Discrete Logarithm Systems and Arithmetic Geometry

Gerhard Frey
Institute for Experimental Mathematics
University of Essen
e-mail: frey@exp-math.uni-essen.de
1 Algebraic Realisation of Discrete Logarithm Systems

For PUBLIC KEY SYSTEMS one has to construct functions $f$ satisfying some "functional equations" and with the most important properties:

- The function $f$ can be evaluated rapidly at every element of $\mathbb{N}$ but
- for randomly chosen $y \in A$ the effort needed to compute $x \in \mathbb{N}$ with $f(x) = y$ is very large.

For this: Use Commutative Algebra, Number Theory and Algebraic Geometry.
1.1 DL-Systems

1.1.1 Exponential systems and key exchange

Given:
(Finite) \( A \subset \mathbb{N} \) with \( 1 \in A \).
Let
\[
e : \mathbb{N} \times A \to A
\]
satisfy the functional equation:

\[
e(n_1, e(n_2, 1)) = e(n_1 \cdot n_2, e(1, 1)).
\]

Enough for

**key exchange:** (basic version)
$M_1, M_2$ want to agree on a common secret key using a public channel.

i) $M_i$ chooses (as randomly as possible) a secret number $n_i$.

ii) $M_i$ sends $y_i := e(n_i, 1)$.

iii) $M_1$ computes $e(n_1, y_2)$, $M_2$ computes $e(n_2, y_1)$.

$M_1$ and $M_2$ share the common key

$$S = e(n_1 n_2, e(1, 1)).$$
The secrecy of $S$ depends (not only)\(^1\) on the secrecy of $n_i$ and so on the difficulty to compute $n_i$ from the knowledge of $y_i = e(n_i, 1)$.

**Definition:** Assume that $e(n, a)$ as function of the first variable behaves like a one way function. Then

$$(e : \mathbb{N} \times A \to A; e(1, 1))$$

is an **exponential system with base point** $e(1, 1)$.

---

\(^1\)we will come back to this in the third lecture
1.1.2 DL and signature

More “structure” for signatures of El-Gamal type:
For an associative function
\[ \oplus : A \times A \rightarrow A \]
define
\[ n \circ a \]
as the \( n - 1 \) fold application of \( \oplus \) to \( a \).
Define
\[ e : \mathbb{N} \times A \rightarrow A \]
as
\[ e(n, a) := n \circ a. \]
e satisfies
\[ e(n_1, e(n_2, a)) = e(n_1n_2, a) \]
and
\[ e(n_1, a) \oplus e(n_2, a) = e(n_1 + n_2, a). \]
Signature scheme:
M chooses randomly and secretly, his **private key** $x \in \mathbb{N}$ and publishes his **public key** $Y := e(x, 1)$.

To sign a message $m$, $M$ uses, in addition to the DL-system, a (publicly known) *hash function* $h$ from $A$ to $\mathbb{N}$.

**Signature 1** $M$ chooses a second random number $k$ and computes

$$s := h(m)x + h(e(k, 1))k.$$  

The signed message consists of

$$(m, e(k, 1), s)$$

To check the authenticity of $(M, m)$ one computes

$S = e(s, 1), P = e(h(m), Y)), H = e(h(e(k, 1)), e(k, 1))$.

and checks whether

$$S = P \oplus H.$$  

**Remark:**

It is obvious that the security of the signature depends on the quality of $e(., 1)$ as one-way function, but it is easily seen that this is not enough.
Definition
For given $a$ in $A$ and $b \in \{n \circ a, n \in \mathbb{N}\}$ the logarithm of $b$ with respect to $a$ is a number $\log_a(b) := n_b \in \mathbb{N}$ with $n_b \circ a = b$.

Let $C$ be a positive real number.

$$(\oplus : A \times A \rightarrow A, 1)$$

is a Discrete Logarithm System (DL-systems) of exponential security $C$ if for random elements $a, b \in A$ the computation of $\log_a(b)$ has (probabilistic) complexity $\geq e^{C \cdot \log(|A|)}$.

**AIM**
Construct DL-systems which are candidates for exponential security $1/2$ (why $C$ not larger? See below!).
1.2 Algebraic Realization of Discrete Logarithms:

Let \((G, \times)\) be a finite group.

**Definition 1.1** A *numeration* \((A, f)\) of \(G\) is a bijective map

\[
f : G \rightarrow A
\]

where \(A\) is a finite subset of \(\mathbb{N}\) containing 1.

A *presentation* of an abstract finite group \(G\) is an embedding of \(G\) into a group with numeration.

Assume that \((A, f)\) is a numeration of the finite group \(G\) and that \(g_0 \in G\) with \(f(g_0) = 1\) is given.
Define

\( \oplus : A \times A \rightarrow A \)

by

\[ a_1 \oplus a_2 := f(f^{-1}(a_1) \times f^{-1}(a_2)). \]

Then

\[ e(n, a) = f(n \circ f^{-1}(a)). \]

**Remark:**

We require that \( \oplus \) is rapidly computable *without* the knowledge of \( f^{-1} \) and the security and the efficiency of the DL-System based on \( \oplus \) will depend crucially on \( f \).

From now on we assume that we have a numeration \( f \) of \( G \) and identify \( G \) with its presentation given by \( f \).
The One-way property of $e$ leads to the **Challenge:**

Compute, for given elements $P$ and $Q$ in $G$ a number $k$ with

$$P = k \circ Q.$$ 

$k$ is called the (discrete) logarithm of $P$ with respect to $Q$.

One sees immediately (Chinese remainder theorem and $p$-adic expansion) that we have to assume that the group order of $G$ is a prime $p$. 
Efficiency and security:
Ideal situation:
Time or space needed (probabilistically) for the computation of the logarithm: polynomial in \( p \).

Time and space needed to write down the elements and the group law of \( G \) and execute a group composition: polynomial in \( \log(p) \).

Task:
Find methods to construct presentations of groups \( \mathbb{Z}/p\mathbb{Z} \) with \( p \) large enough which satisfy these conditions “rather good”.

12
1.3 Generic Systems

We use the algebraic structure “group”. This allows “generic” attacks.

**Shanks’ Baby-Step-Giant-Step Method**

(deterministic)

Take $P, Q \in G$.

Find $k$ with $Q = k \cdot P$.

Principle:

Looking up an element in an ordered set is inexpensive.

Baby step: For $i = 0, \ldots, S \leq \sqrt{p}$

compute

$$(i \cdot P, i).$$

Giant step:

Compute

$$Q - i \cdot S \cdot P$$
Compare the two lists. If
\[ i_0 \cdot P = Q - i_1 \cdot S \cdot P \]
then
\[ k = i_0 + i_1 \cdot S. \]

**Complexity:** \( O(\sqrt{p}) \)

**Disadvantage:**

- needs \( O(\sqrt{p}) \) space
Pollard’s \( \rho \)-Algorithm (probabilistic)

Principle: Random walk in \( G \) closes with high probability after

\[
\approx 1.03 \sqrt{p}
\]

steps.

Controlled random walk (simplest version):

The result \( x_i \) of the \( i \)–th step should depend only on \( x_{i-1} \).

So partite \( G \) “randomly” into three sets \( T_j \) of size \( \approx p/3 \) and take

\[
\begin{align*}
   x_i &= P + x_{i-1} \text{ if } x_{i-1} \in T_1, \\
   x_i &= Q + x_{i-1} \text{ if } x_{i-1} \in T_2, \\
   x_i &= 2x_{i-1} \text{ if } x_{i-1} \in T_3.
\end{align*}
\]

Problem: how to detect a cycle?

E.g.: method due to Floyd
Variants: wild and tame kangaroos, herds of kangaroos, ... (van Orschoot-Wiener, Stein, Teske,...) **Advantages:** nearly no storage needed parallelisable.

Hence: For the complexity to compute discrete logarithms in finite groups the constant $C = 1/2$ is the best one can hope for. We try to do not worse.

**Remark:** Pollard’s method is used for the “world record” w.r.t. Certicom challenge:
Compute DL in an 108-bit elliptic curve.
1.4 Very special examples

Example 1:
\[ G := \mathbb{Z}/p \ . \]
Numeration:
\[ f : G \to \{1, \cdots, p\} \]
given by
\[ f(r + p\mathbb{Z}) := [r]_p \]
where \([r]_p\) is the smallest positive representative of the class of \(r\) modulo \(p\).
The function \(\oplus\) is given by
\[ r_1 \oplus r_2 = [r_1 + r_2]_p \]
which is easy to compute from the knowledge of \(r_i\).

Security?
Given: \(b\) with \(b = e(n, a) = [na]_p\).
Solve

$$b = na + kp$$

with $k \in \mathbb{Z}$.

The *Euclidean algorithm* solves this in $O(\log(p))$ operations in $\mathbb{Z}$:

We do not get a secure Discrete Logarithm System.
**Example 2:** \( G = \mathbb{Z}/p \). Choose a prime \( q \) such that \( p \) divides \( q - 1 \).
Choose \( \zeta \neq 1 \) in \( \mathbb{Z}/q \) with \( \zeta^p = 1 \) (i.e. \( \zeta \) is a primitive \( p \)-th root of unity).
Numeration: For \( 1 \leq i \leq p \) define
\[ z_i := [\zeta^i]_q \] and for \( \bar{i} = i + p\mathbb{Z} \in G \)
\[ f(\bar{i}) := [z_i - z_1 + 1]_q. \]
Addition:
\[ a_i = f(x_i + p\mathbb{Z}) \in \{1, cdots, q - 1\} \]
\[ a_1 \oplus a_2 = [\zeta^{x_1 + x_2}]_q - z_1 + 1]_q. \]
\[ = [(a_1 + z_1 - 1)(a_2 + z_1 - 1) - z_1 + 1]_q \]
\[ e(n, 1) = n \circ 1 = [z^n_1 - z_1 + 1]_q. \]
Security?
For fixed $a$ and random $b \in A$ find $n$ in $\mathbb{N}$ with
\[ b = e(n, a) = n \circ a = [a^n - z_1 + 1]q. \]
This means:
For one fixed $p$-th root of unity and one random $p$-th root of unity in the multiplicative group of $\mathbb{Z}/q$ one has to determine the exponent needed to transform the fixed root of unity into the random element.

The best known method to compute this discrete logarithm is “subexponential” in $q$ (cf. second lecture). It usually is compared with factorization. The suggested size of $p$ is at least 1024 (2048) bits.
1.5 Numeration by Algebraic Groups

We generalize and systematize the examples.
Numerations by algebraic groups over finite fields $\mathbb{F}_q$ where $q$ is a power of a prime $l_0$.
In this lecture we shall give the mathematical background.
In the next lecture we shall explain (down to earth) what can be done in practice.
1.5.1 Algebraic Groups

An algebraic group \( G \) over a field \( K \) is an algebraic reduced, non-singular, noetherian scheme with an addition law, i.e. there is a morphism (in the category of schemes)
\[
m : G \times G \rightarrow G,
\]
an inverse, i.e. a morphism
\[
i : G \rightarrow G,
\]
and a neutral element, i.e. a morphism
\[
e : \text{Spec}(K) \rightarrow G,
\]
satisfying the usual group laws:
\[
m \circ (id_G \times m) = m \circ (m \times id_G) \text{ (associativity)},
\]
\[
m \circ (e \times id_G) = pr_2
\]
where \( pr_2 \) is the projection of \( \text{Spec}(K) \times G \) to \( G \), and
\[
m \circ (i \times id_G) \circ \delta = j_e
\]
where \( \delta \) is the diagonal map from \( G \) to \( G \times G \) and \( j_e \) is the map which sends \( G \) to \( e(\text{Spec}(K)) \).

Down to earth:
For all extension fields \( L \) of \( K \) the set \( G(L) \) (see below) is a group in which the sum and the inverse of elements are computed by evaluating morphisms which are defined over \( K \) and in which the neutral element is the point
\[
0 := e(\text{Spec}(K)) \in G(K).
\]
**Affine parts**

$\mathcal{G}$ can be covered by finitely many affine subvarieties $U$ (open w.r.t. the Zariski topology:
Locally it is “given” by a system of equations of polynomials:
We can choose coordinate functions $X_1, \cdots, X_n$ satisfying the relations

$$F_1(X_1, \cdots, X_n = 0), \cdots,$$

$$F_m(X_1 \cdots, X_n) = 0$$

with $F_j \in K[X_1, \cdots, X_n]$ ($m_i = 0$ is allowed).

The coordinate functions generate an integral domain with quotient field $F(U)$. Its transcendence degree $d$ over $K$ is the dimension of $\mathcal{G}$.
For extension fields $L$ of $K$ let $\mathcal{G}(L)$ be the set of $L$-rational points of $\mathcal{G}$. In the affine part:

$$\mathcal{G}(L) \cap U =$$

$$= \{ x \in L^n, F_1(x) = \cdots = F_m(x) = 0 \}.$$ 

Addition (for $U$ “small enough”):

$$m_U : W \to V$$

$$(x_1, \cdots, x_n) \times (y_1, \cdots, y_n) \mapsto$$

$$(R_1(x_1, \cdots, x_n; y_1, \cdots, y_n), \cdots, R_n(x_1, \cdots, x_n; y_1, \cdots, y_n))$$

with $R_i \in K(X_1, \cdots, X_n, Y_1, \cdots, Y_n)$. For the performance of the cryptosystem the choice of $(W, m_W)$ is crucial; we require small $n$ and low degree of $R_i$. 

24
If we can take $U = G$ then $G$ is an affine group scheme.
The other important kind of group schemes are projective, i.e. they can be embedded into a projective space $\mathbb{P}^n / K$ and are closed in it.
They are called **abelian varieties**. Abelian varieties have many special properties which are not at all clear from the definition.
For instance their addition law has to be **commutative**.
1.5.2 One-dimensional examples

1. The **additive group** $G_a$ is the affine line. Take $X$ as coordinate function.
   \[ m: R(X, Y) = X + Y, \ i(X) = -X \]
   and $e(\text{Spec}(K)) = 0_K$.
   $G_a(L) = L^+$.  

2. For the **multiplicative group** $G_m$ we choose two variables $X_1, X_2$ and the relation $X_1X_2 - 1 = 0$.
   The “addition” $m$ is given by
   \[ (R_1(X_1, X_2; Y_1, Y_2) = X_1Y_1, \ R_2(X_1, X_2; Y_1, Y_2) = X_2Y_2), \]
   $i(X_1, X_2) = (X_2, X_1)$
   $e(\text{Spec}(K)) = (1_K, 1_K)$.
   $G_m(L) = L^*$.  

26
3. **Elliptic curves** $E$

They are the simplest examples for abelian varieties and at the same time, the most important ones in theory and applications today.
1.5.3 Birational Numeration

For “good” numerations of $\mathbb{Z}/p$ we want to use algebraic groups $G$ over finite fields $\mathbb{F}_q$.

Choose a numeration of $\mathbb{F}_q$ and hence of $\mathbb{F}_q^n$.

Choose coordinate functions for open affine $U$ of $G$ and take the induced numeration of $U(\mathbb{F}_q)$.

\[2\] If we want we can use a covering of $G$ by affine parts $U$ to get a numeration of $G(\mathbb{F}_q)$ but for most applications this will not be necessary.
Let
\[ \alpha : \mathbb{Z}/p \to \mathcal{G}(K) \]
be a non-trivial homomorphism. Then \( \alpha \) induces a numeration \( f \) of 
\( \mathbb{Z}/p \cap \alpha^{-1}(U(\mathbb{F}_q)) \) and 
\( \oplus_U =: \oplus \) is given by the rational functions defining the group law of \( \mathcal{G} \) on \( U \). The existence of \( \alpha \) is equivalent with the existence of \( \mathbb{F}_q \)-rational points \( P \) on \( \mathcal{G} \) with order \( p \), and one such \( \alpha \) can be explicitly given if one point \( P_0 \) of order \( p \) is known.
Classification:
Assume that $G$ as connected and commutative. Structure theorem:
Essentially we can use copies of $G_m$ and $G_a$ and abelian varieties for our purposes.

It is easily seen that $G_a$ leads to Example 1 and $G_m$ to Example 2 above.
1.6 Admissible Abelian Varieties

**Aim**

Construct explicitly abelian varieties $A$ satisfying simultaneously

1. A (large) prime $p$ divides $|A(\mathbb{F}_q)|$ and
   \[ \log p \approx \dim(A) \cdot \log q. \]

2. To store a point $P \in A(\mathbb{F}_q)$ one needs only $c_1(\log(p))$ bits of space and to compute $\oplus$ only $c_1(\dim(A)^k)$ operations in $\mathbb{F}_q$ with $c_1, c_2, k$ small (e.g. $c_1 = 1 + \epsilon, k = 2$).

3. All known algorithms for the computation of the discrete logarithm in $A(\mathbb{F}_q)$ have a large ($C = 1/2, p \approx 10^{60}$) exponential complexity.
The embedding of $\mathbb{Z}/p$ into $A(\mathbb{F}_q)$ induces a lot of additional structure: We can use

- Algebraic Number Theory, especially
  1. class field theory, CM-fields and cyclotomic fields
  2. local and global fields
- Algebraic Geometry
  1. function fields over finite fields, over global fields and over $\mathbb{C}$
  2. the theory of abelian varieties and, more generally, group schemes
- and, most importantly, **Galois theory**

for constructions, but also for (at least conceivable) attacks.
2 DL-systems and orders

2.1 Ideal class groups of orders

Remark:
Everything could be done much more general, and for some (few) theoretical and (even fewer) practical considerations this has to be done.

Let $O$ be a (commutative) ring with unit 1 without zero divisors.

Two ideals $A, B$ of $O$ different from 0 can be multiplied:

$$A \cdot B = \{ \Sigma a_i \cdot b_i; a_i \in A, b_i \in B \}.$$ 

Clearly $\cdot$ is associative.

---

$^3$A $\subset O$ is an ideal of $O$ if it is an $O$-module
So if we have a numeration \( f \) of ideals we can construct a map
\[
e(n, f(A)) := f(n \circ A)
\]
as above.

How to compute \( e(n, A) \)?
In general this will be not possible.
Here are some minimal assumptions:
I) \( O \) is \textbf{noetherian}: Every \( A \) is a finitely generated \( O \)-module. So choose a generating system \( \{a_1, \ldots, a_n\} \) for each \( A \).
Then a generating system of the product of two ideals can be computed in finitely many steps. But these systems become longer and longer.
II) $O$ can be embedded into a finitely generated algebra $\tilde{O}$ over an euclidean ring $B$ such that the transition

$$A \mapsto A \cdot \tilde{O}$$

preserves “enough” information. Then ideals $A$ have a base over $B$ (as $\tilde{O}$-modules), and by linear algebra over $B$ one can compute a base in products of ideals.

But there are infinitely many possible choices of bases. So assume

III) There is a rather canonical way to choose a basis for each ideal and $B$ has a numeration. Then one can numerate ideals in $O$. 

35
Severe **disadvantages:**
The system is much too large.
It is insecure.
We have infinite sets.
(We have no group structure.)

**Advantage and disadvantage:**
We are near to the arithmetic of $\mathcal{B}$ and we can compute with ideals if we can compute in $\mathcal{B}$. 
Abstract Algebraic Geometry resp. Commutative Algebra tells us: There are more reasonable objects than ideals (= rank-1-projective modules) over $O$:

**Isomorphy classes of projective rank-1-modules**

or, in fancy language,

$\text{Pic}(O)$

and factor- resp. subgroups.
**Definition:**
Let $A_1, A_1$ be two $O$–modules in $Quot(O)$.
$A_1 \sim A_2$ if there is an element $f \in Quot(O)^*$ with
\[ A_1 = f \cdot A_2. \]

Let $A$ be an ideal of $O$:
$A$ is invertible iff there is an ideal $\tilde{A}$ of $O$ such that
\[ A \cdot \tilde{A} \sim O. \]

$Pic(0)$ is the set of equivalence classes of invertible ideals of $O$, it is an abelian group.
Try $Pic(O)$ as groups into which $\mathbb{Z}/p$ is to be embedded.

Immediate problem: The equivalence classes contain infinitely many ideals. How to describe the elements in $Pic(O)$ for the computer?

Two possibilities:

1. Find a distinguished element in each class (resp. a finite (small) subset of such elements).

2. Find “coordinates” and addition formulas directly for elements of $Pic(O)$.

We need (cf. definition of admissible abelian varieties):
I) There has to be a very fast algorithm to find these distinguished elements. Possible if

- we have “reduction algorithms”, or

- we can use the geometric background of $\text{Pic}(O)$ which leads to **group schemes** resp. **abelian varieties** (link to the first lecture).

Most interesting cases are those for which both methods can be used!
II) We want to embed $\mathbb{Z}/p$ into $Pic(O)$ in a bit-efficient way:
We need

- a fast method for the computation of the order of $Pic(O)$
- (at least) a heuristic that with reasonable probability this order is almost a prime.

III) Discuss and, above all, exclude attacks.
"Generic attack" for DL-systems based on $\text{Pic}(O)$:

We have distinguished ideals: Prime ideals.

We have the arithmetic structure of $\mathcal{B}$.

Since we have to be able to define reduced elements (i.e. ideals) in classes we have in all known cases a “size” of classes which behaves reasonable with respect to addition.
This cries for ...
Index-Calculus.

Principle:
We work in a group $G$.
Find a “factor base” consisting of relatively few elements and compute $G$ as a $\mathbb{Z}$–module given by the free abelian group generated by the base elements modulo relations.
Prove that with reasonable high probability every element of $G$ can be written (fast and explicitly) as a sum of elements in the factor base.
The important task in this method is to balance the number of elements in the factor base to make the linear algebra over \( \mathbb{Z} \) manageable and to “guarantee” smoothness of enough elements with respect to this base.

The expected complexity of this attack is **subexponential**, i.e estimated by

\[
L_N(\alpha, c) := \exp(c \log N)^\alpha (\log \log N)^{1-\alpha}
\]

mit \( 0 < \alpha < 1 \) und \( c > 0 \) for a number \( N \) closely related to \( |G| \).
2.2 Existing Systems

What is used today?
Only two examples:

- \( \mathcal{B} = \mathbb{Z} \), and \( O \) is an order or a localization of an order in a number field
- \( \mathcal{B} = \mathbb{F}_p[X] \), and \( O \) is the ring of holomorphic functions of a curve defined over a finite extension field of \( \mathbb{F}_p \).
2.2.1 Number field case

Orders \( O \) in number fields were proposed very early in the history of public key cryptography (Buchmann-Williams 1988). We restrict ourselves to maximal orders (i.e. the integral closure) \( O_K \) of \( \mathbb{Z} \) in number fields \( K \).

\( O_K \) is a Dedekind domain, its class group \( Pic(O_K) \) is finite. The size of ideals is given by their norm.

The **Theorem of Minkowski** states that in every ideal class there are ideals of “small” norm. The measure is given by

\[
g_K := 1/2 \log | \Delta_K |
\]

(\( \Delta_K \) the discriminant of \( O_K/\mathbb{Z} \)).
The background is the “Geometry of numbers” (Minkowski). By lattice techniques it is possible to compute ideals of small norms in classes, and in these ideals one finds “small” bases.

Most difficult part: To compute the order of $\text{Pic}(O_K)$: Uses analytic methods (L-series) in connection with most powerful tools from computational number theory.

There is a (probabilistic) estimate: The order of $\text{Pic}(O_K)$ behaves like $\exp(g_K)$. 
**Disadvantage:** For given $g$ there are not many fields, and to have $Pic(O_K)$ large the genus of $K$ has to be large.

The parameter “genus” can be splitted into two components:

$n := [K : \mathbb{Q}]$ and ramification locus of $K/\mathbb{Q}$.

If $n$ is large the arithmetic in $O_K$ is complicated (fundamental units, lattice dimension ...)**
Most practical example:
$K$ is an imaginary quadratic field of discriminant $-D^4$.
So $K = \mathbb{Q}(\sqrt{-D})$. The expected size of $Pic(O)$ is $\approx \sqrt{D}$.

**Theory of Gauß:**
$Pic(O_K)$ corresponds to classes of binary quadratic forms with discriminant $D$.

Multiplication of ideals corresponds to composition of quadratic forms.

\footnote{The real case, as well as its counterpart in geometry, is very interesting, too. Key word: Infrastructure(Shanks, ...)}
Reduction of ideals corresponds to the (unique) reduction of quadratic forms:
In each class we find (by using Euclid’s algorithm) a uniquely determined reduced quadratic form

\[ aX^2 + 2bXY + cY^2 \]

with \( ac-b^2 = D, -a/1 < b \leq a/2, a \leq c \) and \( 0 \leq b \leq a/2 \) if \( a = c \).

The great disadvantage:
The index-calculus-attack works very efficiently:
(Under GRH:) The complexity to compute the DL in \( Pic(O_K) \) is

\[ O(L_D(1/2, \sqrt{2} + o(1))). \]
2.3 The geometric case

$\mathcal{B} = \mathbb{F}_p[X]$, and $O$ is the ring of holomorphic functions of a curve defined over a finite extension field $\mathbb{F}_q$ of $\mathbb{F}_p$. Intrinsically behind this situation is a regular projective absolutely irreducible curve $C$ defined over $\mathbb{F}_q$ whose field of meromorphic functions $F(C)$ is given by $\text{Quot}(O)$.

$C$ is the desingularisation of the projective closure of the curve corresponding to $O$.
This relates $\text{Pic}(O)$ closely with the points of the Jacobian variety $J_C$ of $C$ and explains the role of abelian varieties in crypto systems used today.
Singularities
Short remark to non-integral closed $O$:
It corresponds to a singular curve $C'$. The generalized Jacobian variety of $C'$ is an extension of $J_C$ by linear groups. In this way we can realize DL-systems based on tori, especially on the multiplicative group (“classical” DL).

Example:
$\text{Pic}(\mathbb{F}_q[X, Y]/(Y^2 + XY - X^3))$
$= \mathbb{F}_q^*$
and (for a non-square $d$)

$\text{Pic}(\mathbb{F}_q[X, Y]/(Y^2 + dXY - X^3))$

corresponds to the rational points of a non-split one-dimensional torus. Its points have order dividing $q + 1$. 

52
Now points of the multiplicative group $G_m$ defined over finite fields (e.g. $\mathbb{Z}/p$) can be easily lifted to points of $G_m$ over number fields (e.g. use the map $\mathbb{Z} \to \mathbb{Z}/p$).

Hence we can use the arithmetic of $\mathbb{Z}$ to start a subexponential attack by Index-Calculus methods.

V. Miller and N. Koblitz proposed (independently):
Avoid this attack by using higher genus curves.
Key-word: Néron-Tate-height  So ...

53
... assume that $O$ is integrally closed. The corresponding curve $C_O$ is an affine part of $C$.

The inclusion

$$\mathbb{F}_q[X] \to O$$

corresponds to a morphism

$$C_O \to \mathbb{A}^1$$

which extends to a map

$$\pi : C \to \mathbb{P}^1.$$ 

Let $P$ be a point on $C_O$ and $M_P = \{f \in O, f(P) = 0\}$. $M_P$ is a prime ideal in $O$ and the map $P \mapsto M_P$ gives a one-to-one correspondence between Galois orbits of points (over $\overline{\mathbb{F}}_q$) of $C_O$ and maximal ideals of $O$. 

54
If $P$ is a point in $C \setminus C_O$ then $P \in \pi^{-1}(\infty)$ where $\infty := \mathbb{P}^1 \setminus \mathbb{A}^1$.

We shall assume that there is an $\mathbb{F}_q$–rational point $P_{\infty}$ in $\pi^{-1}(\infty)$.

There is a canonical map

$\phi : J_C(\mathbb{F}_q) \to Pic(O)$

which is surjective but not always injective:

Its kernel is generated by divisors of degree 0 with support in the missing set of points $\pi^{-1}(\infty)$. 
More precise: $\mathbb{F}_q$—rational divisors of $C$ are formal sums of points (over $\mathbb{F}_q$) of $C$ which are Galois invariant.

Two divisors are in the same class iff their difference consists of the zeroes and poles (with multiplicity) of a function on $C$.

The points of $J_C$ are the divisor classes of degree 0 of $C$.

The theorem of Riemann-Roch implies that

$$(C \times \ldots \times C)/S_g \quad (g = \text{genus}(C),$$

$S_g$ the symmetric group in $g$ letters)
is birationally isomorphic to $J_C$: 

56
We find a representative $D$ in divisor classes $c$ of the form

$D - g P_\infty$ with $D = \Sigma_{i=1,\ldots,g} a_i P_i$ with $a_i \geq 0$. Now map

$c \mapsto [\prod_{P_i \in C_O} M_{P_i}^{a_i}]$.

Most interesting case: The kernel of $\phi$ is trivial or uninteresting. If so:

We can use the ideal interpretation for computations and the abelian varieties for the structural background.
Especially:

- Addition is done by ideal multiplication

- Reduction is done by Riemann-Roch theorem (replacing Minkowski’s theorem in number field) on curves

but the computation of the order of $Pic(O)$ and the construction of suitable orders is done by using properties of abelian varieties resp. Jacobians of curves.

The key field invariant is again the genus $g_C$. 
Compared with the number theory case we have won a lot of freedom: The parameters are:

1. $p =$ characteristic of the base field
2. $n =$ degree of the ground field of $\mathbb{Z}/p$
3. $g_C = g =$ the genus of the curve $C$ resp. the function field $Quot(O)$.

There are about $p^{3g \cdot n}$ curves of genus $g$ over $\mathbb{F}_{p^n}$.

**Structural relation: Hasse-Weil**

$$| J_C(\mathbb{F}_{p^n}) | = p^{ng} + O(p^{ng/2}).$$

The **key length** is $n \log(p) \cdot g$. 

59
Example
Assume that there is a cover
\[ \varphi : C \to \mathbb{P}^1; \deg \varphi = d, \]
in which a non singular point \( (P_\infty) \) is
totally ramified and induces the place
\((X = \infty)\) in the function field \( \mathbb{F}_q(X) \)
of \( \mathbb{P}^1 \).

Let \( O \) be the normal closure of \( \mathbb{F}_q[X] \)
in the function field of \( C \).
Then \( \phi \) is an isomorphismus.
Examples for curves having such covers
are all curves with a rational Weierstraß
point, especially \( C_{ab} \)-curves and most
prominently hyperelliptic curves in-
cluding elliptic curves.
2.3.1 Hyperelliptic curves

Definition\textsuperscript{5}
Assume that $C$ is a projective irreducible non singular curve of genus $\geq 1$ with a generically etale morphism $\phi$ of degree 2 to $\mathbb{P}^1$.
Then $C$ is a hyperelliptic curve.
In terms of function fields this means:
The function field $F(C)$ of $C$ is a separable extension of degree 2 of the rational function field $\mathbb{F}_q(X)$. Let $\omega$ denote the non trivial automorphism of this extension. It induces an involution $\omega$ on $C$ with quotient $\mathbb{P}^1$.
The fixed points of $\omega$ are called Weierstraß points.

\textsuperscript{5}Elliptic curves ($g = 1$) are included.
Assume that we have a $\mathbb{F}_q$-rational Weierstraß point $P_\infty$.\footnote{If not we are led to the very interesting theory of real hyperelliptic curves} We choose $\infty$ on $\mathbb{P}^1$ as $\phi(P_\infty)$. Then the ring of holomorphic functions $O$ on $C \setminus P_\infty$ is equal to the integral closure of $\mathbb{F}_q[X]$ in $F(C)$:

$$O = \mathbb{F}_q[X, Y]/f_C(X, Y)$$

where $f_C(X, Y)$ is a polynomial of degree 2 in $Y$ and of degree $2g + 1$ in $X$.

**Theorem:** $J_C(\mathbb{F}_q) = Pic(O)$. 

62
From the algebraic point of view we are in a very similar situation as in the case of class groups of imaginary quadratic fields. In fact: Artin has generalized Gauß’s theory of ideal classes of imaginary quadratic number fields to hyperelliptic function fields connecting ideal classes of $O$ with reduced quadratic forms of discriminant $D(f)$ and the addition $\oplus$ with the composition of such forms. This is the basis for the Cantor algorithm which can be written down “formally” and then leads to addition formulas or can be implemented as algorithm.
For $g = 1$: Addition formulas for elliptic curves
For $g = 2$: Formulas (Spallek-Krieger) as good as algorithm.
For $g \leq 3$: Use algorithm.

**Complexity:** $O(g^2)$.

(So $g = 1$ is best, optimizations? Special computer architecture?)
Negative aspect
As in the analogous situation in number theory there exists a subexponential attack based on the index-calculus principle.
But there is one essential difference: Recall: In the number field case the subexponential function was a function in $|D|$ and so of the order of the class group.
Due to Weil the analogue would be $q^g$. But in the known index-calculus algorithm one cannot look at $q$ and $g$ as independent variables.
For instance: If $g = 1$ fixed then we do not get a subexponential attack for $q \to \infty$.
The attack:
The ideal classes of $S$ can be represented by two polynomials of degrees bounded by $g$.
Choose as factor base for the index-calculus attack the ideal classes which can be represented by polynomials of small degrees.

Adleman, DeMarrais and Huang, Müller-Stein-Thiele, Enge-Stein:

For $g/ \log(q) > t$ the discrete logarithm in the divisor class group of a hyperelliptic curve of genus $g$ defined over $\mathbb{F}_q$ can be computed with complexity bounded by $L_{1/2,q^g} \left[ \frac{5}{\sqrt{6}} \left( (1 + \frac{3}{2t})^{1/2} + (\frac{3}{2t})^{1/2} \right) \right]$.
This is for large genus a strong result.
Gaudry has a result much more serious for practical use: For hyperelliptic curves of relatively small genus (in practice: \( g \leq 9 \)) there is an index-calculus attack of complexity

\[ O(q^2(\log(q))^\gamma) \]

with “reasonable small” constants.

“Result”: Orders related to curves with rational Weierstraß points of genus \( \geq 4 \) or closely related abelian varieties should be avoided!

State of the art: We have only three types of rings \( O \) which avoid serious index-calculus attacks and for which \( Pic(O) \) in manageable:

MAXIMAL ORDERS BELONGING TO CURVES OF GENUS 1,2,3!
3 Galois Theory

Let $K$ be a field, $\bar{K}$ its separable closure.
The absolute Galois group of $K$ is
\[
G_K := \text{Aut}(\bar{K}/K).
\]
$G_K$ is a pro-finite group, it is compact w.r.t. the Krull topology.

In our context we have a hierarchy of 3 types of fields with corresponding Galois groups:
• Global fields $K$, e.g. number fields like $\mathbb{Q}$,
• local fields $K_\nu$, i.e. completions of global fields w.r.t. a valuation $\nu$ of $K_s$, like $\mathbb{Q}_p$,
• finite fields $\mathbb{F}_q$ as residue fields of local fields.

We have

$$G_K \supset G_{K_\nu} = \{ \sigma \in G_K; \sigma(\nu) = \nu \}$$

and $G_{\mathbb{F}_q}$ can be identified in a natural way with a factor group of $G_{K_\nu}$ which is the Galois group of the maximal unramified extension of $K_\nu$.

The action of these Galois groups on torsion points of abelian varieties provides the whole arithmetical information about the varieties.
3.1 Counting points

3.1.1 L-series

\( G_{\mathbb{F}_q} \) is generated as topological group by the Frobenius automorphism \( \pi_q \) which maps each element to its \( q - th \) power.

Let \( A \) be an abelian variety defined over \( \mathbb{F}_q \).

For all numbers \( n \) \( \pi_q \) acts on the points \( A(\overline{\mathbb{F}_q})[n] \), the group of elements of \( A(\overline{\mathbb{F}_q}) \) whose order divides \( n \). Hence it induces a linear map on \( A(\overline{\mathbb{F}_q})[n] \) which is, if \( n \) is prime to \( \text{char}(K) \), as \( \mathbb{Z}/n \)-module isomorphic to \( (\mathbb{Z}/n)^{2d} \).
**Fact (Weil):**
The characteristic polynomial of $\pi_q$ w.r.t. this action is the reduction modulo $n$ of a monic polynomial with integer coefficients of degree $2d$. This polynomial is independent of $n$ and is called the **L-series** $L_A(T)$ of $A$ over $\mathbb{F}_q$. 
Since $A(\mathbb{F}_q)$ is the kernel of the map $\pi_q - id$ we get by elementary linear algebra:

$$|A(\mathbb{F}_q)| = |L_A(1)|.$$ 

A trivial but crucial consequence is: $\mathbb{Z}/p$ is embeddable into $A(\mathbb{F}_q)$ iff $L_A(1) \equiv 0 \mod p$.

A fundamental theorem of Weil states that the absolute value of the zeroes of $L_A(T)$ is equal to $\sqrt{q}$ and so we get the result mentioned above:

$$\dim A \cdot \log q \approx \log |A(\mathbb{F}_q)|.$$
So to construct candidates for DL-systems we look for abelian varieties $A$ for which we can

1. compute $L_A(1)$ rapidly, and
2. prove that with a not too small probability a prime of size $\approx q^d$ divides $L_A(1)$.

The second item can be discussed by **global Galois theory** using analytic and algebraic number theory. These theories provide tools like effective versions of Chebotarev’s density theorem and conjectures about the distribution of traces of Frobenius elements (Lang-Trotter) and about the distribution of class groups generalizing heuristics of Cohen-Lenstra.\footnote{cf. lectures of K. Murty}
3.1.2 Constant Field Extensions

Begin with a small field $\mathbb{F}_{q_0}$ and $A$ defined over this field and determine (e.g. by counting or index-calculus) the zeroes $\omega_i$ of the L-series of $A$ over $\mathbb{F}_{q_0}$.

For $m \in \mathbb{N}$ and $q = q_0^m$ the Frobenius automorphism $\pi_q$ is the $m$-th power of $\pi_{q_0}$.

Hence the zeroes of the $L$-series of $A \times \mathbb{F}_q$ are the $m$-th powers of $\omega_i$ and so the order of $A(\mathbb{F}_q)$ can be computed easily.

The method of constant field extensions is used only for very small $q_0$ and large prime $m$. The typical examples are Koblitz curves\footnote{There are obvious generalizations, cf. lecture of T. Lange} defined over fields with 2-power order.
3.1.3 **Schoof’s Algorithm:**

Remember: \( L_A(T) \) is a polynomial with integral coefficients which simultaneously for all natural numbers \( n \) is the characteristic polynomial of \( \pi_q \) acting on torsion points of order \( n \) of \( A \). Since it has integral coefficients (of size depending on \( q \) and \( \dim(A) \) only) it is determined by this action for small \( n \). How to do this for elliptic curves or curves of genus 2 cf. lectures of Morain. For curves of larger genus no practical algorithm is known.
3.1.4 Complex Multiplication

This is a global construction, i.e. one constructs an abelian variety $A$ over a number field such that one can compute the number of points of the reduction of $A$ modulo primes of this field.

1.) We use the arithmetic theory of the Galois groups of special number fields $K$ (called CM-fields) which are totally imaginary quadratic extensions of totally real number fields. Then Class field theory relates endomorphisms of special abelian varieties $A_K$ to elements in orders $\mathcal{O}_K$ in CM-fields $K$ (Shimura - Taniyama).
Examples:
1.) $g = 1$: Class field theory of imaginary fields applied to elliptic curves is used till today. It works very efficiently, the hardest computational problem is the factorization of polynomials of degree $\leq 1000$ over $\mathbb{F}_q$.

2.) $g = 2$: This is implemented by A.Weng (Preprint IEM Essen 2000) in a very efficient way and uses

1. class field theory of fields of degree 2 over real quadratic fields (non-Galois over $\mathbb{Q}$), \(^9\)

2. Invariant theory which is explicit and “easy” and

3. Mestre’s method intersecting invariant forms

\(^9\)to avoid non-necessary automorphisms
Example (Weng (2000)): (g=2) Consider the CM-field

\[ K = \mathbb{Q}(\alpha) = \mathbb{Q}\left( i \sqrt{7 + 2 \frac{-1 + \sqrt{33}}{2}} \right). \]

It has class number two and two polarizations. The class polynomials are given by

\[ H_1(X) = w^4 + 125426939904w^3 + 206483140868310761472w^2 \]
\[ -3777735852531193527889035264w \]
\[ + 4880287864430944225048694259449856, \]

\[ H_2(X) = w^4 + 660000960w^3 + 106952268616185600w^2 \]
\[ + 2725546614937533849600w \]
\[ + 837300145473346170101760000, \]

\[ H_3(X) = w^4 + 189766368w^3 + 7505309625975360w^2 \]
\[ + 434631556065843035136w - 45329807190376508829696. \]
Take \( p = 5900018603715467611181989109202421 \) satisfying \( p = w\overline{w} \) with
\[
w = (-76811578202943299 + 107438053\left(\frac{-1 + \sqrt{33}}{2}\right)) + (521777257258 + 990510120225\left(\frac{-1 + \sqrt{33}}{2}\right))\alpha.
\]

\( C : y^2 = t^5 + 2251831303237605767657618195346350t^4 + 1395987570926578077980910550381755t^3 + 3449986084090239803090552184527208t^2 + 107170423469627799375107316893595t + 2770857204236068378720416405312357. \)
The group order of \( J_C(\mathbb{F}_p) \) is given by
\[
34810219524188617853906269808542764315413963371023671004263947730632.
\]
\[
= 8 \cdot q_{prime} (67 \text{ digits}).
\]
3.) For $g \geq 3$ invariant theory becomes more complicated. It seems to be difficult to construct hyperelliptic curves with only 2 automorphisms. A. Weng is able to find curves with CM with 4 automorphisms.

**Example (g=3)**

We choose

$$p = 123456776543211236173$$

and consider the curve

$$C : y^2 = x^7 + 7x^5 + 14x^3 + 7x.$$  

We can show that $J_C$ over $\mathbb{Q}$ has complex multiplication by

$$K = \mathbb{Q}(i)K_0$$

where $K_0$ is generated by $w^3 - w^2 - 2w + 1$.  

80
We solve the absolute norm equation
\[ p^3 = N_{K/Q}(p). \]
The Pari-library gives us 14 different solutions. The right group order is
\[ n = 1881675801864379891114339535564538805274692594768590688211848 \]
\[ = 8l \] where \( l \) is a prime with 60 decimal digits.
This curve is resistant against the Tate-pairing\(^{10}\) since the order of \( p \) in \( \mathbb{F}_l \) is equal to
\[ 117604737616523743194646220972783675329668287173036918013240. \]

\(^{10}\)cf. last section
3.2 Scalar restriction

We want to discuss the parameter $n = [\mathbb{F}_q : \mathbb{Z}/p]$.

More generally we look at the situation that $q = l_0^f$ with $f \geq 2$.
$\pi l_0$ acts non-trivially on $\mathbb{F}_q$.
What geometric consequences this has for abelian varieties $A$ defined over $\mathbb{F}_q$?
3.2.1 Weil Restriction

Idea: An abelian variety of dimension $d$ over $\mathbb{F}_q$ corresponds to an abelian variety of dimension $f \cdot d$ over $\mathbb{F}_{q^f}$.

Mathematical procedure: Take a field $K$ and a finite separable field extension $L/K$. Let $V$ be a quasi-projective variety (i.e. $V$ can be embedded into a projective space) defined over $L$.

Then there is a quasi-projective variety $W_V$ defined over $K$ with $W_V(K) = V(L)$ and $W_V \times L \cong V^{[L:K]}$. 
Recipe:
Choose coordinate functions $X_1, \cdots, X_n$ of $V$ over $L$ and a basis $(u_1, \cdots, u_m)$ of $L/K$. Define the $n \cdot m$ variables $Y_{i,j}$ by

$$X_i = u_1 Y_{1,i} + \cdots + u_m Y_{m,i},$$

Plug these expressions into the relations defining $V$. Next express the coefficients of the resulting relations as linear combinations of the basis $(u_1, \cdots, u_m)$ and order these relations according to this basis to get the relations of the coordinate functions $Y_{1,1}, \cdots, Y_{m,n}$ of $W_V$ over $K$.

For quasi-projective varieties one has to choose an appropriate cover of $V$ by affine varieties, apply the descent recipe to them and then glue together the resulting affine varieties over $K$. 

84
**Facts:** If $V$ is a projective variety then $W_V$ is projective, and if $V$ is an abelian variety $A$ then $W_A$ gets the structure of an abelian variety over $K$ in a natural way: The addition law is the descent of the addition law of $A$. 
3.2.2 The Case of Finite Fields

Take $K = \mathbb{F}_q$ and $L = \mathbb{F}_{q^m}$ and let $A$ be an abelian variety of dimension $d$ defined over $\mathbb{F}_{q^m}$.

The Weil restriction $W_A$ is an abelian variety defined over $\mathbb{F}_q$ and its group of $\mathbb{F}_q$-rational points is in a natural way isomorphic to $A(\mathbb{F}_{q^m})$.

So the DL-problem on $A/\mathbb{F}_{q^m}$ is equivalent with the DL-problem on the $m \times d$—dimensional abelian variety $W_A$ over $\mathbb{F}_q$. But $W_A$ has more geometric structure: We find $\mathbb{F}_q$-rational subvarieties like curves and hypersurfaces on $W_A$ which are not on $A$. 
It seems that “in general” these subvarieties are rather complicated. For instance take an elliptic curve $E$. Then “in general” one expects that the minimal genus of curves on $W_E$ is $\approx 2^m$ and so at least till now we cannot apply this additional information (positively or negatively) to the DL-problem if $m$ is large. But for small $m$ or special fields $\mathbb{F}_q$ one has to expect a different picture.
For one such example cf. Morain’s lecture.

It deals with $l = 2$ and uses that the elliptic curve is not defined over the ground field.
Again by Galois theory (here: Covers of curves, i.e. global theory) one can prove that one has to expect similar results in general. (cf. thesis of C. Diem, in preparation.)

**Example (Diem)**
Take $l = 2$ and $E$ defined over $\mathbb{F}_{25}$. The elliptic curve $E \times \mathbb{F}_{2155}$ lead to a hyperelliptic curve of genus $2^{10}$ over $\mathbb{F}_{210}$. 
Typically for our present knowledge about Weil descent are

1.) If $f$ is too large the resulting curves are too complicated.
2.) If $f$ is small (e.g. $f \leq 3$) we can use the Weil descent to produce new admissible abelian varieties.
3.) In a medium range the discrete logarithm system attached to $E$ may be weakened.
Constructive examples (Diem):
1.) Assume that the ground field contains a $3 - rd$ root of unity $\mu$.

$$C_0 : y^2 = \mu x_1^7 + Bx_1^4 + A^3/(27\mu)x_1$$

has genus 3. Its Jacobian has a factor which is isogenous to a quotient of the product of an elliptic curve $E$ with itself with parameters $A$ and $B$. It is easy to find choices of $E, q$ which lead to rather good DL-systems.
2.) Assume that $q$ is a power of 3. Take $m = 3$ and an elliptic curve given by
\[ E : Y^2 = X^3 + AX^2 + B. \]
We generate $\mathbb{F}_{q^3}$ by an element $\alpha$ satisfying the equation
\[ \alpha^3 - \alpha = a. \]
Diem finds the curve
\[ y_0^2 = A^{-3}x_1^6 + ax_1^3 + Ax_1^2 - A^2x_1 + aA^3 + A^{-1} + B \]
on the Weil-restriction of $E$ over $\mathbb{F}_q$ which has genus 2.

3.3 Duality

3.3.1 The Tate Pairing

We sall see:
This pairing can be defined over $\mathbb{F}_q$ in
all cases relevant for applications nowadays.
But the background is the **Theory of abelian varieties over $\ell$–adic fields.**
So we give the general setting.
Let $K$ be a field with separable closure $\bar{K}$ and $A/K$ an abelian variety. For simplicity we shall assume that $A$ is principally polarized; so $A$ is equal to its dual variety.
(This is satisfied for Jacobian of curves.)
We shall assume from now on that $n$ is prime to $\text{char}(K)$. 11

$G_K$ acts on $A[n]$, we get the **Kummer sequence** of $G_K$-modules

$$0 \to A(K_S)[n] \to A(K_S) \overset{n}{\to} A(K_S) \to 0$$

11 The case $n = \text{char}(K)$ is even easier to discuss.
Application of Galois cohomology gives the exact sequence

\[ 0 \rightarrow A(K)/nA(K) \xrightarrow{\delta} H^1(G_K, A(K_s)[n]) \xrightarrow{\alpha} H^1(G_K, A(K_s))[n] \rightarrow 0. \]

Next we use that \( A(K_s)[n] \) is as \( G_K \)-module isomorphic to its dual group (since \( A \) is assumed to be principally polarized) and so we can use the cup product to get the **Tate-pairing**

\[ <, >_K: A(K)/nA(K) \times H^1(G_K, A(K_s))[n] \rightarrow H^2(G_K, \mu_n) \]

(where \( \mu_n \) is the group generated by the \( n \)-th roots of unity in \( K_s \))

given by

\[ < P+nA(K), \gamma >_K = \delta(P+nA(K)) \cup \alpha^{-1}(\gamma). \]
The group $H^2(G_K, \mu_n)$ is very important for the arithmetic of $K$: It consists of the elements of order dividing $n$ of the Brauer group $Br(K)$ of $K$.

3.3.2 Brauer Groups of Local Fields

The Brauer group of a finite field is $\{0\}$.

Let $K$ be an $l$–adic field. Local class field theory: $Br(K)$ is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$, the isomorphism is given by the invariant map $\text{inv}_K$.

To use this we need to make a severe assumption which limits the use of the Tate-pairing extremely:
Assume that $K$ contains the $n$–th roots of unity!
Then there exists a totally ramified Galois extension $L/K$ of degree $n$, $Br(K)[n]$ is isomorphic to $L^*/L^*n$ and so the DL-problem in the group $k^*[n] = \mu_n$ is equivalent with the DL-problem in $H^2(G(L/K), L^*)$.

3.3.3 Tate Duality over Local Fields

Let $K$ be an $l$–adic field with residue field characteristic $k$ and let $A$ be a principally polarized abelian variety defined over $K$.

(Tate: $<, >_K$ is non-degenerate.)
What about $H^1(G_K, A(K_s))[n]$ in our situation?

$$H^1(G_K, A(K_s))[n] = \text{Hom}_{U_n}(G(L_n/K(\zeta_n)), A(K_s)[n]).$$

Now apply Tate’s theorem to an abelian variety $\tilde{A}$ which is a lift of the abelian variety $A$ defined over the finite field $k$ containing the $n$–th roots of unity. By reduction resp. Hensel’s lemma we get a non-degenerate pairing

$$\langle , \rangle_k: A(k)/n\cdot A(k) \times \text{Hom}(G(L_n/K), A(k)[n])$$

induced by the Tate pairing.
3.3.4 Computation of the pairing

First step:

Theorem of Lichtenbaum:
Assume that $A = \text{Jac}_C$. Take $P_1 \in A(k)$ and $P_2 \in A(k)[n]$ with corresponding divisor classes $c_i$. Choose divisor $D_i \in c_i$ which are relatively prime.
By assumption there is a function $f$ on $C\!C$ with divisor $n \cdot D_2$.
Then:

$$< P_1 + nA(k), P_2 > = (f(D_1))^{q/n}$$

where $q = |k|$.

Because of complexity reasons it is not possible to work with this definition directly.
2. Step:
Mumford’s $\Theta$–groups: Take $A \times G_m$ with a twisted group structure related to $D_2$.
Take the $n$-fold addition of $(P_2, 1)$ to itself.
Result:

$$n(P_2, 1) = (0, f(D_1)).$$

As usual we use squaring and doubling to see that $<, >$ is computed in $O(\log(n))$ steps involving addition and evaluation of functions of degree $O(g_C))$. Hence:
Assume that $k$ is the field with $q$ elements with $n \equiv 1 \mod n$ and let $A$ be the Jacobian of a curve of genus $g$ defined over $k$.
Then the pairing $<, >$ can be computed in polynomial time w.r.t. $g \cdot \log(q)$. 

98
3.3.5 Application to the Decision Problem

We continue to assume that \( k \) contains the \( n \)-th roots of unity and that \( A \) is the Jacobian of a curve. It is obvious that the DL-problem on \( J_C \) can reduced to the DL-problem in \( k^* \) and so has subexponential complexity in \( q \). But there is another problem related to DL-systems which is used in the proof of security of some crypto protocols:
The **Diffie-Hellman Decision Problem (DHDP).**

Assume that
\[ P, Q, R \in < P_0 > \]
are known.

Let \( P = l \cdot P_0, Q = m \cdot P_0 \).

Decide whether
\[ R = l \cdot m \cdot P_0 \]
(without knowing \( l, m \).

It is known that this problem is as difficult as the DL-problem in generic groups of prime order!
In our situation:
Assume that there is an endomorphism \( \eta \) of \( A \) with

- \( \langle P_0 + nA(k), \eta(P_0) \rangle = \zeta_n \)

where \( \zeta_n \) is a primitive \( n \)-th root of unity

- \( \eta \) can be computed in polynomial time.

Then

\[
\langle P + nA(k), \eta(Q) \rangle = \zeta^{l \cdot m}
\]

and the decision problem related to \( P, Q, R \) reduces in polynomial time to the equality test of \( \langle R + nA(k), \eta(P_0) \rangle \) and \( \langle P + nA(k), \eta(Q) \rangle \) in \( k \).
Examples:
We always assume that $p$ is a prime.
1.) Assume that $A(k)[p^2]$ has order $p$ and that $\zeta_p \in k$. Take $P_0 \in A(k)[p] \setminus \{0\}$. Then
\[ < P_0 + pA(k), P_0 > \neq 1. \]

1.’) Let $E$ be an elliptic curve defined over $k$ and assume that either $p \mid q - 1$ and $p^2 \mid 2 - Tr(\pi_q)$ or that $p^2 \mid q - 1$ and $p \mid 2 - Tr(\pi_q)$. Take $P_0 \in E(k)[p] \setminus \{0\}$. Then
\[ < P_0 + pE(k), P_0 > \neq 1. \]

In both cases we get that DHDP is solvable in polynomial time in $log(q)$. 
2.) Assume that $E$ is a supersingular elliptic curve defined over $k$ with $q = l^f$, $f$ odd. Assume that $\eta$ is an endomorphism of $E$ which is not equal to the multiplication with an integer. Hence $\eta$ is not defined over $k$.

Now assume that $E(k)[p^2]$ is cyclic of order $p$ generated by a point $P$. Then (over the extension field $k_1$ of $k$ in which both $\eta$ is defined and $\zeta_p$ is contained) we get:

Either $< P + pE(k_1), P > \neq 1$ or $< P + pE(k_1), \eta(P) > \neq 1$. 
Especially:
3.) Take \( l \) a prime congruent to 3 mod 4,

\[
E : Y^2 = X^3 - X
\]

over \( \mathbb{F}_{lf} \) with \( f \) odd.
Assume that \( P = (x, y) \) is a point of odd order in \( E(\mathbb{F}_{lf}) \). Let \( \eta \) be the automorphism of \( E \) mapping \( (X, Y) \) to \( (-X, iY) \).
Then

\[
\eta(P) = (-x, iy)
\]

is not \( \mathbb{F}_{lf} \)-rational and so the decision problem in \( < P > \) can be solved in polynomial time in \( l^f \).
3.3.6 Questions

1. Can one compute $<, >$ without using the condition that $K$ contains primitive $n$-th roots of unity?

2. Is $< P + nA(k), . >$ a One-Way-function?

3. Can one use the Hasse sequence of local and global Brauer groups

$$0 \rightarrow Br(K) \rightarrow \bigoplus_{l} Br(K_{l})$$

$$\oplus \text{inv}_{l} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$$