Characterization of Smart-proof curves

August 17, 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 $\frac{E_0}{E_1} \cong E(\mathbb{F}_p)$ 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 are:

- Show lifts that are Smart-proof occur at a $\frac{1}{p}$ probability

- Show that when $a = kp$, the curve is Smart-proof iff $k = 0 \pmod{p}$
- Find all Smart-proof curves with $0 \leq a, b < p$
- Find all Smart-proof curves

2 Experimental results

For a curve $y^2 = x^3 + ax + b$ over $\mathbb{F}_p$, $0 \leq a, b < p$, suppose $y^2 = x^3 + (a + mp)x + (b + np)$ over $\mathbb{Q}_p$ is Smart-proof. It can be experimentally shown that:

- When $a = 0$, the curve is Smart-proof iff $m = 0$.
- When $a \neq 0$, every value of m has a unique value of n.
- $n(m) = n(0) + km$ for some k coprime to p(treating n as a function of m)
- For some values of p(i.e. $23, 29$), k takes on every value once.
- For Smart-proof curves, the attack acts like a random number generator except when $P = \pm Q$ where it gives accurate results.

3 Smart proof lifts

3.1 Alternate characterization

We have a morphism from E_1 to $p\mathbb{Z}_p$ given by $(x : y : z) \to \frac{x}{y}$. Unfortunately this map is may not be a morphism from E_0 to $\mathbb{Z}_p$ but instead to some other group. Taking $\mod p^2$, we have $E_1 \to \mathbb{Z}/p\mathbb{Z}$ and E_0 to an abelian group of order p^2, which is either $\mathbb{Z}/p^2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z})^2$. This shows that E_0 is either isomorphic to $\mathbb{Z}_p$ or $p\mathbb{Z}_p \oplus \mathbb{Z}/p\mathbb{Z}$. In the first case, $pE_0 = E_1$ and the curve is not Smart-proof while in the second case, $pE_0 = pE_1$ and the curve is Smart-proof.
The smart proof case implies the existence of a p-torsion group, so this problem is looking for lifts with a p-torsion group.

3.2 $a = 0$

Rough sketch for proof of $a = 0$:
Frobenius isogeny lifts from $\mathbb{F}_p$ to $\mathbb{Q}_p$
Dual isogeny of frob is separable and has kernel $E(\mathbb{F}_p)$, hence kernel can be lifted to give a p-torsion group.

3.3 General case

todo: by some serre tate thing lifts parametrized by $\mathbb{Z}_p$ and those in $p\mathbb{Z}_p$ are smart proof