Characterization of Smart-proof curves

June 3, 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 [1], 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 of points on $E/\mathbb{Q}_p$:

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

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 $E/\mathbb{F}_p$. Now working in $E/\mathbb{Q}_p$, we have $pP, pQ, kP - Q \in E_1$ since curve is of order p. $k\psi(pP) - \psi(pQ) = p\psi((kP - Q)) = 0$, 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 $k = \frac{0}{0}$, 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 $0 \leq a, b < p$
- Given a, b, p, determine the necessary and suffient conditions such that the elliptic curve is Smart proof.

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:

- For Smart-proof curves, the attack acts like a random number generator except when $P = \pm Q$ where it gives accurate results.
- 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.

3 Smart-proof lifts

Let $f \in \mathrm{End}\left(E/\overline{\mathbb{F}_p}\right)$ be the Frobenius endomorphism and let $\hat{f}$ be the dual isogeny. The kernel of the dual isogeny is $E/\mathbb{F}_p$, which has order p, hence it is separable. Suppose that $f, \hat{f}$ gets lifted to an endomorphism $\tilde{f}, \tilde{\hat{f}} \in \mathrm{End}\left(E/\mathbb{Q}_p\right)$. Since $\hat{f}$ is separable, $\ker \hat{f} \cong \ker \tilde{\hat{f}} \cong E/\mathbb{F}_p$, which is precisely $E_0[p]$. Then E_0 splits to $E_1 \times E_0[p]$, hence $pE_0 = pE_1$. Conversely, if the kernel is trivial then $pE_0 = E_1$.

These results show that if for any lifted point P, $pP \in E_2$, then this is true for all points, similarly if $pP \in E_1$, then this is true for all points. The former case only occurs iff the Frobenius endomorphism can be lifted to an endomorphism.

One way to look at the curve $y^2 = x^3 + ax + b$ over $\mathbb{Q}_p$ is transforming it to $\mathbb{Z}_p$ via $[x : y : z] \to [x : z : y]$ and we end up with $x^3 + axy^2 + by^3 - y = 0$. Reduce mod p^2 and we have a (abelian) group of points on a curve with p^2 elements, so the group is either $\left(\frac{\mathbb{Z}}{p\mathbb{Z}}\right)^2$ or $\frac{\mathbb{Z}}{p^2\mathbb{Z}}$. The former gives a Smart-proof lift while latter gives

a non-Smart-proof lift as the only p-torsion points are of the form $[kp : 0 : 1]$.

This transformation also shows that if a, b results in a Smart-proof curve, then after adding p^2 to either a, b, the curve remains Smart-proof. Hence to show that $\frac{1}{p}$ lifts are smart proof, we only need to show that out of the p^2 possible lifts mod p^2, p of them are Smart-proof.

The addition laws can be derived easily:

$$x^3 + axy^2 + by^3 - y = 0$$
$$\left(3x^2 + ay^2\right) dx + \left(2axy + 3by^2 - 1\right) dy = 0$$

$$\lambda = \begin{cases} \frac{P_y - Q_y}{P_x - Q_x} & P \neq Q \\ \frac{3P_x^2 + aP_y^2}{1 - 2aP_xP_y - 3bP_y^2} & P = Q \end{cases}$$

$$y = \lambda x + (P_y - \lambda P_x)$$

Given two points, P, Q, we can calculate the point $R = P + Q$, where we denote the components as:

$$P = (P_x, P_y), \qquad Q = (Q_x, Q_y), \qquad R = P + Q = (R_x, R_y).$$

$$x^3 + ax\left(\lambda x + (P_y - \lambda P_x)\right)^2 + b\left(\lambda x + (P_y - \lambda P_x)\right)^3 - \left(\lambda x + (P_y - \lambda P_x)\right) = 0$$
$$\left(1 + a\lambda^2 + b\lambda^3\right) x^3 + \lambda\left(2a + 3b\lambda\right)\left(P_y - \lambda P_x\right) x^2 + O(x) = 0$$
$$-R_x = \frac{\lambda\left(2a + 3b\lambda\right)\left(\lambda P_x - P_y\right)}{1 + a\lambda^2 + b\lambda^3} - P_x - Q_x$$
$$-R_y = \lambda R_x + (P_y - \lambda P_x)$$
$$R_x = \frac{\lambda\left(2a + 3b\lambda\right)\left(P_y - \lambda P_x\right)}{1 + a\lambda^2 + b\lambda^3} + P_x + Q_x$$
$$R_y = -\lambda R_x + (\lambda P_x - P_y)$$

Note if $P_x = Q_x$ and $P_y \neq Q_y$, then $R_x = -P_x$ and $R_y = \frac{aP_x}{b} + P_y + Q_y$

References

[1] N. P. Smart, *The discrete logarithm problem on elliptic curves of trace one*, *Journal of Cryptology* **12** (1999) 193.

[2] S. V. S. V. Franck Leprévost, Jean Monnerat, *Generating anomalous elliptic curves*, *Information Processing Letters* **93** (2005) 225.

A DEFCON Challenge

A.1 Challenge

During DEFCON 2020, we were asked to supply curve parameters (p, a, b) and two points $(P, Q = kP)$ to a server. The server generates an elliptic curve using sagemath: `E = EllipticCurve(GF(p), [a,b])` and then asserts that `E.order() == p` and that p has above a threshold number of bits. The challenge is solved if given (P, Q), the value returned by `launch_attack(P, Q, p)` is not equal to k.

We can understand this challenge as finding an anomalous elliptic curve which is not vulnerable to Smart's attack. The source code for `launch_attack(P, Q, p)` is included below.

```
def launch_attack(P, Q, p):
    E = P.curve()
    Eqp = EllipticCurve(Qp(p, 8), [ZZ(t) for t in E.a_invariants()])

    P_Qps = Eqp.lift_x(ZZ(P.xy()[0]), all=True)
    for P_Qp in P_Qps:
        if GF(p)(P_Qp.xy()[1]) == P.xy()[1]:
            break

    Q_Qps = Eqp.lift_x(ZZ(Q.xy()[0]), all=True)
    for Q_Qp in Q_Qps:
        if GF(p)(Q_Qp.xy()[1]) == Q.xy()[1]:
            break

    p_times_P = p * P_Qp
    p_times_Q = p * Q_Qp

    x_P, y_P = p_times_P.xy()
    x_Q, y_Q = p_times_Q.xy()

    phi_P = -(x_P / y_P)
    phi_Q = -(x_Q / y_Q)
    k = phi_Q / phi_P

    return ZZ(k) % p
```

A.2 Solution

During the competition, it was found by studying many curves with small integer parameters that the attack failed for curves with $a = 0$. We found a solution by producing an anomalous curve using the complex multiplication method of [2]. When $a = 0$, the j invariant of the curve is also zero. For $j = 0$, we pick a discriminant $D = 3$.

The primes which generate anomalous curves must be of the form:

$$p = 3m(m + 1) + 3$$

for an odd integer m. We can create a prime above the threshold by picking a large m and searching for a prime. We then select $a = 0$, and run through values of b, until the curve is anomalous.

Trivia The above primes are all in the form of $x^3 - y^3$, for $x = y + 1$ and are called *Cuban primes*, OEIS A002407.

Note When looking for small values to fool the attack, we found many curves with $j \neq 0$, but we could not find a pattern sufficient to easily generate these curves with a prime large enough to satisfy the threshold of the challenge. This is what motivated this research.