqrt{M}}{2}, \sqrt{M}]$
4: $p \leftarrow \frac{t^2+dc^2}{4}$
5: $N \leftarrow p + 1 - t$
6: **until** p, N/cof_{dc^2} are integers and p, c, N/cof_{dc^2} are prime
7: $j \leftarrow$ root of the Hilbert class polynomial for $\mathbb{Q}(\sqrt{-d})$ mod p
8: $E \leftarrow$ elliptic curve over $\mathbb{F}_p$ with $j(E) = j$ and $|E(\mathbb{F}_p)| = N$
9: **return** E

Remark 4.1. Algorithm 1 is not optimized for efficiency. For example, if $d \equiv 0 \bmod 4$, then t must be even. Thus by choosing only even values of t in Step 2, we expect the runtime to be reduced by a factor of 2. We present the unoptimized version for simplicity.

Remark 4.2. The reason for removing $0, 1, 2$ from possible values of t is to avoid the attacks described in [35], [25], and [12].

Remark 4.3. One drawback[4] of using the CM method is that we do not have full control over the prime p. That is, we can not choose p arbitrarily and then construct an isolated curve over $\mathbb{F}_p$. This makes it more

3 The value of cof_a was calculated by considering the equation $4N = (t-2)^2 + a$ modulo powers of 2 and 3. Here a represents dc^2 from equation (2.1).

4 We would like to thank the referee for pointing out this drawback.

difficult to find p with special properties, such as a small Hamming weight (which can lead to more efficient implementations). However, we can lower the Hamming weight of p with the following modifications. Instead of choosing c randomly, fix c to be a large prime of small Hamming weight. Also, restrict the search for t to integers with small Hamming weight. Because p is given by a simple expression in t and c, the resulting value of p will likely have small Hamming weight.

First we will explain the last steps of the algorithm. The following facts are the basis of the well-known CM method [7, Section 18.1]:
(i) The Hilbert class polynomial of $K = \mathbb{Q}(\sqrt{-d})$ has a root in $\mathbb{F}_p$ by construction.
(ii) There exists an elliptic curve $E/\mathbb{F}_p$ with N points and $j(E) = j$.
An efficient algorithm for finding E, given j and N can be found in [30]. Since $j(E)$ is a root of the Hilbert class polynomial mod p, it follows that $\operatorname{End} E \cong \mathcal{O}_K$, cf. [36, Section 2.8]. If the choice of d is bounded by a constant, then Steps 7 and 8 in the algorithm have a running time of $O(1)$. The main factor in the running time comes from the loop in Steps 2 through 5.

Proposition 4.4. *If the main loop of Algorithm 1 terminates, then the curve E returned by the algorithm is isolated with gap $\frac{\sqrt{M}}{2}$ and set-size $\frac{1}{\pi}\sqrt{d}\log d$.*

Proof. We are assuming p, c, N/cof_{dc^2} are prime and we want to show that E is isolated. Let $K = \mathbb{Q}(\sqrt{-d})$. By the explanation above, $\operatorname{End} E \cong \mathcal{O}_K$. Let $\pi \in \operatorname{End} E$ denote the Frobenius endomorphism of E. In $\mathcal{O}_K$, π corresponds (up to conjugation) to $\frac{t+c\sqrt{-d}}{2}$. We also know that $c = [\mathcal{O}_K : \mathbb{Z}[\pi]]$. Because c was chosen to be prime, there are two endomorphism classes in the isogeny class of E corresponding to $\mathcal{O}_K$ and $\mathbb{Z}[\pi]$. The endomorphism class of $\mathcal{O}_K$ contains $h(\mathcal{O}_K) \le \frac{1}{\pi}\sqrt{d}\log d$ curves. Therefore, E is isolated with gap $c \ge \frac{\sqrt{M}}{2}$ and set-size $\frac{1}{\pi}\sqrt{d}\log d$. □

Remark 4.5. It is easy to alter Algorithm 1 to produce curves that are $(\infty, 1)$-isolated, meaning that the entire isogeny class contains a single curve, similar to Example 3.6. To do this, we choose d such that $\mathbb{Q}(\sqrt{-d})$ has class number 1, and fix $c = 1$. However, we do not know how to prove that curves generated this way usually have an embedding degree $> \log^2 p$. This is because there are too few values of t such that p and N/cof_d are simultaneously prime. Even though the Bateman–Horn conjecture gives an asymptotic formula, it is not enough to prove a bound on the embedding degree using the methods in Section 5.

5 Improbability of the MOV attack on isolated curves

5.1 Notation

In [1], Balasubramanian and Koblitz proved that a random prime order elliptic curve over a random prime field almost always has a large embedding degree. Their work has been extended in several ways [8, 24]. We want to emulate the main theorem of [1] for isolated curves. The main difference is that in [1], the authors were able to vary the prime and the number of points subject only to the Hasse bound. There is less flexibility in our case due to restrictions on the conductor c and the discriminant d.

We will use the following notation:
- $-d$ is a fixed small (< 100) fundamental discriminant of a quadratic imaginary field,
- $p = p(t, c) = \frac{t^2+dc^2}{4}$,
- $N = N(t, c) = p + 1 - t$,
- $\mathrm{cof} = \mathrm{cof}(c) = \mathrm{cof}_{cd^2}$ as defined in Section 4,
- $r = r(t, c) = \frac{N}{\mathrm{cof}}$.

Remark 5.1. Note that r is *not* a polynomial in t, c because $\mathrm{cof}(c)$ depends only on the valuation of dc^2 at 2 and 3. We will apply a linear change of variables in c in order to fix the cofactor.

Define the following sets:

$$\begin{aligned} S_M &= \{(t,c) \in [1, \sqrt{M}] \times [\sqrt{M}/2, \sqrt{M}] : p, r, c \text{ are prime}\},\\ S_{M,K} &= \{(t,c) \in S_M : \text{the order of } p \text{ in } (\mathbb{Z}/r\mathbb{Z})^\times \text{ is at most } K\},\\ S_M(t) &= \{c : (t,c) \in S_M\},\\ S_{M,K}(t) &= \{c \in S_M(t) : (t,c) \in S_{M,K}\}. \end{aligned}$$

The set S_M represents possible pairs t, c that Algorithm 1 could use to generate an isolated curve. In particular, the expected number of pairs t, c sampled by Algorithm 1 is $\frac{|S_M|}{M}$. The set $S_{M,K}$ represents those pairs which result in a curve with embedding degree at most K. The sets $S_M(t)$ and $S_{M,K}(t)$ represent pairs with a fixed t value.

5.2 Main results

Our goal for this subsection is to find an upper bound for $\frac{S_{M,K}(t_0)}{S_M(t_0)}$ for a fixed integer t_0. This is roughly the probability that Algorithm 1 returns a curve with embedding degree at most K given that $t = t_0$.

First we give an upper bound for $S_{M,K}(t_0)$.

Proposition 5.2. *Let K, M be any positive integers. Then there is a universal constant $\mathcal{A}_1$ such that for any integer t_0 with $|t_0| > 1$,*

$$|S_{M,K}(t_0)| < \mathcal{A}_1 K^2 \log|t_0|.$$

Proof. Let $L_k = \{\text{primes } \ell : \ell \mid (t_0 - 1)^k - 1\}$. By construction

$$r \mid p^k - 1 \iff r \mid (p - N)^k - 1 = (t_0 - 1)^k - 1.$$

Hence there is a map $\varphi : S_{M,K}(t_0) \to \bigcup_{k=1}^K L_k$ given by $c \mapsto r(t_0, c)$.

Next we will show that $|\varphi^{-1}(\ell)| \le 16$. Note that $N(t_0, c)$ is a quadratic polynomial in c, so there are at most two values of c such that $N(t_0, c)$ is the same. There are eight possible values of cof_c, hence there are at most sixteen values of c which could give the same value of $r(t_0, c)$. Therefore

$$|S_{M,K}(t_0)| = \left|\varphi^{-1}\left(\bigcup_{k=1}^K L_k\right)\right| \le 16\left|\bigcup_{k=1}^K L_k\right|.$$

It remains to bound the L_k. The number of prime divisors of $(t_0 - 1)^k - 1$ is bounded by $\log_2 |t_0 - 1|^k \le k \log_2(|t_0| + 1)$. Hence

$$\left|\bigcup_{k=1}^K L_k\right| \le \sum_{k=1}^K |L_k| \le \sum_{k=1}^K k \log_2(|t_0| + 1) = \frac{K(K+1)}{2} \log_2(|t_0| + 1) \le 2.4K^2 \log(|t_0|).$$

The last inequality holds for all $|t_0| \ge 2$, so we may take $\mathcal{A}_1 = 2.4$. □

Next we will to bound $S_M(t_0)$ from below. Because t_0 is fixed, we will be able to apply the Bateman–Horn conjecture. However, in order to apply the conjecture, we first need a change of coordinates which makes p and r into polynomials satisfying Bunyakovsky's property.

Lemma 5.3. *Let $-d$ be a fundamental discriminant for a quadratic imaginary field such that $d < 100$. Then there are computable constants $m_1, b_1, m_2, b_2 \in \mathbb{Z}_{\ge 0}$ such that the linear change of variables $t' = t'(t) = m_1 t + b_1$ and $c' = c'(c) = m_2 c + b_2$ satisfy:*

(i) *$f_{d(c')^2}$ is constant as a function of c.*

(ii) *$p' = p(t', c')$ and $r' = r(t', c')$ are integer polynomials in t and c.*

(iii) *For any $t \in \mathbb{Z}$, the product $p' \cdot r' \cdot c'/\gcd(m_2, b_2)$ satisfies Bunyakovsky's property as a polynomial in c.*

Remark 5.4. In condition (iii) of Lemma 5.3, we include $c'/\gcd(m_2, b_2)$ rather than just c' because of the case $d \equiv 7 \bmod 8$. In this case, $p = \frac{t^2 + dc^2}{4}$ is an odd integer only if t and c are even. In particular, we cannot have both c' and p' simultaneously prime when $d \equiv 7 \bmod 8$.

d	t'	c'	d	t'	c'
3	$2160t+1$	$2c+1$	51	$624240t+1$	$2c+1$
4	$3840t$	$2c+1$	52	$648960t+4$	$2c+1$
7	$94080t+10$	$4c$	55	$5808000t+18$	$4c$
8	$46080t+6$	$6c+1$	56	$2257920t+6$	$6c+1$
11	$87120t+15$	$6c+1$	59	$2506320t+15$	$6c+1$
15	$432000t+34$	$4c$	67	$1077360t+1$	$2c+1$
19	$86640t+1$	$2c+1$	68	$3329280t+12$	$6c+1$
20	$288000t+24$	$6c+1$	71	$783976320t+10$	$12c$
23	$82270080t+10$	$12c$	79	$11982720t+10$	$4c$
24	$138240t+10$	$2c+1$	83	$4960080t+3$	$6c+1$
31	$1845120t+10$	$4c$	84	$1693440t+40$	$2c+1$
35	$882000t+3$	$6c+1$	87	$14532480t+10$	$4c$
39	$2920320t+10$	$4c$	88	$1858560t+6$	$2c+1$
40	$384000t+6$	$2c+1$	91	$1987440t+1$	$2c+1$
43	$443760t+1$	$2c+1$	95	$1403568000t+34$	$12c$
47	$343543680t+10$	$12c$			

Table 1. Choices of t',c' in Lemma 5.3 found using Sage [38].

Proof of Lemma 5.3. We will prove the claim in detail for $d=4$ by showing $t'=3840t$ and $c'=2c+1$ satisfy properties (i)–(iii). The other cases are similar, and the corresponding change of coordinates are given in Table 1.

(i) For any c, we have that $d(c')^2 \equiv 4 \bmod 32$ and $d(c')^2 \not\equiv 2 \bmod 3$. Hence $\mathrm{cof}_{d(c')^2}=2$ for all c.

(ii) To show p' and r' are integer polynomials, we just have to expand out the definitions:

$$p' = p(t',c') = 3686400t^2+4c^2+4c+1,$$
$$r' = r(t',c') = \frac{N(t',c')}{2} = 1843200t^2+2c^2-1920t+2c+1.$$

(iii) Let $g(t,c)=p'\cdot r'\cdot c' \in \mathbb{Z}[t,c]$ and $t_0\in\mathbb{Z}$. To show that $g(t_0,c)\in\mathbb{Z}[c]$ satisfies Bunyakovsky's property, it is sufficient to check that $\gcd\{g(t_0,0),\dots,g(t_0,5)\}=1$ as $g(t_0,c)$ is a degree 5 polynomial in c.[5] A direct computation[6] shows that

$$3g(t,0)+4g(t,1)+17g(t,2)-36g(t,3)+23g(t,4)-5g(t,5)=960.$$

Therefore

$$\begin{aligned}\gcd\{g(t_0,0),\dots,g(t_0,5)\} &= \gcd\{g(t_0,0),\dots,g(t_0,5),960\}\\ &= \gcd\{g(0,0),g(0,1),\dots,g(0,5)\}=1.\end{aligned}$$

The second to last equality follows from the fact that $t'\equiv 0 \bmod 960$ by construction. The last equality follows from the fact that $g(0,0)=1$. □

Remark 5.5. We expect Lemma 5.3 to hold for all d with many different possibilities for m_i, b_i.

Proposition 5.6. *Assume the Bateman–Horn conjecture and that $d<100$ and $d\not\equiv 7 \bmod 8$. Let m_1, b_1 be the constants from Lemma 5.3. For any integer t_0, there are constants $\mathcal{A}_2$, $\mathcal{B}_2$ such that for all $M>\mathcal{B}_2$,*

$$|S_M(m_1t_0+b_1)| > \mathcal{A}_2\frac{\sqrt{M}}{\log^3 M}.$$

The constants $\mathcal{A}_2$, $\mathcal{B}_2$ depend on t_0. Moreover, the constant $\mathcal{A}_2$ is effectively computable.

5 This condition is also sufficient, see [5, Exercise 1.3].

6 This computation was done by constructing the matrix with rows given by the coefficients of the $g(t,i)$, and then computing the Hermite normal form using Sage.

Proof. Let $t'(t) = m_1 t + b_1$ and $c'(c) = m_2 c + b_2$ be the change of coordinates given by Lemma 5.3. Then $p' = p(t'(t_0), c')$, $r' = r(t'(t_0), c')$, and c' are integer polynomials in $\mathbb{Z}[t, c]$, and satisfy Bunyakovsky's property. Moreover, p' and r' are irreducible because their roots are linear combinations of the roots of $p(t_0, c)$ and $N(t_0, c)$, respectively. The latter are complex as long as $t'(t_0) \neq 0, 2$. Thus p', r', and c' satisfy the hypothesis of the Bateman–Horn conjecture as polynomials in $\mathbb{Z}[c]$.

Let $S'_M(t_0)$ denote the set of c_0 such that $c'(c_0) \in S_M(t'(t_0))$, and

$$P_{p',r',c'}(\sqrt{M}) = \{c_0 \in [1, \sqrt{M}] : p'(c_0), r'(c_0), \text{ and } c'(c_0) \text{ are prime}\}.$$

By above, we can apply the Bateman–Horn conjecture to the polynomials p', r', and c'. This means that there is a constant $\mathcal{C}$, depending on the polynomials p', r', and c' (which depend only on d and t_0), such that

$$|P_{p',r',c'}(\sqrt{M})| \sim \mathcal{C}\frac{\sqrt{M}}{\log^3 \sqrt{M}}.$$

Notice that $S'_M(t_0) = P_{p',r',c'}(\sqrt{M}) \cap J(\sqrt{M})$, where $J(M) = [\frac{1}{m_1}(\frac{1}{2}\sqrt{M} - b_1), \frac{1}{m_1}(\sqrt{M} - b_1)]$. We will assume $M \gg \max\{m_1^2, 16b_1^2\}$ so that

$$\begin{aligned}
|S'_M(t_0)| &= \left|P\left(\frac{1}{m_1}\left(\frac{1}{2}\sqrt{M} - b_1\right)\right)\right| - \left|P\left(\frac{1}{m_1}(\sqrt{M} - b_1)\right)\right| \\
&\sim \mathcal{C}\frac{\frac{1}{m_1}(\frac{1}{2}\sqrt{M} - b_1))}{\log^3 \frac{1}{m_1}(\frac{1}{2}\sqrt{M} - b_1))} - \mathcal{C}\frac{\frac{1}{m}(\sqrt{M} - b_1))}{\log^3 \frac{1}{m_1}(\sqrt{M} - b_1))} \\
&\geq \frac{\mathcal{C}}{2m_1}\frac{\sqrt{M} - 2b_1}{\log^3 M} \\
&> \frac{\mathcal{C}}{4m_1}\frac{\sqrt{M}}{\log^3 M}.
\end{aligned}$$

Thus there is some constant $\mathcal{B}_2$ such that

$$|S'_M(t_0)| > \frac{\mathcal{C}}{4m_1}\frac{\sqrt{M}}{\log^3 M} \quad \text{for all } M > \mathcal{B}_2.$$

Note that the constant $\mathcal{B}_2$ depends on t_0. The map $c_0 \mapsto c'(c_0)$ gives us an inclusion $S'_M(t_0) \hookrightarrow S_M(t'(t_0))$. Therefore the inequality in the claim holds with $\mathcal{A}_2 = \frac{\mathcal{C}}{4m_1}$.

It remains to show that the constant $\mathcal{C}$ given in the Bateman–Horn conjecture is computable.[7] Let

$$g_1 = t_0^2 + dc^2, \quad g_2 = (t_0 - 2)^2 + dc^2, \quad g_3 = c, \quad \text{and} \quad G = g_1 \cdot g_2 \cdot g_3.$$

Define $\omega_i(p)$ to be the number of roots of g_i mod p and $\omega(p)$ to be the number of roots of G mod p. Then G differs from $p' \cdot r' \cdot c'$ by a linear change of coordinates and scaling. It follows that the constant $\mathcal{C}$ differs from the product

$$\mathcal{C}_2 = \prod_{p \geq 5} \frac{1 - \frac{\omega(p)}{p}}{(1 - \frac{1}{p})^3}$$

in at most a finite number of factors. So it is sufficient to show $\mathcal{C}_2$ is computable. Notice that for any prime $p \geq 5$:

$$\begin{aligned}
g_1(c) \equiv g_2(c) \equiv 0 \bmod p &\implies p \mid t_0 + 2, \\
g_1(c) \equiv g_3(c) \equiv 0 \bmod p &\implies p \mid t_0, \\
g_2(c) \equiv g_3(c) \equiv 0 \bmod p &\implies p \mid t_0 - 2.
\end{aligned}$$

7 The proof of convergence for the constant in the Bateman–Horn conjecture only relies on the Chebotarev density theorem. Hence by using an effective version [23], one can show that the constant is always effectively computable. However, we present this more direct proof which offers a more concrete picture of the constant.

Let S denote the set of primes dividing $6dt_0(t_0-2)(t_0+2)$. Then for any prime $p \notin S$,

$$\omega(p) = \omega_1(p) + \omega_2(p) + \omega_3(p).$$

Let $\chi(p) = 1$ if $-d$ is a square mod p and -1 otherwise. Then one can show that for any $p \notin S$ we have that

$$\omega_1(p) = \omega_2(p) = \chi(p) + 1,$$

therefore

$$\omega(p) = 2(\chi(p)+1) + 1.$$

Note that the product

$$\prod_p \frac{1 - \frac{2(\chi(p)+1)+1}{p}}{(1-\frac{1}{p})^3} = \mathcal{C}_3 \prod_p \Big(1 - \frac{\chi(p)}{p}\Big)^2,$$

where $\mathcal{C}_3$ is an effectively computable constant. By Dirichlet's analytic formula,

$$\prod_p \Big(1 - \frac{\chi(p)}{p}\Big)^2 = \Big(\frac{k\sqrt{d}}{2\pi h}\Big)^2,$$

where k, h are the number of roots of unity and class number of $\mathbb{Q}(\sqrt{-d})$, respectively. □

Theorem 5.7. *Assume the Bateman–Horn conjecture and that $d < 100$, and suppose $d \not\equiv 7 \bmod 8$. Let m_1, b_1 be the constants from Lemma 5.3, which depend only on d. For any fixed integer t_0, there are constants $\mathcal{A}_3, \mathcal{B}_3$ such that the probability that $c \in S_{M,K}(m_1t_0 + b_1)$ given that $c \in S_M(m_1t_0 + b_1)$ is bounded above by*

$$\mathcal{A}_3 \frac{K^2 \log^4 M}{\sqrt{M}}$$

for all $M > \mathcal{B}_3$. The constant $\mathcal{A}_3$ is computable.

Proof. We have to bound $S_{M,K}(m_1t_0 + b_1)/S_M(m_1t_0 + b_1)$ above. This follows immediately from the previous propositions. Proposition 5.2 gives an upper bound for $S_{M,K}(m_1t_0 + b_1)$, and Proposition 5.6 gives a lower bound for $S_M(m_1t_0 + b_1)$. □

Warning 2. We do not have a computable upper bound for the constant $\mathcal{B}_3$.

5.3 Proof of Theorem 1.2

We can now prove Theorem 1.2 using a modified version of Algorithm 1. In order to apply Theorem 5.7, we need to modify Algorithm 1 so that t lies in an interval independent of the input bound M.

Algorithm 2. Isolated curve.

Input: positive integer M.

Output: isolated (with gap $\sqrt{p/50 - 100}$ and set-size 8) elliptic curve defined over $\mathbb{F}_p$ with $M/2 \le p \le M$.

1: $-d \leftarrow$ fundamental discriminant such that $1 \le d \le 100$ and $d \not\equiv 7 \bmod 8$
2: $m_1, b_1, m_2, b_2 \leftarrow$ constants from Lemma 5.3
3: $t \leftarrow$ integer such that $3 \le t \le 100$ and $t \equiv b_1 \bmod m_1$
4: **repeat** Steps 5–7
5: $\quad c \leftarrow$ random integer in $[\sqrt{(2M - t^2)/d}, \sqrt{(4M - t^2)/d}]$ with $c \equiv b_2 \bmod m_2$
6: $\quad p \leftarrow \frac{t^2+dc^2}{4}$
7: $\quad N \leftarrow p + 1 - t$
8: **until** p, c, and $N/\mathrm{cof}(dc^2)$ are prime
9: $j \leftarrow$ root of the Hilbert class polynomial for $\mathbb{Q}(\sqrt{-d})$ mod p
10: $E \leftarrow$ elliptic curve over $\mathbb{F}_p$ with $j(E) = j$ and $|E(\mathbb{F}_p)| = N$
11: **return** E

Proof of Theorem 1.2. We will show that Algorithm 2 satisfies the claims in Theorem 1.2.

By the Bateman–Horn conjecture and Lemma 5.3, for any fixed d, t as chosen in the algorithm, the number of possible values of $c \le \sqrt{M}$ such that $p, c, N/\mathrm{cof}(dc^2)$ are simultaneously prime, is $\Omega(\sqrt{M}/\log^3 M)$. Because there is a finite number of possibilities for t, d, which are independent of M, this implies that the expected number of iterations of the main loop of Algorithm 2 is $O(\log^3 M)$.

The probability that the embedding degree of the returned curve is less than $\log^2 p$ follows from Theorem 5.7 using $K = \log^2 M$. Note that here we are using that t, d are bounded independently of M, in order to average the result of Theorem 5.7 for all values of t in the interval $[3, 100]$.

The resulting curve E has N points, where $N = r \cdot \mathrm{cof}(dc^2)$ and r is prime. Recall that $\mathrm{cof}(dc^2) \mid 24$ by definition (see equation (4.1)). Also, E is isolated with gap c and set-size 8 because c is prime, and the bound $d \le 100$ implies that the class number of $\mathbb{Q}(\sqrt{-d})$ is at most 8. The lower bound $c \ge \sqrt{p/50 - 100}$ follows from a straightforward computation. □

Remark 5.8. The bound on t in Algorithm 2 is mostly arbitrary. It is important that the upper bound on $|t|$ is independent of M. The lower bound $t \ge 3$ is for the same reason as the restriction on t in Algorithm 1.

6 Extending the results

The goal of this section is to discuss the following issues with Theorem 1.2:

- The algorithm used in the proof (Algorithm 2) places a restriction on t, limiting the amount of randomness in the selection of an isolated curve.
- It does not give a computable bound lower bound for what "sufficiently large" is.

Recall that the main idea of both Algorithm 1 and Algorithm 2 is to search for integers t, c such that three functions $(p(t, c), r(t, c)$ and $c)$ are simultaneously prime. Algorithm 2 imposes a restriction on t that allowed us to reduce to the one variable case and apply the Bateman–Horn conjecture. We expect that the restriction on t is unnecessary, and that the following properties hold:

(i) The expected number integers t, c sampled in Algorithm 1 is $O(\log^3 M)$.
(ii) The probability that a curve returned by Algorithm 1 has an embedding degree $< \log^2 M$ is $O(\frac{\log^8 M}{\sqrt{M}})$.
(iii) The implied constants in these estimates are computable.

In the notation of Section 5, all three properties reduce to giving computable bounds for S_M and $S_{M,K}$. Recall that the expected number of iterations of the main loop of Algorithm 1 is roughly $\frac{|S_M|}{M}$ and the probability of an embedding degree less than K is about $\frac{|S_{M,K}|}{|S_M|}$. For Theorem 1.2, we fixed t and gave bounds for $S_{M,K}(t)$ and $S_M(t)$ in Proposition 5.2 and Proposition 5.6, respectively. We would like to extend those bounds to $S_{M,K}$ and S_M.

Proposition 6.1. *There is a computable constant $\mathcal{A}_4$ such that for any positive integers M and K,*

$$|S_{M,K}| \le \mathcal{A}_4 K^2 \sqrt{M} \log M.$$

Proof. By definition, $|S_{M,K}| \le \sum_{t=1}^{\sqrt{M}} |S_{M,K}(t)|$. Then by Proposition 5.2,

$$|S_{M,K}| \le \sum_{t=1}^{\sqrt{M}} \mathcal{A}_1 K^2 \log t \le \mathcal{A}_1 K^2 \sqrt{M} \log \sqrt{M},$$

where $\mathcal{A}_1$ is the constant from Proposition 5.2. Hence we may take $\mathcal{A}_4 = \frac{\mathcal{A}_1}{2}$. □

Problem 6.2. Find a computable number $\mathcal{A}_5$, depending only on the fundamental discriminant d, such that for any positive integer M,

$$|S_M| > \mathcal{A}_5 \frac{M}{\log^3 M}.$$

Remark 6.3. A solution to Problem 6.2 would be useless in practice if $\mathcal{A}_5$ is too small (e.g. 2^{-100}). Hence we implicitly require that $\mathcal{A}_5$ lies within a reasonable range, such as $\mathcal{A}_5 > 2^{-20}$.

6.1 An alternative conjecture

Even under the Bateman–Horn conjecture we are unable to solve Problem 6.2. This is because the Bateman–Horn conjecture only gives an asymptotic formula; it does not provide information about the error term.[8] However, there is another natural conjecture one may consider related to the Bateman–Horn conjecture.

Conjecture 6.4. Let $f_1, \dots, f_k \in \mathbb{Z}[x, y]$ be such that every f_i is irreducible and $\gcd_{a,b\in\mathbb{Z}} \prod f_i(a, b) = 1$. Let $P_{f_1,\dots,f_k}(N)$ denote the number of pairs a, b such that $0 \le a, b \le N$ and $f_1(a, b), \dots, f_k(a, b)$ are simultaneously prime. Then for any $N_0 > 0$, there exists a computable constant C (depending on N_0 and the f_i) such that

$$P_{f_1,\dots,f_k}(N) > C\frac{N^2}{\log^k N} \quad \text{for all } N > N_0.$$

Remark 6.5. As stated, the constant C in Conjecture 6.4 depends on N_0. We could have equivalently stated the conjecture with C independent of N_0. However, in practice we usually avoid small values of N.

Recall that before the prime number theorem was proven, Chebyshev showed that $\pi(N) \ge \frac{\log 2}{2}\frac{N}{\log N}$ for all $N \ge 2$, cf. [33, Theorem 5.3]. In a way, Conjecture 6.4 is to the Bateman–Horn conjecture as Chebyshev's inequality is to the prime number theorem. Conjecture 6.4 is weaker than the Bateman–Horn conjecture in the sense that it only asks for a lower bound, not an asymptotic formula. In fact, Conjecture 6.4 would follow from the Bateman–Horn conjecture if it had included a clause about the error term.

6.2 Heuristic evidence

The same heuristics used to justify the Bateman–Horn conjecture suggest that $P_{f_1,\dots,f_k}$ in Conjecture 6.4 has the right order of magnitude. Let $f(x, y) \in \mathbb{Z}[x, y]$ such that $\gcd_{x,y\in\mathbb{Z}} f(x, y) = 1$. If we pretend that $f(x, y)$ acts like a random number, then the probability that $f(x, y)$ is prime should be roughly $\frac{1}{\log|f(x,y)|}$. If x, y are chosen independently from a uniform distribution on $[0, N]$, then the probability that $f(x, y)$ is prime should be roughly $\frac{1}{d\log N}$, where d is the degree of f (i.e. the highest total degree of any monomial in f). Given multiple polynomials $f_1, \dots, f_k$ satisfying the hypothesis in Conjecture 6.4, we expect that the probability that they are simultaneously prime is the product of the probabilities for each f_i, up to some constant correction factor. This suggests that $P_{f_1,\dots,f_k} = \Theta(\frac{N^2}{\log^k N})$, but gives no insight into the constants.

6.3 Theoretical evidence

Conjecture 6.4 also differs from the Bateman–Horn conjecture in that it applies to polynomials in two variables. There are many cases where the conjecture can be proven. For example, we can apply the prime number theorem for quadratic fields to estimate how often certain quadratic forms are prime [15, Theorem 21.1]. The Friedlander–Iwaniec theorem [14] gives an asymptotic density of primes of the form $x^2 + y^4$. More recently considered were pairs x, y such that $x^2 - xy + y^2$ and $2x - y$ are both prime [29]. One of the examples closest to Problem 6.2 is the following result of Fouvry and Iwaniec.

Theorem 6.6 (Fouvry and Iwaniec [15, Theorem 20.3], [11]). *Let Λ be the von Mangoldt function defined by*

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k \text{ for some prime } p, \\ 0 & \text{otherwise.} \end{cases}$$

Then

$$\sum_{x^2+y^2\le N} \Lambda(x)\Lambda(x^2 + y^2) = \frac{\pi H}{4}N + O\Big(\frac{N}{\log^{1/4} N}\Big),$$

8 We do know that any error bound would necessarily depend on the polynomials by [13, Theorem 1].

where the sum is over positive integer, $H = \prod_p (1 - \frac{\chi(p)}{p-1})$*, and*

$$\chi(p) = \begin{cases} 1, & p \equiv 1 \bmod 4, \\ -1, & p \equiv 3 \bmod 3, \\ 0, & p = 2. \end{cases}$$

Corollary 6.7. *Let* $P_{x,x^2+y^2}(N)$ *denote the number of pairs* $x, y \in [0, N]$ *such that* x *and* $x^2 + y^2$ *are simultaneously prime. Then*

$$P_{x,x^2+y^2}(N) = \Omega\Big(\frac{N^2}{\log^2 N}\Big).$$

Proof. First notice that

$$\begin{aligned} P_{x,x^2+y^2}(N) &= \sum_{\substack{x,x^2+y^2 \text{prime} \\ 0<x,y<N}} 1 \\ &\geq \sum_{\substack{x,x^2+y^2 \text{prime} \\ 0<x^2+y^2<N^2}} 1 \\ &\geq \frac{1}{2\log^2 N} \sum_{\substack{x,x^2+y^2 \text{prime} \\ 0<x^2+y^2<N^2}} \Lambda(x)\Lambda(x^2+y^2). \end{aligned}$$

The only difference between the last sum and the sum in Theorem 6.6, is that the latter includes prime powers. The number of prime powers less than N^2 is bounded above by $\log(N)\pi(N) < 2N$. For each prime power p^k less than N, there are at most $4(k+1)$ pairs x, y such that $x^2 + y^2 = p^k$. This is because there are at most $k+1$ ideals in $\mathbb{Z}[i]$ with norm p^k, and each has at most four distinct generators. Therefore

$$P_{x,x^2+y^2}(N) \geq \frac{1}{2\log^2 N} \sum_{x^2+y^2 \leq N^2} \Lambda(x)\Lambda(x^2+y^2) - \frac{4N}{\log N}.$$

The claim now follows from Theorem 6.6. □

If we restrict to even values of t, then for $d = 4$ we have that $p(t, c) = (\frac{t}{2})^2 + c^2$. Hence the corollary above implies that for $d = 4$ we have

$$\#\Big\{t, c : p = \frac{t^2 + dc^2}{4} \text{ and } c \text{ are prime and } p \leq M\Big\} = \Omega\Big(\frac{M}{\log^2 M}\Big).$$

This agrees with our heuristics because we have two polynomials and the probability both are prime is roughly $1/\log^2 M$ when choosing t, c randomly in $[0, \sqrt{M}]$. We expect the same principal term for other values of d. Furthermore, adding the requirement that $r(t, c)$ is prime should change the principle term by a factor of $1/\log M$. It is unclear if the methods used in the proof of Theorem 6.6 could extend to cover pairs t, c such that all three functions p, r, and c are all simultaneously prime.

6.4 Numerical evidence

We implemented Algorithm 1 with $d = 4$ using a few modifications for efficiency, such as only choosing odd values of c and even values of t. For a few values of M, we counted the number of iterations the main loop ran until the algorithm returned. Equivalently, this is the number of pairs t, c chosen at random until p, r, and c were simultaneously prime. The number of iterations was always below $\log^3 M$ as shown in Figure 1.

We also computed the embedding degree of a curve returned by Algorithm 1 with $M = 2^{98}$. In 10,000 runs we observed 0 curves with embedding degree $< \log^2(M)$. This should be compared with the bound

$$\frac{\log^8(M)}{\sqrt{M}} \approx 0.80527.$$

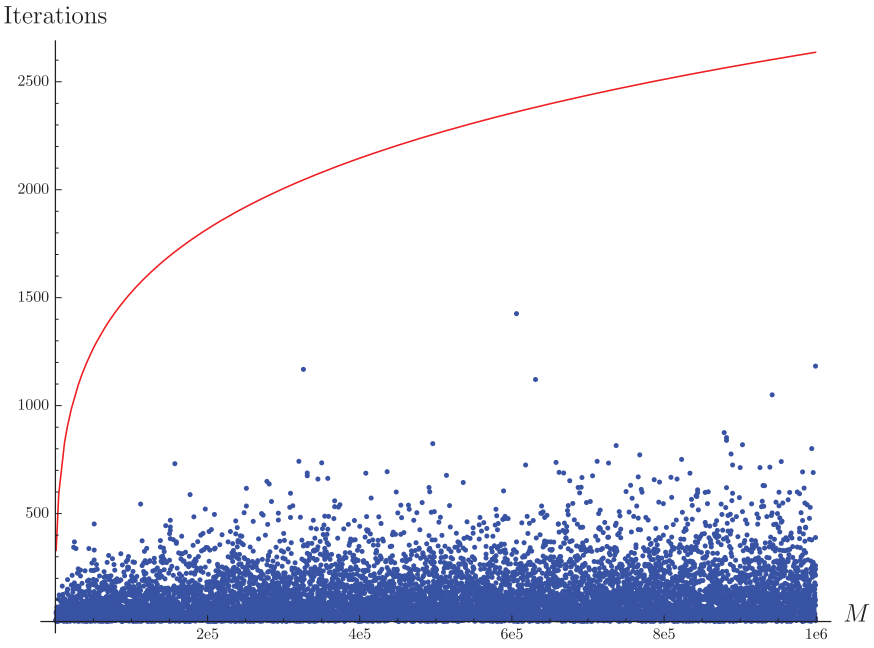

Figure 1. Comparing the observed number of samples of t, c used in Algorithm 1 with $\log^3 M$ for various values of M.

7 Conclusion

We acknowledge that a solution to Problem 6.2 may not be as mathematically interesting as proving an asymptotic formula with an optimal error bound for a generalized, two variable Bateman–Horn conjecture. However, a solution to Problem 6.2 would be enough to:

(i) Prove the efficiency of an algorithm to generate an isolated curve with large embedding degree.

(ii) Prove that the space of isolated curves is large enough to provide sufficient randomness in parameter selection.

These facts are enough to show that isolated curves provide cryptosystems resistant to the isogeny based attacks described in the introduction.

Acknowledgment: I would like to thank my advisor Neal Koblitz for all of his support and guidance while working on this paper. I would also like to thank Bianca Viray for her patience in reading many first drafts, as well as David Jao for helpful conversations about computing isogenies between elliptic curves at a conference. Finally, I am grateful to my fellow graduate students for listening to me talk about elliptic curves in every seminar.

References

[1] R. Balasubramanian and N. Koblitz, The improbability that an elliptic curve has subexponential discrete log problem under the Menezes–Okamoto–Vanstone algorithm, *J. Cryptology* **11** (1998), no. 2, 141–145.

[2] P. T. Bateman and R. A. Horn, A heuristic asymptotic formula concerning the distribution of prime numbers, *Math. Comp.* **16** (1962), 363–367.

[3] R. Bröker, D. Charles and K. Lauter, Evaluating large degree isogenies and applications to pairing based cryptography, in: *Pairing-Based Cryptography – Pairing 2008*, Lecture Notes in Comput. Sci. 5209, Springer, Berlin (2008), 100–112.

[4] R. Bröker, K. Lauter and A. V. Sutherland, Modular polynomials via isogeny volcanoes, *Math. Comp.* **81** (2012), no. 278, 1201–1231.

[5] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Math. Surveys Monogr. 48, American Mathematical Society, Providence, 1997.

[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.
[7] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Discrete Math. Appl. (Boca Raton), Chapman & Hall/CRC, Boca Raton, 2006.
[8] A. C. Cojocaru and I. E. Shparlinski, On the embedding degree of reductions of an elliptic curve, *Inform. Process. Lett.* **109** (2009), no. 13, 652–654.
[9] D. A. Cox, *Primes of the Form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication*, 2nd ed., Pure Appl. Math. (Hoboken), John Wiley & Sons, Hoboken, 2013.
[10] A. Entin, On the Bateman–Horn conjecture for polynomials over large finite fields, preprint (2014), http://arxiv.org/abs/1409.0846.
[11] E. Fouvry and H. Iwaniec, Gaussian primes, *Acta Arith.* **79** (1997), no. 3, 249–287.
[12] G. Frey, M. Müller and H.-G. Rück, The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems, *IEEE Trans. Inform. Theory* **45** (1999), no. 5, 1717–1719.
[13] J. Friedlander and A. Granville, Limitations to the equi-distribution of primes. IV, *Proc. Roy. Soc. London Ser. A* **435** (1991), no. 1893, 197–204.
[14] J. Friedlander and H. Iwaniec, Using a parity-sensitive sieve to count prime values of a polynomial, *Proc. Natl. Acad. Sci. USA* **94** (1997), no. 4, 1054–1058.
[15] J. Friedlander and H. Iwaniec, *Opera de Cribro*, Amer. Math. Soc. Colloq. Publ. 57, American Mathematical Society, Providence, 2010.
[16] D. Jao, S. D. Miller and R. Venkatesan, Do all elliptic curves of the same order have the same difficulty of discrete log?, in: *Advances in Cryptology – ASIACRYPT 2005*, Lecture Notes in Comput. Sci. 3788, Springer, Berlin (2005), 21–40.
[17] D. Jao, S. D. Miller and R. Venkatesan, Expander graphs based on GRH with an application to elliptic curve cryptography, *J. Number Theory* **129** (2009), no. 6, 1491–1504.
[18] D. Jao and V. Soukharev, A subexponential algorithm for evaluating large degree isogenies, in: *Algorithmic Number Theory*, Lecture Notes in Comput. Sci. 6197, Springer, Berlin (2010), 219–233.
[19] J. Katz and Y. Lindell, *Introduction to Modern Cryptography*, 2nd ed., Chapman & Hall/CRC Cryptogr. Netw. Secur., CRC Press, Boca Raton, 2015.
[20] A. H. Koblitz, N. Koblitz and A. Menezes, Elliptic curve cryptography: The serpentine course of a paradigm shift, *J. Number Theory* **131** (2011), no. 5, 781–814.
[21] N. Koblitz and A. Menezes, The brave new world of bodacious assumptions in cryptography, *Notices Amer. Math. Soc.* **57** (2010), no. 3, 357–365.
[22] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, Ph.D. thesis, University of California at Berkeley, 1996, http://echidna.maths.usyd.edu.au/~kohel/pub/thesis.pdf.
[23] J. C. Lagarias and A. M. Odlyzko, Effective versions of the Chebotarev density theorem, in: *Algebraic Number Fields*, Academic Press, London (1977), 409–464.
[24] F. Luca, D. J. Mireles and I. E. Shparlinski, MOV attack in various subgroups on elliptic curves, *Illinois J. Math.* **48** (2004), no. 3, 1041–1052.
[25] A. J. Menezes, T. Okamoto and S. A. Vanstone, Reducing elliptic curve logarithms to logarithms in a finite field, *IEEE Trans. Inform. Theory* **39** (1993), no. 5, 1639–1646.
[26] A. Menezes and E. Teske, Cryptographic implications of Hess' generalized GHS attack, *Appl. Algebra Engrg. Comm. Comput.* **16** (2006), no. 6, 439–460.
[27] A. Menezes, E. Teske and A. Weng, Weak fields for ECC, in: *Topics in Cryptology – CT-RSA 2004*, Lecture Notes in Comput. Sci. 2964, Springer, Berlin (2004), 366–386.
[28] S. D. Miller and R. Venkatesan, Spectral analysis of Pollard rho collisions, in: *Algorithmic number theory*, Lecture Notes in Comput. Sci. 4076, Springer, Berlin (2006), 573–581.
[29] M. Pandey, On Eisenstein primes, preprint (2016), https://arxiv.org/abs/1607.00469v1.
[30] K. Rubin and A. Silverberg, Choosing the correct elliptic curve in the CM method, *Math. Comp.* **79** (2010), no. 269, 545–561.
[31] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208; erratum, *Acta Arith.* **5** (1958), 259.
[32] R. Schoof, Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46** (1987), no. 2, 183–211.
[33] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, 2nd ed., Cambridge University Press, Cambridge, 2009.
[34] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Grad. Texts in Math. 106, Springer, New York, 2009.
[35] N. P. Smart, The discrete logarithm problem on elliptic curves of trace one, *J. Cryptology* **12** (1999), no. 3, 193–196.
[36] A. V. Sutherland, Isogeny volcanoes, in: *ANTS X – Proceedings of the Tenth Algorithmic Number Theory Symposium*, Open Book Ser. 1, Mathematical Sciences Publishers, Berkeley (2013), 507–530.
[37] W. Wang, *Isolated curves for hyperelliptic curve cryptography*, Ph.D. thesis, University of Washington, 2012, http://search.proquest.com/docview/1197791596.
[38] The Sage Developers, *SageMath, the Sage Mathematics Software System (Version 6.10)*, 2016, http://www.sagemath.org/.