

**On computing discrete logarithms in
Formal groups and its applications
Or
How I Learned To Stop Worrying (about
the Anomalous case) And Love Formal
Groups**

Iftikhar A Burhanuddin
burhanud@usc.edu

Joint work with
Ming-Deh Huang and Qing Luo

Computer Science Department
University of Southern California

July 28, 2003
ACA, Raliegh

Outline

1. DLP and Cryptography
2. Elliptic Curves
3. Formal Groups
4. Elliptic Curve Formal Group
5. DLP over certain groups
6. Conclusions

DLP & Cryptography

G an abelian (additive) group.

| System | Problem (easy) | Inverse (“hard”) |
|-----------|--------------------------------|---------------------------|
| RSA | Multiplication in \mathbf{Z} | Factoring in \mathbf{Z} |
| DLP / G | Repeated “addition” | Computing DL |

where easy = \exists poly time algorithm, “hard” = known algorithms take more than poly time.

Given $\alpha, \beta \in G$ and $\beta \in \langle \alpha \rangle$ to compute $u \in \mathbf{Z}$ such that

$$\beta = [u]\alpha$$

is called the **D**iscrete **L**ogarithm **P**roblem.

Decisional DLP. Given $\alpha, \beta \in G$ does there exist $u \in \mathbf{Z}$ such that

$$\beta = [u]\alpha?$$

Example 1. $G = \mathbf{F}_q$ where $q = p^n$.

Say $q = p = 10000000019$ and $g = 2 \pmod{p}$.

$h = 3400422793 \pmod{p}$.

Task. Given $h = u \cdot g$ in \mathbf{F}_p to compute u .

Technique. Use the multiplicative structure of \mathbf{F}_p .

$$u = h * (g)^{-1} = 6700211406$$

Example 2. Classical version. $G = \mathbf{F}_q^*$ where $q = p^n$. DH key exchange (1976)

Say $q = p = 10000000019$ and $g = 2 \pmod{p}$.

$h = 3400422793 \pmod{p}$.

Task. Given $h = g^u$ in \mathbf{F}_p^* to compute u .

Technique. Naive takes $O(p)$ worst case time.
 $u = 1729$.

- \exists subexponential DLP algorithms. Index Calculus takes $O(L_p[c, 1/2])$ group ops, advanced sieving methods (NFS / FFS) take $O(L_p[c, 1/3])$ time

A weak instance: $\#\mathbf{F}_q^* = q - 1$ is smooth.
Avoided by ensuring $q - 1$ has a large prime.

Example 3 Fancier (Modern) versions: Koblitz, Miller (1985)

$E(\mathbf{F}_q)$, $J(\mathbf{F}_q)$, $A(\mathbf{F}_q)$ - \mathbf{F}_q rational points of an elliptic curve, jacobian of a curve, abelian variety resp.

- known algorithms take exponential time to compute DL :(or :)

A weak instance: **Anomalous** case

$$\#E(\mathbf{F}_q) = p^i$$

Technique (Smart / Satoh-Araki): Lifting to local fields and formal groups.

Elliptic Curves

An **elliptic curve** over a field K is a smooth projective curve E of genus 1 defined over K with a specified point $O \in E(K)$.

Every E can be embedded as a smooth curve in \mathbf{P}^2 and given by a "Weierstrass equation"

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

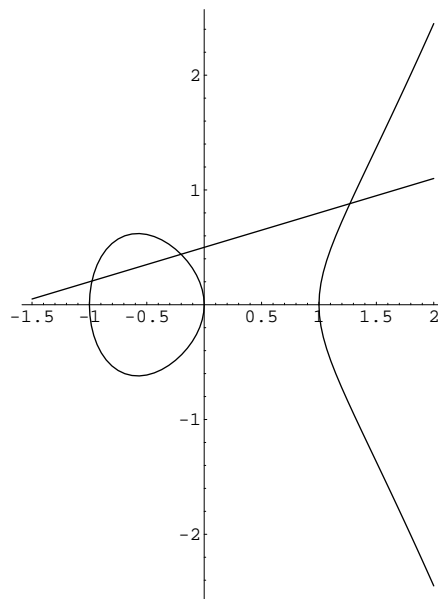
with $a_i \in K$ and O is $[0, 1, 0]$ the point at ∞ .

Moreover, every smooth Weierstrass plane cubic curve is an elliptic curve.

If $\text{char } K \neq 2, 3$, then E has a Weierstrass equation with $a_1 = a_2 = a_3 = 0$ and is written $y^2 = x^3 + ax + b$. Non-singularity \Leftrightarrow the discriminant $\Delta := -16(4a^3 + 27b^2) \neq 0$.

E has a unique holomorphic differential (up to scalar) which is given by

$$\omega_E = \frac{dx}{2y}$$



$$E/\mathbf{R} : y^2 = x^3 - x, \Delta = -4$$

Addition law on E (chord-tangent method):

$P_1, P_2 \in E(K)$ with $P_1 \neq P_2$ and drawing a line L thru P_1, P_2 , we get a third point P_3 i.e.

$L \cap E = \{P_1, P_2, P_3\}$, we write

$$P_1 \oplus P_2 := -P_3$$

where inverse of $P = (x, y) \in E(K)$ is $-P = (x, -y) \in E(K)$.

$\Rightarrow E(K)$ an abelian group with O as identity.

If $\text{char } K \neq 2, 3$ addition law is given by:

$$P = (x_1, y_1), Q = (x_2, y_2), P \oplus Q = (x_3, y_3).$$

$$x_3 = -x_1 - x_2 + \alpha^2; \quad y_3 = -y_1 + \alpha(x_1 - x_3)$$

$$\alpha = \begin{cases} (y_2 - y_1)/(x_2 - x_1) & \text{if } P \neq Q \\ (3x_1^2 + a)/2y_1 & \text{if } P = Q \end{cases}$$

Elliptic Curves over finite fields

Gp-order. (Hasse's window) $\#E(\mathbf{F}_q) = q + 1 - t$ with $|t| \leq 2\sqrt{q}$.

Gp-structure. $E(\mathbf{F}_q)$ is cyclic or $\mathbf{Z}/d_1\mathbf{Z} \times \mathbf{Z}/d_2\mathbf{Z}$ where $d_1|d_2$ and $d_1|q - 1$.

Questions.

- Determining $\#E(\mathbf{F}_q)$ aka Point counting
... \exists polynomial time algorithms
 - Schoof (q large prime)
 - Satoh ($q = p^n$, p small n large)
- Computing d_i and generators ... no known polynomial time algorithms
- DLP over $E(\mathbf{F}_q)$. **Anomalous** case is the focus of this talk.

Formal group (F-gp) laws

A f-gp law is a generalization of the binary operation of a group.

Let R is a comm ring with identity and X be (X_1, \dots, X_n) .

An n -dim (or more aptly n -parameter) **f-gp law** over a ring R is an n -tuple of formal series in $2n$ variables

$X \oplus_F Y := F(X, Y) = (F_1(X, Y), \dots, F_n(X, Y))$
 $\in R[[X, Y]]^n$ such that (in succinct nonstandard notation)

1. $X \oplus_F Y = X + Y +$ higher degree terms
2. $(X \oplus_F Y) \oplus_F Z = X \oplus_F (Y \oplus_F Z)$ (associativity)

3. $X \oplus_F 0 = X$ and $0 \oplus_F Y = Y$ (identity)

4. $X \oplus_F I(X) = 0$ (inverse)

Also if $X \oplus_F Y = Y \oplus_F X$ then F is a **commu-**
tative f-gp law.

But no underlying group yet!

Simple 1-dim Examples.

1. $G_a(z_1, z_2) = z_1 + z_2$

2. $G_m(z_1, z_2) = z_1 + z_2 + z_1 z_2$

3. $F_E(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2 (z_1^2 z_2 + z_1 z_2^2) - (2a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3) z_1^2 z_2^2 + 2a_3 z_1 z_2^3) + \dots \in \mathbf{Z}[a_1, \dots, a_6] [[z_1, z_2]]$

Formal group Law of an Elliptic Curve

Motivation to look at objects locally is they become easier to analyze. So let's examine the elliptic curve and its group law locally at O .

Notation.

K a field of characteristic zero

$K[E]_O$ the local ring of functions of E defined at O

N the maximal ideal of $K[E]_O$

$K[\hat{E}]_O$ the completion of the local ring at N

$K[\hat{E}]_O \cong K[[z]]$ for some "local uniformizer" z (i.e. a generator of N) at O .

Express Weierstrass coordinates x, y as power series in z .

$$m : E \times E \rightarrow E$$

$$(P, Q) \mapsto P \oplus Q$$

And express what the elliptic curve group law looks like locally at O as a power series.

In more **concrete terms** we start by applying a change of coordinates $(z = -\frac{x}{y}, w = -\frac{1}{y})$

$$x \rightarrow \frac{z}{w}$$

$$y \rightarrow -\frac{1}{w}$$

↓

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

$$\rightarrow w = z^3 + a_1zw + a_2z^2w + a^3w^2 + a_4zw^2 + a_6w^3 (= f(z, w))$$

$$O \rightarrow (z, w) = (0, 0)$$

Translate things which happen on the LHS to RHS.

z has a zero of order 1 at O and hence is a generator of N .

By repeated substitution we obtain the formal series

$$w(z) = z^3(1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + a_3)z^3 + (a_1^4 + 3a_1^2a_2 + 3a_1a_3 + a_2^2 + 2a_4)z^4 + \dots) \in \mathbf{Z}[a_1, \dots, a_6][[z]]$$

which is the unique power series satisfying $w(z) = f(z, w(z))$. Hence a point is now parameterized by one parameter.

↓

$$\begin{aligned} x(z) &= \frac{z}{w(z)} \\ &= z^{-2} - a_1z^{-1} - a_2 - a_3z - (a_4 + a_1a_3)z^2 - \dots \\ y(z) &= -\frac{1}{w(z)} \\ &= -z^{-3} + a_1z^{-2} + a_2z^{-1} + a_3 + (a_4 + a_1a_3)z - \dots \end{aligned}$$

Using these we can write down a power series which gives the group law of E at O . Chord-Tangent method: Draw a line through points $P_i = (z_i, w(z_i)), i = 1, 2$ and this line will hit the curve at P_3 the inverse of which will give us point $P_1 \oplus P_2 = -P_3 = (z_3, w(z_3))$

$$z_3 = F_E(z_1, z_2) = z_1 + z_2 - a_1 z_1 z_2 - a_2 (z_1^2 z_2 + z_1 z_2^2) - (2a_3 z_1^3 z_2 - (a_1 a_2 - 3a_3) z_1^2 z_2^2 + 2a_3 z_1 z_2^3) + \dots \in \mathbf{Z}[a_1, \dots, a_6][[z_1, z_2]]$$

Elliptic Curve Formal Group

There's no underlying group yet. F-gp laws are just a generalisation of a binary operation. For

$$F(z_1, z_2) = z_1 + z_2 + \text{terms of degree } \geq 2$$

Taking R to be a complete local ring and assigning the variables values from M the maximal ideal of R then the power series converge.

Et voila! Definition of the f-gp law \Rightarrow we have a group.

For $z_1, z_2 \in M$, $\hat{F}(M)$ is abelian group with $F(z_1, z_2)$ the group operation.

F also induces a group structure on M^i which results in this filtration sequence

$$\hat{F}(M) \supset \hat{F}(M^2) \supset \dots \supset \hat{F}(M^i) \supset \dots \supset \hat{F}(0)$$

Remark. Most of the theorems which follow will hold for n -dim comm formal groups over complete local rings but will look at specific ones keeping our application to cryptography in mind.

Notation.

| | |
|-----------------|---|
| K | finite extension of \mathbf{Q}_p with normalized valuation $v : K^* \rightarrow \mathbf{Z}$ |
| R | the ring of integers of $K = \{x \in K \mid v(x) \geq 0\}$ |
| R^* | the unit group of $R = \{x \in K \mid v(x) = 0\}$ |
| M | the maximal ideal of $R = \{x \in K \mid v(x) > 0\}$ |
| π | a uniformizer for R (i.e., $M = \pi R$) |
| k | the residue field of $R = R/M = \mathbf{F}_q$ |
| p | characteristic of k |
| M^c | the set of c tuples of elements in M |
| M^d | ideal of R with elements of the form $\sum_{i=1}^k m_1 m_2 \dots m_d, \quad m_i \in M, k \in \mathbf{Z}_{>0}$ |
| $F_E(z_1, z_2)$ | 1-dim comm elliptic curve f-gp law over R |

Assuming normalized valuation $v(\pi) = 1$.

Examples. For $z_1, z_2 \in M$

- $\hat{G}_a(M)$ with $G_a(z_1, z_2) = z_1 + z_2$. So it is $(M, +)$. Nice!
- $\hat{G}_m(M)$ with $G_m(z_1, z_2) = z_1 + z_2 + z_1z_2$.
- $\hat{E}(M)$ with $F_E(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - (2a_3z_1^3z_2 - (a_1a_2 - 3a_3)z_1^2z_2^2 + 2a_3z_1z_2^3) + \dots$

The latter is the **Elliptic curve f-gp**

The elliptic curve formal group filtration sequence

$$\hat{E}(M) \supset \hat{E}(M^2) \supset \dots \supset \hat{E}(M^i) \supset \dots \supset \hat{E}(0)$$

Theorem

- For $i \geq 1$. Induced by the identity map on sets

$$\hat{E}(M^i)/\hat{E}(M^{i+1}) \cong M^i/M^{i+1} = \mathbf{F}_q$$

Logarithm map

Idea. Solving DLP on an additive f-gp is easy. So why not impose an additive structure on the given f-gp?

$$\begin{aligned}\omega_E(z) &= \frac{d(w(z))}{2y(z)+a_1x(z)+a_3} \\ &= (1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + 2a_3)z^3 + \dots)dz \\ \log_E(z) &= \int \omega_E(z) \\ &= z + \frac{1}{2}a_1z^2 + \frac{1}{3}(a_1^2 + a_2)z^3 + \frac{1}{4}(a_1^3 + 2a_1a_2 + 2a_3)z^4 + \dots\end{aligned}$$

Remark. The invariant differential ω_E induces an invariant differential on the formal group, the formal integration of which gives the logarithm map.

Theorem.

- For $r > v(p)/(p - 1)$

$$\log_{F_E} : \hat{E}(M^r) \cong \hat{G}_a(M^r)$$

A level (in the filtration sequence) preserving map.

$v(p) = e =$ ramification index.

If K is a unramified extension of \mathbf{Q}_p and $p \neq 2$ then taking $r = 1 > 1/p - 1$ we have

$$\hat{E}(M) \cong \hat{G}_a(M) = M$$

The Reduction map

The natural reduction map

$$\begin{aligned} R &\rightarrow R/\pi R = k = \mathbf{F}_q \\ t &\mapsto \bar{t} = t \bmod \pi \end{aligned}$$

A Weierstrass equation for an elliptic curve is of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in K$

We would like to talk about reducing an elliptic curve modulo π meaningfully and hence need to work with a minimal Weierstrass equation for the curve which is obtained by a change of coordinates.

Defintion. A minimal Weierstrass equation for an elliptic curve E/K is a Weierstrass equation if $v(\Delta)$ is minimized with $a_i \in R$.

Theorem

- Every elliptic curve E/K has a minimal Weierstrass equation which is unique (upto change of coordinates)

So given a minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in R$ the reduction of E modulo π is the curve \overline{E} over k given by

$$\overline{E} : y^2 + \overline{a_1}xy + \overline{a_3}y = x^3 + \overline{a_2}x^2 + \overline{a_4}x + \overline{a_6}$$

where $\overline{a_i}$ denotes reduction of a_i modulo π .

\overline{E} is unique upto standard change of coordinates for Weierstrass equations over k .

Observe that the reduced curve \overline{E} may be singular.

$$\begin{array}{ccc} \mathbf{P}^2(K) & \rightarrow & \mathbf{P}^2(R/M) \\ E(K) & \rightarrow & \overline{E}(k) \\ P & \mapsto & \overline{P} \end{array}$$

is called the **reduction map**.

$$P = [x, y, z] \in E(K)$$

$$\Rightarrow [x, y, z] \in R^3 \text{ with at least one of them in } R^*$$

$$\Rightarrow \bar{P} = [\bar{x}, \bar{y}, \bar{z}] \in \bar{E}(k)$$

We say E has **good** (or stable) reduction if \bar{E} is non singular.

We'll assume **good** reduction from here on.

Theorem We have the following exact sequence and $E_1(K)$ is the kernel of the reduction map

$$0 \rightarrow E_1(K) \rightarrow E(K) \rightarrow \bar{E}(k) \rightarrow 0$$

Notation.

$$E_1(K) = \{P \in E(K) \mid \bar{P} = \bar{O}\}$$

$$E_r(K) = \{P \in E(K) \mid v(x(P)) \leq -2r\} \text{ for } r \geq 1$$

We have a filtration sequence of subgroups of $E(K)$

$$E(K) \supset E_1(K) \supset E_2(K) \supset \dots \supset E_i(K) \supset \dots \supset O$$

Theorem.

$$\lambda : \begin{cases} E_1(K) & \cong & \hat{E}(M) \\ P & \mapsto & -\frac{x(P)}{y(P)} \end{cases}$$

and this isomorphism identifies for $i \geq 1$

$$E_i(K) \cong \hat{E}(M^i)$$

$$\begin{array}{ccccccc} E(K) \supset & E_1(K) & \supset & E_2(K) & \dots & \supset & E_i(K) & \dots \\ & \cong & & \cong & & & \cong & \\ & \hat{E}(M) & \supset & \hat{E}(M^2) & \dots & \supset & \hat{E}(M^i) & \dots \end{array}$$

Remark. Working with $a_i \in R$ makes the associated f-gp law

$$F_E(z_1, z_2) \in \mathbf{Z}[a_1, \dots, a_6] [[z_1, z_2]] \subset R [[z_1, z_2]].$$

ECDLP over a finite extension of \mathbb{Q}_p

Definition (Discrete logarithm problem over $E(K)$).

Given points $S, T \in E(K)$ with $T \in \langle S \rangle$ to compute $u \in \mathbb{Z}$ such that $T = uS$.

Let E be an elliptic curve defined over K and let its minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in R$ and $v(\Delta) \geq 0$. We assume that E has **good reduction** at π .

↓

We denote the reduced elliptic curve over $k = \mathbb{F}_q$ by \overline{E} which is given by

$$y^2 + \overline{a}_1xy + \overline{a}_3y = x^3 + \overline{a}_2x^2 + \overline{a}_4x + \overline{a}_6$$

where $\bar{a}_i \in \mathbf{F}_q$ and $\bar{a}_i = a_i \bmod \pi$.

Let $n = \#\bar{E}(\mathbf{F}_q)$ denote the order of the group of \mathbf{F}_q rational points on \bar{E} .

From the exact sequence mentioned earlier we have

$$E(K)/E_1(K) \cong \bar{E}(\mathbf{F}_q)$$

Main idea. Move the problem to $\hat{E}(M)$ via $E_1(K)$ realising its easier to work with $\hat{E}(M)$ since a subgroup of it has an additive structure given by the following map

$$\log_E = \begin{cases} \hat{E}(M^r) & \rightarrow \hat{G}(M^r) \\ z & \mapsto z + \frac{1}{2}a_1z^2 + \frac{1}{3}(a_1^2 + a_2)z^3 + \\ & \frac{1}{4}(a_1^3 + 2a_1a_2 + 2a_3)z^4 + \\ & \dots \end{cases}$$

where $r = \lceil v(p)/(p-1) \rceil$. Let $[l]$ denote \times by l -map for $l \in \mathbf{Z}$. The diagram below illustrates our algorithm.

$$\begin{array}{ccccccc}
E(K) & \supset & E_1(K) & \supset & E_2(K) & \dots & \supset & E_r(K) \\
& & \cong & & \cong & & & \cong \\
& & \widehat{E}(M) & \supset & \widehat{E}(M^2) & \dots & \supset & \widehat{E}(M^r) \\
& & & & & & & \cong \\
& & & & & & & \widehat{G}(M^r)
\end{array}$$

$$\begin{array}{ccccc}
E(K) & \xrightarrow{[n]} & E_1(K) & \xrightarrow{[q^r]} & E_r(K) \\
R & \mapsto & R' \leftarrow nR & \mapsto & R'' \leftarrow q^r R' \\
\\
& \xrightarrow{\lambda} & \widehat{E}(M^r) & \xrightarrow{\log_E} & \widehat{G}_a(M^r) \\
& \mapsto & z_{R''} \leftarrow -\frac{x(R'')}{y(R'')} & \mapsto & \log_E(z_{R''})
\end{array}$$

Algorithm. So given points $S, T \in E(K)$ with $T \in \langle S \rangle$, $[n]S \neq O$ and $[q^r]S \neq O$, we compute

1. $s' \leftarrow (\log_E \circ \lambda \circ [q^r] \circ [n])(S)$
2. $t' \leftarrow (\log_E \circ \lambda \circ [q^r] \circ [n])(T)$
3. $u' \leftarrow t'/s'$

- The algorithm will solve the above problem provided $S \notin E(K)[n], S \notin E(K)[q^r]$.
- There is a trade-off between the π -adic precision and the number of terms of the logarithm map.
- Observe that we multiply a point in $E(K)$ by n to move it to $E_1(K)$ and then by q^r to push it into $E_r(K)$. In case the point is already in $E_1(K)$ then we'll need fewer transformations (in fact none if the point is in $E_s(K)$ where $s \geq r$).
- DLP on the torsion subgroup is an interesting one.

Example DLP over $E(\mathbb{Q}_p)$.

$$p = 36877.$$

$$E : y^2 = x^3 + ax + b \text{ where } a = 15190, b = 5862 \in \mathbb{Q}_p$$

$$\#\overline{E}(\mathbb{F}_p) = 36682.$$

$$S = [30673 + O(36877^{10}), 25638 + 11357 * 36877 + 32020 * 36877^2 + 1686 * 36877^3 + 26623 * 36877^4 + 35328 * 36877^5 + 23493 * 36877^6 + 4970 * 36877^7 + 15941 * 36877^8 + 26470 * 36877^9 + O(36877^{10})]$$

$$T = [2076 + 7557 * 36877 + 11588 * 36877^2 + 4309 * 36877^3 + 23926 * 36877^4 + 36834 * 36877^5 + 23270 * 36877^6 + 15761 * 36877^7 + 2252 * 36877^8 + 18487 * 36877^9 + O(36877^{10}), 18844 + 1498 * 36877 + 5454 * 36877^2 + 8729 * 36877^3 + 5065 * 36877^4 + 32634 * 36877^5 + 7765 * 36877^6 + 12696 * 36877^7 + 14654 * 36877^8 + 1091 * 36877^9 + O(36877^{10})]$$

$$m = 9804 + 25033 * p + 24032 * p^2 + 5917 * p^3 + 29272 * p^4 + 18260 * p^5 = 1245367616390581101158191006$$

Algorithm: $m = 9804 + 25033 * 36877 + 24032 * 36877^2 + 5917 * 36877^3 + 29272 * 36877^4 + 18260 * 36877^5 + 34092 * 36877^6 + 788 * 36877^7 + 21855 * 36877^8 + O(36877^9)$

DLP over $E(\mathbf{F}_q)$

Definition (Discrete logarithm problem over $E(\mathbf{F}_q)$) Given points $\bar{S}, \bar{T} \in \bar{E}(\mathbf{F}_q)$ with $\bar{T} \in \langle \bar{S} \rangle$ to compute $u \in \mathbf{Z}_{>1}$ such that $\bar{T} = u\bar{S}$.

Let \bar{E} be an elliptic curve over \mathbf{F}_q defined by the equation

$$y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

where $a_i \in \mathbf{F}_q$.

↓ lift

Let E denote the elliptic curve over K a finite extension of \mathbf{Q}_p obtained by lifting the coefficients of \bar{E} to K and defined by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

where $a_i \in R, \bar{a}_i = a_i \bmod \pi$.

The \mathbf{F}_q rational points of E are lifted to $E(K)$

Let $n = \#\overline{E}(\mathbf{F}_q)$ denote the order of the group of \mathbf{F}_q rational points on \overline{E} .

$$\begin{array}{ccc} S & T & \in E(K) \\ \uparrow & \uparrow & \uparrow \\ \overline{S} & \overline{T} & \in \overline{E}(\mathbf{F}_q) \end{array}$$

The diagram below illustrates our algorithm.

$$\begin{array}{ccccccc} E(\mathbf{F}_q) & \xrightarrow{\text{lift}} & E(K) & \xrightarrow{[n]} & E_1(K) & \xrightarrow{[q^r]} & \\ \overline{R} & \mapsto & R & \mapsto & R' \leftarrow nR & \mapsto & \\ \\ E_r(K) & \xrightarrow{\lambda} & \widehat{E}(M^r) & \xrightarrow{\log_E} & \widehat{G}_a(M^r) & & \\ R'' \leftarrow q^r R' & \mapsto & z_{R''} \leftarrow -\frac{x(R'')}{y(R'')} & \mapsto & \log_E(z_{R''}) & & \end{array}$$

Algorithm. Given points $\overline{S}, \overline{T} \in \overline{E}(\mathbf{F}_q)$ with $\overline{T} \in \langle \overline{S} \rangle$, $nS \neq O$ and $q^r S \neq O$, we compute

1. Lift $\overline{S}, \overline{T}$ to $S, T \in E(K)$
2. $s' \leftarrow (\log_E \circ \lambda \circ [q^r] \circ [n])(S)$

$$3. t' \leftarrow (\log_E \circ \lambda \circ [q^r] \circ [n])(T)$$

$$4. u' \leftarrow t'/s'$$

Proof of Correctness. Theorem. (The Extended Snake Lemma) Every commutative diagram of abelian groups

$$\begin{array}{ccccccccc} & & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \rightarrow & 0 \\ & & \downarrow \alpha & & \downarrow \beta & & \downarrow \gamma & & \\ 0 & \rightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' & & \end{array}$$

with exact rows gives rise to an exact sequence

$$\begin{array}{l} 0 \rightarrow \ker f \rightarrow \ker \alpha \rightarrow \ker \beta \rightarrow \ker \gamma \\ \xrightarrow{\phi} \text{coker} \alpha \rightarrow \text{coker} \beta \rightarrow \text{coker} \gamma \rightarrow \text{coker} g' \rightarrow 0 \end{array}$$

This algorithm is essentially computing the **connecting homomorphism** of the snake lemma

$$\begin{array}{ccc} \phi : \overline{E}(k) & \rightarrow & E_1(K)/nE_1(K) \\ \overline{P} & \mapsto & Q + nE_1(K) \end{array}$$

where $g(P) = \bar{P}$ where g is the reduction map and $nP = Q \in E_1(K)$.

$$0 \rightarrow E_1(K) \rightarrow E(K) \rightarrow \bar{E}(k) \rightarrow 0$$

$\alpha = \beta = \gamma = [l] = \times$ by l map, $l \in \mathbf{Z}$

$$\begin{array}{ccccccc} E_1(K) & \xrightarrow{f} & E(K) & \xrightarrow{g} & \bar{E}(k) & \rightarrow & 0 \\ \downarrow [l] & & \downarrow [l] & & \downarrow [l] & & \\ 0 \rightarrow E_1(K) & \xrightarrow{f'} & E(K) & \xrightarrow{g'} & \bar{E}(k) & & \end{array}$$

Snake lemma

$$E_1(K) \cong \hat{E}(M)$$

$$l = |\bar{E}(k)| = n$$

$\pi = p$ ($K =$ unramified extension) and $p \neq 2$

$$\hat{E}(M) \cong \hat{G}_a(M) = M$$

\Downarrow
 \Downarrow
 \Downarrow
 \Downarrow
 \Downarrow

$$0 \rightarrow 0 \rightarrow 0 \rightarrow E(K)[n] \rightarrow \bar{E}(k)$$

$$\xrightarrow{\phi} M/nM \rightarrow E(K)/nE(K) \rightarrow \bar{E}(k) \rightarrow 0 \rightarrow 0$$

case i. $n = p^i \Rightarrow M/p^i M = R/p^i R \Downarrow$

$$0 \rightarrow 0 \rightarrow 0 \rightarrow E(K)[p^i] \rightarrow \bar{E}(k)$$

$$\xrightarrow{\phi} M/p^i M \rightarrow E(K)/p^i E(K) \rightarrow \bar{E}(k) \rightarrow 0 \rightarrow 0$$

When the latter happens we just try again.
 This is the **Anomalous aka Trace 1 case**).

case ii. $\gcd(n, p) = 1 \Rightarrow n \notin M \quad M/nM = 0 \quad \Downarrow$

$$\begin{array}{ccccccc}
 0 & \rightarrow & 0 & \rightarrow & 0 & \rightarrow & E(K)[n] \rightarrow \overline{E}(k) \\
 \underbrace{\phi}_{\rightarrow} & & 0 & \rightarrow & E(K)/nE(K) & \rightarrow & \overline{E}(k) \rightarrow 0 \rightarrow 0
 \end{array}$$

F-gp part has disappeared! Here connecting homomorphism ϕ is the 0-map!

case iii. $n = p^i s, \gcd(s, p) = 1, i \geq 0.$

Can be divided into case *i* and *ii*.

Example: DLP over $E(\mathbf{F}_p)$

$$p = 15737.$$

$$\overline{E} : y^2 = x^3 + \overline{a}x + \overline{b} \text{ where } \overline{a} = 9506 \bmod p, \overline{b} = 6137 \bmod p \\ p \in \mathbf{F}_p$$

$$\#\overline{E}(\mathbf{F}_p) = 15737$$

$$\overline{S} = [4802 \bmod p, 5670 \bmod p] \in \overline{E}(\mathbf{F}_p)$$

$$\overline{T} = [3147 \bmod p, 1336 \bmod p] \in \overline{E}(\mathbf{F}_p)$$

Given $T = [m]S$ to compute $\mathbf{m}(= 9300)$

$$K = \mathbf{Q}_p$$

$$E : y^2 = x^3 + ax + b \text{ where } a = 9506, b = 6137 \in \mathbf{Q}_p$$

$$S = [4802 + O(15737^{10}), 5670 + 6209 * 15737 + 6181 * 15737^2 + 11030 * 15737^3 + 9879 * 15737^4 + 7477 * 15737^5 + 13345 * 15737^6 + 7098 * 15737^7 + 10884 * 15737^8 + 4131 * 15737^9 + O(15737^{10})] \in E(\mathbf{Q}_p)$$

$$T = [3147 + O(15737^{10}), 1336 + 8363 * 15737 + 7083 * 15737^2 + 8484 * 15737^3 + 5161 * 15737^4 + 10488 * 15737^5 + 12052 * 15737^6 + 12094 * 15737^7 + 9242 * 15737^8 + 6886 * 15737^9 + O(15737^{10})] \in E(\mathbf{Q}_p)$$

$$\mathbf{Algorithm} : \mathbf{m} = 9300 + 7322 * 15737 + 765 * 15737^2 + 13317 * 15737^3 + 2180 * 15737^4 + 9271 * 15737^5 + 9946 * 15737^6 + 4386 * 15737^7 + O(15737^8)$$

Semaev-Rück's algorithm

| | |
|---------------|---|
| X | a projective irreducible nonsingular curve / \mathbf{F}_q of genus $g \geq 1$ |
| $\Omega^1(X)$ | \mathbf{F}_q -vector space of holomorphic differentials on X |
| $Pic_0(X)_m$ | m -torsion part of the gp of divisor classes of deg 0 on X |

Theorem. The DL in $Pic_0(X)_{p^n}$ computed in $O(n^2 \log p)$ ops in \mathbf{F}_q

ϕ is an injective isomorphism.

$$\phi: \begin{array}{ccccc} Pic_0(X)_p & \rightarrow & \Omega^1(X) & \rightarrow & \mathbf{F}_q^{2g-1} \\ \overline{D} & \longmapsto & df/f & \longmapsto & (a_0, \dots, a_{2g-2}) \end{array}$$

where $p \cdot D = (f)$ and $\deg D = 0$.

Representing df/f locally at a \mathbf{F}_q -rational point P_0 : Let t be a local parameter at P_0 . $df/f = gdt$ where $g = \sum_{i=0}^{\infty} a_i t^i$.

Riemann-Roch $\Rightarrow df/f$ is uniquely determined by a_0, \dots, a_{2g-2} .

DLP on m -dim comm f-gp over R

K is a finite extension of \mathbb{Q}_p , R its ring of integers.

Definition (DLP on a m -dim comm f-gp over R) Given $S = (s_1, \dots, s_m)$, $T = (t_1, \dots, t_m) \in \hat{F}^m(M)$ and $T \in \langle S \rangle$ to compute $u \in \mathbb{Z}$ such that $T = [u]S$.

Algorithm So given points $S, T \in \hat{F}^m(M)$ with $T \in \langle S \rangle$, $[q^{mr}]S \neq O$, we compute

1. $S' \leftarrow (\log_{F_i} \circ [q^{mr}])(S)$
2. $T' \leftarrow (\log_{F_i} \circ [q^{mr}])(T)$
3. $u \leftarrow T'(S')^{-1}$

The way the multiplication by an integer map is defined (see above) tells us that we need only **one** of the power series of the logarithm map which is a m -tuple to compute u though we need the m -tuple of power series for repeated addition.

Conclusions

- When $\gcd(n, p) = 1$ then f-gp based attack fails. $E(K)[n] \cong \overline{E}(k) \cong E(K)/nE(K)$. What can be said about DLP on $E(K)[n]$?
- Elliptic curves with $n = p^i$ and small non- p part to be avoided. Group order should be divisible by a large prime different from p .
- Does Smart/Satoh-Araki's method extend to Rück's?
- If we can “efficiently” impose an additive structure on a group then DLP is easy.