

**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

November 7, 2003
Mathematics of Public-Key Cryptography
University of Illinois, Chicago

Outline

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

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

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

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

A weak instance: **Anomalous** case

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

Technique (Smart / Satoh-Araki): Case $q = p$.

p -adic elliptic logarithm ψ_p

$$\psi_p((x, y)) \equiv -\frac{x}{y} \pmod{p^2}$$

$$u \equiv \frac{\psi_p([p]Q)}{\psi_p([p]P)} \pmod{p}$$

Formal group (F-gp) laws

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

An n -dim **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

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

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 .

$$\begin{aligned} m : E \times E &\rightarrow E \\ (P, Q) &\longmapsto P \oplus Q \\ m^* : K[\hat{E}]_O &\rightarrow K[\hat{E}]_O \times K[\hat{E}]_O \end{aligned}$$

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

$$\begin{aligned} x &\rightarrow \frac{z}{w} \\ y &\rightarrow -\frac{1}{w} \end{aligned}$$

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 $P_1 \oplus P_2 = -P_3 = (z_3, w(z_3))$

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

Formal Group

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

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.

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

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

Formal Group 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 $F_E(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - (2a_3z_1^3z_2 - (a_1a_2 - 3a_3)z_1^2z_2^2 + 2a_3z_1z_2^3) + \dots$

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

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

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

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

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

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

Idea. Solving DLP on an additive f-gp is easy.

Logarithm map

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

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

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

$v(p) = e =$ 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

Let E be given by a minimal Weierstrass equation

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

where $a_i \in R$ and $v(\Delta) \geq 0$ 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 .

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

is called the **reduction map**.

We say E has **good** (or stable) reduction if \overline{E} is non singular which we'll **assume** from here on.

Theorem

$$0 \rightarrow \mathbf{E}_1(K) \rightarrow \mathbf{E}(K) \rightarrow \overline{\mathbf{E}}(k) \rightarrow 0$$

Notation.

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

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

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

Theorem.

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

and this isomorphism identifies for $i \geq 1$

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

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

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

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

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

We have

$$E(K)/E_1(K) \cong \overline{E}(\mathbb{F}_q)$$

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

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

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 $E(\mathbb{Q}_p)$.

$$p = 36877.$$

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

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

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

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

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

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 $\bar{S}, \bar{T} \in \bar{E}(\mathbf{F}_q)$ with $\bar{T} \in \langle \bar{S} \rangle$ to compute $u \in \mathbf{Z}_{>1}$ such that $\bar{T} = [u]\bar{S}$.

$$\bar{E}/\mathbf{F}_q : y^2 + \bar{a}_1xy + \bar{a}_3y = x^3 + \bar{a}_2x^2 + \bar{a}_4x + \bar{a}_6$$

↓ lift

$$E/K : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

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

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

The diagram below illustrates our algorithm.

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

Algorithm. Given $\overline{S}, \overline{T} \in \overline{E}(\mathbf{F}_q)$ 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.

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

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

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

Snake lemma

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

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

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

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

↓
↓
↓
↓
↓

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

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

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

$$\begin{array}{c} 0 \rightarrow E(K)[p^i] \rightarrow \overline{E}(k) \xrightarrow{\phi} M/p^i M \\ \rightarrow E(K)/p^i E(K) \rightarrow \overline{E}(k) \rightarrow 0 \end{array}$$

Anomalous aka Trace 1 case (when it fails we just try again)

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

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

F-gp part disappears. $\phi = 0!$

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

Can be divided into case i and $ii.$

case $n = p^i$ algorithm fails “sometimes”

$$T - [m]S = R \in E_i(K) \setminus E_{i+1}(K)$$

$$([p]T) - [m]([p]S) = ([p]R) \in E_{i+1}(K) \setminus E_{i+2}(K)$$

$$\frac{(\log \circ \lambda)([p]T)}{(\log \circ \lambda)([p]S)} - m = \frac{(\log \circ \lambda)([p]R)}{(\log \circ \lambda)([p]S)}$$

$$m' - m \in p^{i-j}R \setminus p^{i-j+1}R$$

(good) $j < i \Leftrightarrow m' \equiv m \pmod{p}$

(bad) $j = i \Leftrightarrow m' \not\equiv m \pmod{p}$

$$\begin{aligned} 0 \rightarrow E(K)[p^i] \rightarrow \overline{E}(k) \xrightarrow{\phi} M/p^i M \\ \rightarrow E(K)/p^i E(K) \rightarrow \overline{E}(k) \rightarrow 0 \end{aligned}$$

(good) $\#E(K)[p^i] = 0 \Rightarrow \phi$ injects

(bad) $\#E(K)[p^i] = p^i \Rightarrow \phi = 0$

Probability of failure?

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

$$p = 15737.$$

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

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

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

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

Given $T = [m]S$ to compute $m(= 9300)$

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

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

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

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

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

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.

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

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 $g = \sum_{i=0}^{\infty} a_i t^i$.

DLP on m -dim comm f-gp over R

Q-Theorem (Honda). If $F(X, Y)$ is an m -dimensional commutative formal group law over a \mathbf{Q} -algebra R , then there is a unique strict isomorphism $\alpha(X) : F(X, Y) \rightarrow G_a^m(X, Y)$.

K/\mathbf{Q}_p finite, 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 $u \in \mathbf{Z}$ 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. $u \leftarrow T'(S')^{-1}$

Formal Group of the Jacobian of an Algebraic Curve

Margaret Freije.

K a field of char 0

C a complete nonsingular algebraic curve of genus g over K

A Jacobian of C , which is a g -dim abelian variety over K

O the local ring of functions defined at the origin

\hat{O} the completion of O wrt its maximal ideal

$\hat{O} \cong K[[z_1, \dots, z_g]]$ where (z_1, \dots, z_g) is a system of parameters at the origin

$$\begin{aligned} m &: A \times A \rightarrow A \\ m^* &: \hat{O} \rightarrow \hat{O} \times \hat{O} \end{aligned}$$

$\hat{A}(X, Y) = (\hat{A}_1(X, Y), \dots, \hat{A}_g(X, Y))$ the formal group law of A

Construction:

P_0 a K -rational point on C , which is
not a Weierstrass point
 t a local parameter at P_0

$\{\eta_1, \dots, \eta_g\}$ a basis for the hol. diff of C s.t.

$$\eta_i \equiv (-t)^{i-1} dt \pmod{t^g dt}$$

$$l_i(t) := \int \eta_i \text{ s.t. } l_i(0) = 0$$

$$\begin{aligned} L_i(t_1, \dots, t_g) &:= l_i(t_1) + \dots + l_i(t_g) \\ &= \mathcal{L}_i(s_1(T), \dots, s_g(T)) \end{aligned}$$

$(s_1(T), \dots, s_g(T))$ set of local parameters at
the origin of A .

Theorem. $\mathcal{L}(X) = (\mathcal{L}_1(X), \dots, \mathcal{L}_g(X))$ is the
strict logarithm of the Jacobian of C , i.e.,

$$\hat{A}(X, Y) = \mathcal{L}^{-1}(\mathcal{L}(X) + \mathcal{L}(Y))$$

is the formal group law of the Jacobian of C
and $\mathcal{L}(X) \equiv X \pmod{\deg 2}$

Conclusions

- If $\gcd(n, p) = 1$ then f-gp based attack fails. What can be said about DLP on $E(K)[n]$? $E(K)[n] \cong \overline{E}(k) \cong E(K)/nE(K)$.
- (Smart/Satoh-Araki) 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.