Smart's Attack Over Non Prime Field

Pierre Chrétien

June 2025

1 Introduction

Let p be a prime, an elliptic curve $E/\mathbb{F}_p$ is said to be *anomalous* if $\sharp E(\mathbb{F}_p) = p$, equivalently these are *trace one curves*. Such curves are vulnerable to Smart's attack [6] which reduces the discrete logarithm problem (DLP) from $E(\mathbb{F}_p)$ to $(\mathbb{F}_p, +)$ which is trivial. Smart's attack over prime fields is a usual tool to solve some CTF. Variations include applying Smart's attack cautiously in order to avoid canonical lifts of $E/\mathbb{F}_p$ (which make the attack fail)[1]. Smart's attack generalizes easily to trace one elliptic curves over non prime fields (i.e. $\mathbb{F}_q$ with $q = p^n$, $n \geq 2$), see [1]. The rest of this note is organized as follows. Section 2 presents standard Smart's attack subtleties and pitfalls. Section 3 presents Smart's attack over non prime fields following [1] and fill in some gaps in the theory presented there. Section 4 gives implementation details of Smart's attack in SageMath, commenting the code available on GitHub[2].

This note is purely for educational purpose. One also provides a SageMath implementation of the attack for anomalous curves over non prime fields.

2 Comments about the prime field case

Comprehensive presentations of Smart's attack may be found in [1], [2]. There are various implementations over $\mathbb{F}_p$[3,4]. Let p be a prime and $\overline{E}/\mathbb{F}_p$ be an elliptic curve such that $\sharp\overline{E}(\mathbb{F}_p) = p$.

1. Given an instance of the DLP, $k\overline{P} = \overline{Q}$ in $\overline{E}$, Smart's attack recovers the secret key (only modulo p though), subject to $pQ \notin E_2(\mathbb{Q}_p)$, where Q is any lift of $\overline{Q}$ to a lift $E/\mathbb{Q}_p$ of $\overline{E}$. This might force us to try another lift of Q and run the attack once again, see below.
2. As noted in [6], the attack might fail in the case one hits a so called canonical lift $E/\mathbb{Q}_p$ of $\overline{E}$, which occurs with negligible probabilty. See also StackExchange[5]. This was a flaw to be exploited in, for example, DEF CON CTF Qualifier 2020.
3. Smart's attack also shows up when dealing with group structure of elliptic curves over $\mathbb{Z}/p^e\mathbb{Z}$, see [3] (active CTF using this remark are still online at the time of writing, so one do not give any further detail).

3 Smart's attack over non prime field

3.1 Backgroung material

Let p be a prime, $n \in \mathbb{N} - \{0\}$ and $q = p^n$. Let $f(X) \in \mathbb{Z}_p[X]$ be monic of degree n such that $\overline{f}(X) \in \mathbb{F}_p[X]$ is irreducible (thus separable since $\mathbb{F}_p$ is finite). According to [4] Chap I §6, $f(X)$ is irreducible in $\mathbb{Q}_p[X]$ and $\mathbb{L} = \mathbb{Q}_p[X]/(f(X))$ is the unramified extension of $\mathbb{Q}_p$ of degree n. Moreover, the residue field of $\mathbb{L}$ is isomorphic to $\mathbb{F}_q$. The valuation v_p of $\mathbb{Q}_p$ extends uniquely to a valuation $v_{\mathbb{L}}$ on $\mathbb{L}$ with ramification index $e_{\mathbb{L}/\mathbb{Q}_p} = 1$, i.e. p is a uniformizer for $\mathbb{L}$ and one still denotes $v_p = v_{\mathbb{L}}$ (see [4] Chap II §3). One denotes by $\mathcal{O}_{\mathbb{L}} = \{x \in \mathbb{L}, v_p(x) \geq 0\}$ the ring of integers of $\mathbb{L}$. Let $\overline{E}/\mathbb{F}_q$ be an elliptic curve such that $\sharp\overline{E}(\mathbb{F}_q) = q$. Let $E/\mathbb{L}$ be a lift of $\overline{E}/\mathbb{F}_q$ and denote

$$E_1(\mathbb{L}) = \{P \in E(\mathbb{L}), \overline{P} = 0_{\overline{E}}\}$$

One has the exact sequence (see [5] VII 2.1)

$$0 \to E_1(\mathbb{L}) \to E(\mathbb{L}) \to \overline{E}(\mathbb{F}_q) \to 0$$

which yields $E(\mathbb{L})/E_1(\mathbb{L}) \simeq \overline{E}(\mathbb{F}_q)$.

[1] https://ctftime.org/writeup/20698

[2] https://github.com/pierrechr/pierre.c/tree/main/NonPrimeSmart

[3] https://wstein.org/edu/2010/414/projects/novotney.pdf

[4] https://crypto.stackexchange.com/questions/70454/why-smarts-attack-doesnt-work-on-this-ecdlp

[5] https://math.stackexchange.com/questions/3688569/canonical-lift-of-elliptic-curve-in-smart-attack

Let $\hat{E}/\mathcal{O}_{\mathbb{L}}$ be the formal group associated to $E/\mathbb{L}$. As long as $E/\mathbb{L}$ is a minimal Weierstrass model (that is with coefficients in $\mathcal{O}_{\mathbb{L}}$ and such that $v_p(\Delta_E)$ is minimal among such equations, see [5] VII.1), one has the following isomorphim

$$\begin{aligned}\theta : E_1(\mathbb{L}) &\xrightarrow{\sim} \hat{E}(p\mathcal{O}_{\mathbb{L}}) \\ (x,y) &\mapsto -\frac{x}{y}\end{aligned}$$

Let $E_n(\mathbb{L}) = \{(x,y) \in E(\mathbb{L}), v_p(x) \leq -2n, v_p(y) \leq -3n\} \cup \{0_E\}$. The proof of θ being an isomorphism generalizes to

$$\begin{aligned}\theta_n : E_n(\mathbb{L}) &\xrightarrow{\sim} \hat{E}(p^n\mathcal{O}_{\mathbb{L}}) \\ (x,y) &\mapsto -\frac{x}{y}\end{aligned}$$

Proof. Following the proof of [5] VII 2.2, one only has to check that the restriction of θ from $E_1(\mathbb{L})$ to $E_n(\mathbb{L})$ has image $\hat{E}(p^n\mathcal{O}_{\mathbb{L}})$. Let $x, y \in E_n(\mathbb{L})$, then $v_p(x) \leq -2n$ and $2v_p(y) = 3v_p(x)$ thus

$$2v_p(\frac{x}{y}) = 2v_p(x) - 2v_p(y) = -v_p(x) \geq 2n \Rightarrow \frac{x}{y} \in p^n\mathcal{O}_{\mathbb{L}}$$

Note that, conversely, $u \in p^n\mathcal{O}_{\mathbb{L}}$ corresponds to $(x(u); y(u)) \in \hat{E}$ with

$$\begin{aligned}w(u) &= u^3(1 + A_1u + A_2u^2 + \dots) \\ x(u) &= \frac{u}{w(u)} = \frac{1}{u^2} - \frac{\alpha_1}{u} - \alpha_2 \dots \\ y(u) &= -\frac{1}{w(u)} = -\frac{1}{u^3} + \frac{\alpha_1}{u^2} + \frac{\alpha_2}{u} \dots\end{aligned}$$

Then $v_p(x(u)) = -2v_p(u) \leq -2n$, $v_p(y(u)) = -3v_p(u) \leq -3n$, thus $(x(u), y(u)) \in E_n(\mathbb{L})$. □

According to [5] IV.6.4., the formal logarithm induces an isomorphism for any non zero integer r (note that, in our discussion, $v(p) = v_p(p) = 1$, thus the condition $r > \frac{v(p)}{p-1}$ holds).

$$\log_{\mathcal{F}} : \hat{E}(p^r\mathcal{O}_{\mathbb{L}}) \xrightarrow{\sim} (p^r\mathcal{O}_{\mathbb{L}}, +)$$

This yields an isomorphism $\psi = \log_{\mathcal{F}} \circ \theta_n : E_n(\mathbb{L}) \xrightarrow{\sim} (p^n\mathcal{O}_{\mathbb{L}}, +)$

Remark 1. This is somehow an abuse of notation since ψ depends on n, but these isomorphisms are compatible with inclusions $E_{n+1}(\mathbb{L}) \subset E_n(\mathbb{L})$ and $(p^{n+1}\mathcal{O}_{\mathbb{L}}, +) \subset (p^n\mathcal{O}_{\mathbb{L}}, +)$.

3.2 The attack

Assume that one is given an instance of the DLP :

$$\overline{P} = k \times \overline{G}, \quad \overline{P}, \overline{G} \in \overline{E}(\mathbb{F}_q), \quad k \in \mathbb{Z}$$

Let $k = \sum_{i=0}^{n-1} k_i p^i$ be the p-adic expansion of k modulo $p^n = q$. Let $S := P - kG$ where $P, G \in E(\mathbb{L})$ are lifts of $\overline{P}, \overline{G}$. Then $\overline{S} = 0_{\overline{E}}$, thus $S \in E_1(\mathbb{L})$. Since (recall that p is a uniformizer of $\mathbb{L}$, thus $p\mathcal{O}_{\mathbb{L}}$ is the maximal ideal of $\mathcal{O}_{\mathbb{L}}$)

$$E_1(\mathbb{L})/E_2(\mathbb{L}) \simeq (p\mathcal{O}_{\mathbb{L}}/p^2\mathcal{O}_{\mathbb{L}}, +) \simeq (\mathcal{O}_{\mathbb{L}}/p\mathcal{O}_{\mathbb{L}}, +) \simeq (\mathbb{F}_q, +)$$

one has $qS \in E_2(\mathbb{L})$. Thus, one has

$$\begin{aligned}\psi(qS) = \psi(qP) - k\psi(qG) &\in p^2\mathcal{O}_{\mathbb{L}} \\ \Rightarrow k\psi(qG) = \psi(qP) &\mod p^2 \qquad\qquad (*)\end{aligned}$$

One the other hand, $qP, qG \in E_1(\mathbb{L})$ since $E(\mathbb{L})/E_1(\mathbb{L}) \simeq \overline{E}(\mathbb{F}_q)$ which has order q by assumption. This gives

$$\begin{aligned}qP \in E_1(\mathbb{L}) \Rightarrow \psi(qP) \in p\mathcal{O}_{\mathbb{L}} \Rightarrow \psi(qP) = 0 + a_1p + a_2p^2 + \dots, \quad a_i \in \mathcal{O}_{\mathbb{L}} \\ qG \in E_1(\mathbb{L}) \Rightarrow \psi(qG) \in p\mathcal{O}_{\mathbb{L}} \Rightarrow \psi(qG) = 0 + b_1p + b_2p^2 + \dots, \quad b_i \in \mathcal{O}_{\mathbb{L}}\end{aligned}$$

Then $(*)$ reads, as long as p does not divide b_1,

$$k\psi(qG) = \psi(qP) \mod p^2 \Rightarrow kb_1p = a_1p \mod p^2 \Rightarrow kb_1 = a_1 \mod p \Rightarrow k = \frac{a_1}{b_1} \mod p$$

Remark 2. This is the exact same pitfall as in the prime field case : if $b_1 = 0 \mod p$, i.e. $qG \in E_2(\mathbb{L})$, then $qP = qS + qkG \in E_2(\mathbb{L})$ (note that $E_2(\mathbb{L})$ is a group), i.e. $a_1 = 0 \mod p$ and $(*)$ reads $0k = 0 \mod p^2$ giving no information about k.

That is, one recovered k_0 in the p-adic expansion of k. Next, put $P_1 = P - k_0G, G_1 = pG$ and note that

$$\begin{aligned}
\overline{P_1} &= \overline{P} - k_0\overline{G} \\
&= k_1p\overline{G} + k_2p^2\overline{G} + \cdots + k_np^n\overline{G} \\
&= k_1\overline{G_1} + k_2p\overline{G_1} + \cdots + k_np^{n-1}\overline{G_1} \\
&= \Big(\frac{k-k_0}{p}\Big)\overline{G_1}
\end{aligned}$$

By the above process one recovers k_1. Iterating yields the secret key k.

4 Comments on implementation and pitfalls

4.1 Finding trace one elliptic curves

In order to bench test our code, one first need to find an elliptic curve such that $\overline{E}(\mathbb{F}_q) = q$. Using standard complex multiplication and Class Field Theory, finding some trace 1 curve $\overline{E}/\mathbb{F}_q$ boils down to find a prime p, an integer n, and a discriminant D such that

$$4p^n = 1 + Dy^2,$$

has an integer solution y (this is the so called *norm equation*).

When $n = 1$ there are plenty of such primes for a given D (see [2]). But when $n > 1$, this is no more the case. It is a work in progress to study in some more details this last situation. For now, one only gives a naive brute force search algorithm and somehow direct computation of Hilbert polynomial H_D using SageMath in order to produce trace one elliptic curves of $\mathbb{F}_q$. This has also been implemented in C++ using NTL for efficiency reasons.

4.2 The attack

Disclaimer : this implementation if purely for educational purpose and is not intended to be optimized. It has been produced to give insight into the technical details of the attack. Nonetheless, to the best of our knowledge this is the first correct implementation available of the attack over non prime fields.

We will go through some meaningfull steps of the SageMath code available on our GitHub project[6]. Let `kP = Q` be an instance of the DLP in an anomalous elliptic curve $E/\mathbb{F}_q$.

1. The first trap is to overlook the meaning of *the residue field of* $\mathcal{O}_\mathbb{L}$ *being (isomorphic to)* $\mathbb{F}_q$. One first has to retrieve the representation of $\mathbb{F}_q$ used to describe $E/\mathbb{F}_q$, then work it out to the correct representation of $\mathbb{L}$.

```
E = P.curve()
kE = E.base_field()
p = kE.characteristic()
n = kE.degree()
modE = kE.modulus()
Qur.<a> = Qp(p,prec=prec).extension(modE,prec=prec)
k = Qur.residue_field()
mod = k.modulus()
assert mod == modE
```

2. The fields `k` and `kE` have the same modulus (with a down-to-earth point of view : multiplication and addition tables are the same) but are not equal, so one has to use some way to go from a representation to another, that is switch the primitive elements.

```
ak = k.gens()[0]
akE = kE.gens()[0]
phi_kE_to_k =  FiniteFieldHomomorphism_generic(Hom(kE,k))
phi_k_to_kE =  FiniteFieldHomomorphism_generic(Hom(k,kE))
assert phi_kE_to_k(akE) == ak
```

[6] https://github.com/pierrechr/pierre.c/tree/main/NonPrimeSmart

This is obviously a very theoretic way of writing down the isomorphism between finite fields but has the advantage of being general. In our situation, retrieving the coefficients of some `z` in `k` as a polynomial in `ak` and writing the polynomial with those coefficients in the variable `akE` would be fine as `mod == modE`.

3. Next, one has to lift elements from `kE` (or `k` after applying `phi_kE_to_k`) to $\mathbb{L}$ taking care of the precision of the p-adic expansion.

```
f = ResidueLiftingMap._create_(kE,Qur)
```

   Actually, the above `ResidueLiftingMap` method might be somehow lazy and lift with precision $\mathcal{O}(p)$, which is insufficient for the attack to be successful (which requires precision at least $\mathcal{O}(p^2)$). That's why our code uses the method `lift_to_precision()` to get x-coordinates in $\mathbb{L}$ with the desired precision before lifting to the elliptic curve.

4. Finally, in order to avoid canonical lifts, one introduces some randomness in the coefficients of the lift. In the very unlikely case where one hits such a lift (and the attack fails), one has to run the attack again.

```
EllipticCurve(Qur,[f(a).lift_to_precision(prec) +randint(0,p)*p for a in E.a_invariants()])
```

Remark 3. At the time of writing, while checking bibliography, the author found another implementation of the full attack available on GitHub[7]. Unfortunately, it is subject to the pitfalls described above as shown by the following code.

```
E = P.curve()
F = E.base_ring()
modE = F.modulus()
q = F.order()
qq = Qq(q, names="g")
modqq = qq.residue_field().modulus()
assert modE == modqq
```

References

[1] Hofman S. J. The discrete logarithm problem on anomalous elliptic curves. Bachelor's thesis, University of Groningen, 2020.

[2] Franck Leprévost, Jean Monnerat, Sébastien Varrette, and Serge Vaudenay. Generating anomalous elliptic curves. *Information Processing Letters*, 93(5):225–230, 2005.

[3] Massimiliano Sala and Daniele Taufer. Group structure of elliptic curves over $\mathbb{Z}/\mathrm{N}\mathbb{Z}$. *Journal of Mathematical Cryptology*, 18(1), January 2024.

[4] Jean-Pierre Serre. *Corps locaux.* Hermann, 2004.

[5] Joseph H Silverman. *The Arithmetic of Elliptic Curves.* Graduate texts in mathematics. Springer, Dordrecht, 2009.

[6] N.P. Smart. The discrete logarithm problem on elliptic curves of trace one. *J. Cryptology*, 12:193–196, 1999.

[7] https://github.com/jvdsn/crypto-attacks/blob/master/attacks/ecc