

Classification of Smart-proof curves

HATS lightning talk

August 29, 2020

Inspiration

DEFCON CTF Quals 2020 NotToBeFooled challenge writeup by author:

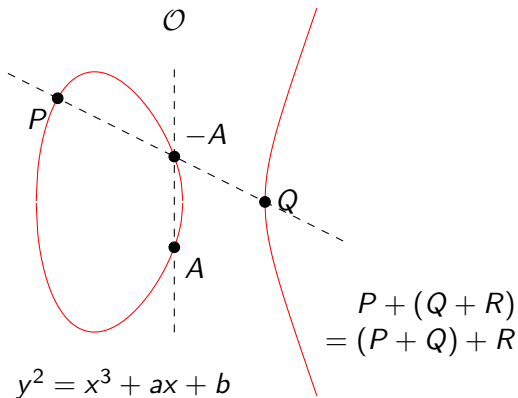
Inspired by <https://crypto.stackexchange.com/questions/70454/why-smarts-attack-doesnt-work-on-this-ecdlp?rq=1>, and the original Smart attack's paper, to make the generated curve immune to Smart attack, you can move the generated curve around while keeping the order unchanged. The easiest way is to use $D = 3$, under which $j = 0$, and you will notice that $a = 0$ and $b = 0$ according to equation (3) and (4) in the above paper. In this case, if we change the value of b , the order of the curve doesn't change, yet the lifted curve will be equivalent to change to $y^2 = x^3 + 0 \cdot x + (0 + p \cdot b)$.

So to solve this, all we need to do is to generate a random prime above the threshold, fix a to 0, and enumerate b .

Note that this is not the only solution. There are so many elliptic curves satisfying this property. If you have a way to compute the complete set, please let me know. :)

```
def find_safe_curve(p):
    for b in xrange(1, p):
        if b % 10 ** 4 == 0:
            print("Testing..., b = %d" % b)
        E = EllipticCurve(GF(p), [0, b])
        if E.order() == p:
            print("order is satisfied!")
            if test_safe(E, p, b):
                print("Find Safe Anomalous Curve")
            yield (E, b)
```

Elliptic curves



Typically done over $\mathbb{F}_p (= \text{mod } p)$ for crypto.

Smart attack

Usually given P, Q , finding a k such that $P = kQ$ is hard.

If there are p points on the curve over \mathbb{F}_p , Smart attack gives us a way to solve for k .

The challenge wants us to input a curve with p points but fails the Smart attack.

Smart attack

Usually given P, Q , finding a k such that $P = kQ$ is hard.

If there are p points on the curve over \mathbb{F}_p , Smart attack gives us a way to solve for k .

The challenge wants us to input a curve with p points but fails the Smart attack.

There is a case when the method will not work and that happens when the curve over \mathbb{Q}_p that one lifts to is the canonical lift. This will happen with probability $1/p$, which

Smart attack details

p -adic numbers are numbers of the form

$$a = a_{-2}p^{-2} + a_{-1}p^{-1} + a_0 + a_1p^1 + \cdots = \dots a_1a_0.a_{-1}a_{-2}$$

Smart attack details

p -adic numbers are numbers of the form

$$a = a_{-2}p^{-2} + a_{-1}p^{-1} + a_0 + a_1p^1 + \cdots = \dots a_1a_0.a_{-1}a_{-2}$$

$$p\text{-adic logarithm: } \log(x, y) \rightarrow -\frac{x}{y}$$

$$\text{Smart attack: } Q = kP \implies k = \frac{\log pQ}{\log pP}$$

[demo]

Smart-proof curves

Lifted curves that fail the smart attack must satisfy:

- For any point P , $(pP)_x$ has a p^{-4} term

Smart-proof curves

Lifted curves that fail the smart attack must satisfy:

- For any point P , $(pP)_x$ has a p^{-4} term
- Exists some point P with $pP = \mathcal{O}$

Smart-proof curves

Lifted curves that fail the smart attack must satisfy:

- For any point P , $(pP)_x$ has a p^{-4} term
- Exists some point P with $pP = \mathcal{O}$
- Curve must have same j -invariant mod p^2 as canonical lift

j -invariant

Consider curves $y^2 = x^3 + ax + b$, $y^2 = x^3 + a'x + b'$

Can we go from one to another with a substitution in x, y ?

j -invariant

Consider curves $y^2 = x^3 + ax + b$, $y'^2 = x^3 + a'x + b'$

Can we go from one to another with a substitution in x, y ?

$$j = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

If j -invariant are the same, then yes! ($\implies a^3 b'^2 = a'^3 b^2$)

Finding Smart-proof curves

Canonical lift is Smart-proof!

Finding Smart-proof curves

Canonical lift is Smart-proof!

Smart-proof-ness is completely determined by the a related curve mod p^2

\implies if j -invariant is same mod p^2 as canonical lift, the curve is Smart-proof

[demo]

Parametrizing solutions

Suppose $y^2 = x^3 + ax + b$ is Smart-proof and $3bm \equiv 2an \pmod{p}$
 $\Rightarrow y^2 = x^3 + (\tilde{a} + mp)x + (\tilde{b} + np)$

Parametrizing solutions

Suppose $y^2 = x^3 + ax + b$ is Smart-proof and $3bm \equiv 2an \pmod{p}$
 $\Rightarrow y^2 = x^3 + (\tilde{a} + mp)x + (\tilde{b} + np)$

At least $\frac{1}{p}$ of lifts are Smart-proof

Computing Smart-proof lifts

Canonical lift is way too complicated and takes too long to compute

1. $W := \lceil M^{\mu/(\mu+1)} \rceil$; $d :=$ any lift of $(\partial_Y \Phi_p(\sigma^{-1}(c), c))^{-1}$ to $R/p^W R$;
2. $y :=$ any lift of c ;
- 3.
4. // the first loop
5. **for** ($i := 1$; $i < W$; $++ i$) {
6. $x := \sigma^{-1}(y) \bmod p^{i+1}$;
7. $y := y - \Phi_p(x, y) d \bmod p^{i+1}$;
8. }
- 9.
10. $x := \sigma^{-1}(y) \bmod p^W$;
11. $D_X := \partial_X \Phi_p(x, y) \bmod p^W$; $D_Y := \partial_Y \Phi_p(x, y) \bmod p^W$;
- 12.
13. // the second loop
14. **for** ($m := 1$; $m W < M$; $++ m$) {
15. Lift y to $R/p^{(m+1)W} R$.
16. $x := \sigma^{-1}(y) \bmod p^{(m+1)W}$;
17. $V := \Phi_p(x, y) \bmod p^{(m+1)W}$; // note $V \equiv 0 \bmod p^{mW}$
- 18.
19. // the inner loop
20. **for** ($i := 0$; $i < W$; $++ i$) {

Computing Smart-proof lifts

Canonical lift is way too complicated and takes too long to compute

Suppose the lift $y^2 = x^3 + ax + (b + np)$ is Smart-proof and leave n unknown

Try to solve for n with conditions for Smart-proof

[demo]

All solutions

Have we found all solutions?

All solutions

Have we found all solutions?

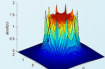
STOP DOING MATH

- NUMBERS WERE NOT SUPPOSED TO BE GIVEN NAMES
- YEARS OF COUNTING yet NO REAL-WORLD USE FOUND for going higher than your FINGERS
- Wanted to go higher anyway for a laugh? We had a tool for that: It was called "GUESSING"
- "Yes please give me ZERO of something. Please give me INFINITY of it" - Statements dreamed up by the utterly Deranged

LOOK at what Mathematicians have been demanding your Respect for all this time, with all the calculators & abacus we built for them
(This is REAL Math, done by REAL Mathematicians):




?????



???????



??????????????????

"Hello I would like  apples please"

They have played us for absolute fools

All solutions

Have we found all solutions?

Let A/k be an ordinary abelian variety with k being a perfect field of characteristic $p > 0$. Let \mathbb{A}/R be a lift with R being a Artinian local ring with residue field k .

Let $A^{\acute{e}t}$ be the étale quotient and \hat{A} is the formal completion of A . Then we have the following étale exact sequence $0 \rightarrow \hat{A} \rightarrow A \rightarrow A^{\acute{e}t} \rightarrow 0$ which splits when A is ordinary. $A^{\acute{e}t}$ can be represented in terms of the Tate module $T_p A$ as $T_p A(k) \otimes_{\mathbb{Z}_p} \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$.

We first start off with the Weil pairing $e_{p^n} : A[p^n] \times A^t[p^n] \rightarrow \mu_{p^n}$ and restrict to the k to get $e_{p^n} : \hat{A}[p^n] \times A^t(k)[p^n] \rightarrow \mu_{p^n}$ which gives us $\hat{A}[p^n] \cong \text{Hom}_{\mathbb{Z}/p^n\mathbb{Z}}(A^t(k)[p^n], \mu_{p^n})$.

For the lifted variety \mathbb{A}/R , since R is Artinian, we have a similar exact sequence that splits, $0 \rightarrow \hat{\mathbb{A}} \rightarrow \mathbb{A}[p^\infty] \rightarrow \mathbb{A}^{\acute{e}t} \rightarrow 0$. Again $\mathbb{A}^{\acute{e}t}$ can be represented as $T_p A(k) \otimes_{\mathbb{Z}_p} \frac{\mathbb{Q}_p}{\mathbb{Z}_p}$, which gives us the following exact sequences and commutative diagrams

$$\begin{array}{ccccccc} 0 & \longrightarrow & T_p E(k) & \longrightarrow & T_p E(k) \otimes_{\mathbb{Z}_p} \frac{\mathbb{Q}_p}{\mathbb{Z}_p} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \hat{\mathbb{A}} & \cdots \cdots \cdots & \hat{\mathbb{A}}[p^\infty] & \longrightarrow & T_p A(k) \otimes_{\mathbb{Z}_p} \frac{\mathbb{Q}_p}{\mathbb{Z}_p} \longrightarrow 0 \end{array}$$

which constructs $\hat{\mathbb{A}}$ via a pushout and parametrizes lifts by $\text{Ext}^1(\hat{\mathbb{A}}, T_p A(k) \otimes_{\mathbb{Z}_p} \frac{\mathbb{Q}_p}{\mathbb{Z}_p})$.

Furthermore, we can extend the isomorphism $\hat{A}[p^n] \cong \text{Hom}_{\mathbb{Z}/p^n\mathbb{Z}}(A^t(k)[p^n], \mu_{p^n})$ to $\hat{\mathbb{A}}[p^n] \cong \text{Hom}_{\mathbb{Z}/p^n\mathbb{Z}}(A^t(k)[p^n], \mu_{p^n})$ and by taking a categorical limit, we obtain $\hat{\mathbb{A}} \cong \text{Hom}_{\mathbb{Z}_p}(T_p A^t(k), \hat{\mathbb{G}}_m)$

Finally we can obtain the Serre-Tate coordinates. The isomorphism in the previous paragraph gives us a bilinear form $E_{\hat{\mathbb{A}}} : \hat{\mathbb{A}} \times T_p A^t(k) \rightarrow \hat{\mathbb{G}}_m$ and the pushout gives us a morphism for each lift, $\phi_{\hat{\mathbb{A}}} : T_p E(k) \rightarrow \hat{\mathbb{A}}$ and finally define the bilinear form $q(\hat{\mathbb{A}}; \alpha; \alpha_t) = E_{\hat{\mathbb{A}}}(\phi_{\hat{\mathbb{A}}} \alpha, \alpha_t)$. We can select basis elements for $T_p E(k)$ as a free module over \mathbb{Z}_p , giving us $q(\hat{\mathbb{A}}; -, -) \in \text{Hom}_{\mathbb{Z}_p}(T_p A(k) \otimes T_p A^t(k), \hat{\mathbb{G}}_m(R)) \cong \mathbb{Z}_p^{g^2}$

With these, we have the following theorem:

Theorem 2. *At most $\frac{1}{p}$ of lifts of ordinary elliptic curves, when taken mod p^n for any n , has p -torsion.*

Open problems

How do we generate curves with $0 \leq a, b < p$ that are Smart-proof?

Classification of Smart-proof curves

HATS lightning talk

August 29, 2020