Characterization of Smart-proof curves

August 27, 2020

Abstract

The points of an elliptic curve over a finite field forms an finite abelian group, hence frequently used in cryptography due to the conjectured difficulty of solving the discrete logarithm problem. However certain classes of curves have computationally simple solutions to the discrete logarithm, for instance curves of trace 1, known as anomalous curves. This attack was first published by Smart, hence its nickname, the 'Smart Attack'. This attack lifts curves from $\mathbb{F}_p$ to $\mathbb{Q}_p$. However, it has a small chance of lifting to a curve where the attack fails. This paper's main objective is to classify such lifts.

1 Introduction

Suppose $kP = Q$ with P, Q known and k unknown. This is the discrete logarithm problem(DLP) for elliptic curves and is generally difficult. However if the trace of the curve is 1, then this can be translated to the DLP over $\mathbb{F}_p^+$, which is simply solving $\frac{a}{b} \pmod p$. Such curves are known as anomalous curve. From now all curves are assumed to be anomalous.

For a curve $E(\mathbb{F}_p)$, to translate the DLP to $\mathbb{F}_p^+$, first lift it to $E(\mathbb{Q}_p)$ and define the subgroups of the group $E(\mathbb{Q}_p)$:

$$E_r = \{(x, y) \in E/\mathbb{Q}_p | v_p(x) \leq -2r, v_p(y) \leq -3r\} \cup \{\infty\}$$

Note that $\frac{E(\mathbb{Q}_p)}{E_1} \cong E(\mathbb{F}_p)$ and $\frac{E_1}{E_2} \cong \mathbb{F}_p^+$, which the first isomorphism given by reduction mod p last isomorphism given by $\psi : (x, y) \to -\frac{x}{py}$.

Assume that $kP = Q$ in $E(\mathbb{F}_p)$. Lift P, Q to $E(\mathbb{Q}_p)$ and we have $pP, pQ, kP - Q \in E_1$ since curve is of order p. Furthermore, $k\psi(pP) - \psi(pQ) = p\psi(kP - Q) = 0$, so $k = \frac{\psi(pQ)}{\psi(pP)}$, which is a DLP over $\mathbb{F}_p^+$ and is computationally extremely easy. Note that if $pP \in E_2$, then we get $0 \cdot k + 0 = 0$, so the proof does not work for this case. For such a lift, the lifted curve is called *Smart-proof*

Main Objectives The main objectives of this paper is to find all Smart-proof lifts for a given anomalous curve.

2 Classification

2.1 Alternate characterization

Consider a exact sequence of modules $0 \to N \to E \to M \to 0$. Extensions E, E' are isomorphic iff

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & E & \longrightarrow & M & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle u} & & \| & & \\ 0 & \longrightarrow & N & \longrightarrow & E' & \longrightarrow & M & \longrightarrow & 0 \end{array}$$

Using the five lemma, E and E' are isomorphic as modules.

Lemma 1. *The structure of* $E(\mathbb{Q}_p)$ *is* $\frac{\mathbb{Z}_p \oplus \mathbb{Z}}{(k,p)\mathbb{Z}}$ *for* $0 \leq k < p$.

Proof. We have the exact sequence $0 \to E_1 \to E(\mathbb{Q}_p) \to E(\mathbb{F}_p) \to 0$ with $E_1 \cong p\mathbb{Z}_p$ and $E(\mathbb{F}_p) \cong \mathbb{F}_p$.

We can find all possible structures of $E(\mathbb{Q}_p)$ by first considering the following commutative diagram of exact sequences:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & p\mathbb{Z} & \longrightarrow & \mathbb{Z} & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle u} & & \Vert & & \\ 0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & G & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \end{array}$$

and we apply the $\mathrm{Hom}(-, \mathbb{Z}_p)$ functor to the top exact sequence to obtain the exact sequence $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_p) \to \mathrm{Hom}(p\mathbb{Z}, \mathbb{Z}_p) \to \mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p) \to 0$. We have $\mathrm{Ext}^1(\mathbb{F}_p, p\mathbb{Z}_p \cong \mathbb{Z}_p) = \mathbb{F}_p$, and for any element in it we can find an element in $\mathrm{Hom}(p\mathbb{Z}, \mathbb{Z}_p)$ and construct G as the pushout of $\mathbb{Z}_p \to p\mathbb{Z} \to \mathbb{Z}$, giving us the extensions $\frac{\mathbb{Z}_p \oplus \mathbb{Z}}{(k,p)\mathbb{Z}}$ with $k \in \mathbb{F}_p$ as the structure of $E(\mathbb{Q}_p)$.

One can verify quickly by chasing that extensions that are isomorphic gives rise to the same element in $\mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p)$ and that adding any element of $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_p)$ to an element of $\mathrm{Hom}(p\mathbb{Z}, \mathbb{Z}_p)$ gives rise to isomorphic extensions.

For $k = 0$, this gives $\mathbb{Z}_p \oplus \mathbb{F}_p$ and for $k = 1$ this gives $\mathbb{Z}_p$. For other k a mental model for this would be $\mathbb{Z}_p$ but with the carry for the p^0 term being $p \cdot p^{0\text{`}} =' k \cdot p^1$, somewhat like a messed up construction of the Witt vector. □

If the exact sequence splits, then $pE(\mathbb{Q}_p) = p(E_1 \oplus \mathbb{F}_p) = pE_1 = E_2$ and the curve has p-torsion points and is Smart-proof. Otherwise $pE(\mathbb{Q}_p) = E_1$ as there is a carry and the curve is not Smart-proof. This shows that the Smart-proof condition and the condition that the lift to $\mathbb{Q}_p$ has p-torsion are the same.

2.2 Canonical lift

Lemma 2. *If the Frobenius isogeny lifts, then the lifted curve has p-torsion points*

Proof. Consider the dual to the Frobenius isogeny, the composition of these two isogenies is a multiplication by p isogeny and the dual is separable. Since the Frobenius isogeny stabalizes $E(\mathbb{F}_p)$, the dual annihilates it and these points can be lifted to a p-torsion group for $E(\mathbb{Q}_p)$. □

For a elliptic curve E over $\mathbb{F}_p$, there exists a unique curve $\tilde{E}$ over $\mathbb{Q}_p$ such that the Frobenius isogeny lifts as well. This curve is the canonical lift and by the above lemma, it has p-torsion points.

2.3 Other lifts

$E(\mathbb{Q}_p)/E_2$ is a group of order p^2, hence it is either $\mathbb{Z}/p^2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^2$. As $E(\mathbb{Q}_p)$ is either $\frac{\mathbb{Z}_p \oplus \mathbb{F}_p}{(k,p)\mathbb{Z}}$, $k \nmid p$ or $E_1 \oplus \mathbb{F}_p$, the structure of $E(\mathbb{Q}_p)/E_2$ determines if p-torsion points exists. More specifically if the group is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$, then no p-torsion points exists, otherwise it is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^2$ and p-torsion points exist.

Consider the morphism $\phi : (x : y : z) \to (x : z : y)$. This morphism maps points in E_n to points in $(p^n\mathbb{Z}_p)^2$, allowing us to easily take quotients by E_n. More specifically, $\phi(E)\left(\mathbb{Z}/p^2\mathbb{Z}\right) \cong E(\mathbb{Q}_p)/E_2$, hence we only need to look at points on $\phi(E) \mod p^2$. This motivates the following theorem regarding lifts with p-torsion points

Theorem 1. *For a curve* $E(\mathbb{F}_p)$*, let* $E(\mathbb{Q}_p)$ *be a lift and* $\tilde{E}(\mathbb{Q}_p)$ *be the canonical lift. If* $j(E) \equiv j\left(\tilde{E}\right) \pmod{p^2}$*, then* $E(\mathbb{Q}_p)$ *has p-torsion points.*

Proof. Let $\tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b}$ be the canonical lift and $E : y^2 = x^3 + ax + b$ be a lift such that their j-invariant are equal under $\mod p^2$, then $\tilde{a}^3b^2 \equiv a^3\tilde{b}^2 \pmod{p^2}$. Let $u = \left(\frac{\tilde{a}}{a}\right)^{\frac{1}{4}} = \left(\frac{\tilde{b}}{b}\right)^{\frac{1}{6}} \pmod{p^2}$, if either

a or b is 0 $(\text{mod } p^2)$, then let u be the non-degenerate equality. As $\tilde{a} \equiv a \pmod{p}, \tilde{b} \equiv b \pmod{b}$, the fractions are of the form $1 + kp$ and we can choose the nth roots to be 1 $(\text{mod } p)$, giving us the nth roots $1 + \frac{k}{n}p$.

Consider the morphism $(x : y : z) \to (u^2x : u^3y : z)$ mapping E to $E' : y^2 = x^3 + u^4ax + u^6b$. By definition of u, the coefficients of this curve is the same as $\tilde{E}$ under $\text{mod } p^2$ and under ϕ, both curves are identical and have identical group structure, hence $E(\mathbb{Q}_p)$ has p-torsion points. □

We have the following corollary giving us a simple description of all such curves:

Corollary 1. *If* $3b(a - \tilde{a}) \equiv 2a\left(b - \tilde{b}\right) \pmod{p^2}$, *then* $E(\mathbb{Q}_p)$ *has* p*-torsion points.*

Proof. Since they are lifts of the same curve, we let $a = \tilde{a} + mp, b = \tilde{b} + np$. Then the equality reduces to $3bm \equiv 2an \mod p$. Since $\tilde{a}^3b^2 \equiv (a - mp)^3 b^2 \equiv a^3b^2 - 3a^2b^2mp \pmod{p^2}$ and $a^3\tilde{b}^2 \equiv a^3(b - np)^2 \equiv a^3b^2 - 2a^3bnp \pmod{p^2}$ and the assumption gives $3a^2b^2mp \equiv 2a^3bnp \pmod{p^2}$, $\tilde{a}^3b^2 \equiv a^3\tilde{b}^2 \pmod{p^2}$ and the j invariants are the same, hence by the theorem above, $E(\mathbb{Q}_p)$ have p-torsion points. □

With this corollary, we see that $\frac{1}{p}$ of the lifts, when taken mod p^n for any n, has p-torsion.

2.4 Torsion-free lifts

To fully classify all lifts, we need to show that all other lifts must be torsion-free. Unfortunately this is not as simple and we will use results from Serre-Tate theorem, which states that deformations to an abelian variety is the same as deformations to its p-divisible group. This theorem gives us coordinates in the moduli space of lifts that helps us show that $\frac{1}{p}$ of lifts have p-torsion points.

//probably try to see if there is a easier way to do for elliptic curves

3 Future work

We have only used a small portion of Serre-Tate theory when showing that only $\frac{1}{p}$ lifts have p-torsion, hence are Smart-proof. The case of elliptic curves may have a simpler explanation as we have the exact sequence $0 \to \hat{\mathbb{E}}(m) \to \mathbb{E}(K) \to E(k) \to 0$ where K is a local field and $\mathbb{E}/K$ is a lift of E/k. By taking the p-torsion subgroup, this sequence is a connected étale sequence and splits. Furthermore $E \cong E^t$ along with all the Tate modules and these all have an action over $\text{Gal}\left(\frac{\bar{\mathbb{Q}}_p}{\mathbb{Q}_p}\right)$.

We have verified that for $0 \leq a, b < p^2$, there are only $\frac{1}{p}$ Smart-proof lifts and they satisfy the $3bm = 2an$ equality.

We have also checked that Smart attack indeed fails for these curves and they fail at roughly a rate of $\frac{p-2}{p-3}$, which is predicted if there is the map from points on the curve to E_2 is purely set-theoretic. Interestingly some points are also mapped to E_3.

We can evidently write n as a function of m, $n(m) = n(0) + kp$, interestingly for some primes, for instance $p = 19, 23, 29, 31, 47$, k takes on every single value once from 1 to $p - 1$ while for others like $p = 43, 53, 61, 71, 73, 79, 83, 89, 97$(we only checked $p < 100$, k takes on every value from 1 to $p - 1$ but potentially multiple times. It may be interesting to explore why this happens at such small primes as one may expect k to take on random values, so we should almost never see the case where it takes every single value in $\mathbb{Z}_p^\times$ once.

4 Appendix

The full diagram chase of Lemma 1 is given here for verification purposes.

Let G be a extension of $\mathbb{F}_p$ by $\mathbb{Z}_p$, so $0 \to \mathbb{Z}_p \xrightarrow{f} G \xrightarrow{g} \mathbb{F}_p \to 0$ is exact.

Suppose G' is a equivalent extension, so there exists a map $G \to G'$ that makes the following diagram commute:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & G & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \\ \| & & \| & & \downarrow & & \| & & \| \\ 0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & G' & \longrightarrow & \mathbb{F}_p & \longrightarrow & 0 \end{array}$$

then by five lemma, $G \cong G'$.

Showing equivalent extensions give rise to the same element in $\mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p)$:

Given any extension, consider the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & p\mathbb{Z} & \xrightarrow{a} & \mathbb{Z} & \xrightarrow{b} & \mathbb{F}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle u} & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}_p & \xrightarrow{f} & G & \xrightarrow{g} & \mathbb{F}_p & \longrightarrow & 0 \end{array}$$

Define the map u to be any map that makes the right most square commute, it exists as $\mathbb{Z}$ is projective. This gives us a map v as for any element $x \in p\mathbb{Z}$, $bax = guax = 0$, so there exists a unique element in $\mathbb{Z}_p$ that x can be mapped to to maintain commutativity.

Apply $\mathrm{Hom}(-, \mathbb{Z}_p)$ to the top exact sequence to obtain $0 \to \mathrm{Hom}(\mathbb{F}_p, \mathbb{Z}_p) \xrightarrow{b^*} \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}_p) \xrightarrow{a^*} \mathrm{Hom}(p\mathbb{Z}, \mathbb{Z}_p) \to \mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p) \to 0$.

Suppose we have another map u' that makes the right most square commute. $g(u - u') = 0$, so $\mathrm{Im}(u - u') \subseteq \mathrm{Im}\, f$ and there exists a morphism $c : \mathbb{Z} \to \mathbb{Z}_p$ such that $fc = u - u'$. Since $u'a = (u - fc)a = f(v - ca)$, our v' that makes the diagram with u' commute is $v - ca$. Hence the map u determines a unique element in $\mathrm{coker}\, a^* = \mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p)$.

Finally if G, G' are equivalent extensions, then we have $p\mathbb{Z} \xrightarrow{v} \mathbb{Z}_p = \mathbb{Z}_p$ where the first $\mathbb{Z}_p$ belongs to the extension G and the second belongs to the extension G'. This results in the same element in $\mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p)$.

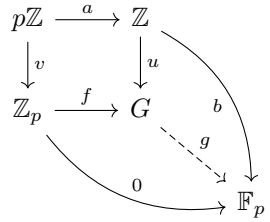
Showing an element of $\mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p)$ give rise to a single extension up to equivalence:

Given $k \in \mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p) \in \mathbb{F}_p$, we choose a $v \in \mathrm{Hom}(p\mathbb{Z}, \mathbb{Z}_p)$ as $v : p \to k$. Then our commutative diagram becomes

$$\begin{array}{ccccccccc} 0 & \longrightarrow & p\mathbb{Z} & \xrightarrow{a} & \mathbb{Z} & \xrightarrow{b} & \mathbb{F}_p & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle u} & & \| & & \\ 0 & \longrightarrow & \mathbb{Z}_p & \dashrightarrow^{f} & G & \dashrightarrow^{g} & \mathbb{F}_p & \longrightarrow & 0 \end{array}$$

where dotted arrows are maps yet to be constructed.

Construct G, f, u as the pushout of $\mathbb{Z}_p \xleftarrow{v} p\mathbb{Z} \xrightarrow{a} \mathbb{Z}$. Explicitly this is $\frac{\mathbb{Z}_p \oplus \mathbb{Z}}{(k,-p)\mathbb{Z}}$, $f : x \to (x, 0)$ and $u : y \to (0, y)$. Since this is a pushout, g exists and is unique via the following diagram:



This can be made explicit by sending (x, y) to y. This coordinate map for $\mathbb{Z}_p \oplus \mathbb{Z} \to \mathbb{F}_p$ sends (x, y) to y mod p and has $(k, -p)\mathbb{Z}$ in the kernel, hence the map sending $(x, y) \in G$ to y is well defined.

The composite gu sends y to $y \mod p$, which is what b does so the triangle commutes. The composite fg sends x to 0, so the entire diagram commutes and the constructed map g is the unique map that comes from the pushout.

Finally we need to show that $G \xrightarrow{g} \mathbb{F}_p \to 0$ is exact. Evidently $(0, k) \in G$ for all $k \in \mathbb{F}_p$, so this map is surjective and the entire diagram commutes and is exact.

We are only left with showing that if extensions E, E' are constructed by the same element in $\mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p)$, then they are equivalent. For the maps in the commutative diagram for E', we include a $'$ to differentiate it from the commutative diagram for E.

For any element v' that has the same image in $\mathrm{Ext}^1(\mathbb{F}_p, \mathbb{Z}_p)$ as v, we have $v - v' \in \mathrm{Im}\, a^*$, so there exists some $c : \mathbb{Z} \to \mathbb{Z}_p$ such that $v - v' = ac$ and we can define u' as $u - fc$. Hence we can assume that $v' = v$. This gives us the following commutative diagram

$$\begin{array}{ccccccccc}
0 & \longrightarrow & p\mathbb{Z} & \xrightarrow{a} & \mathbb{Z} & \xrightarrow{b} & \mathbb{F}_p & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle u} & & \| & & \\
0 & \longrightarrow & \mathbb{Z}_p & \xrightarrow{f} & G & \xrightarrow{g} & \mathbb{F}_p & \longrightarrow & 0 \\
 & & \| & & & & \| & & \\
0 & \longrightarrow & \mathbb{Z}_p & \xrightarrow{f'} & G' & \xrightarrow{g'} & \mathbb{F}_p & \longrightarrow & 0
\end{array}$$

Since G, G' are pushouts, we have one unique morphism between them, hence they are isomorphic.

This gives us the extensions $\frac{\mathbb{Z}_p \oplus \mathbb{Z}}{(k,-p)\mathbb{Z}}$ for $k \in \mathbb{F}_p$.