Mathematical Background of Public Key Cryptography

Gerhard Frey
University of Duisburg-Essen
Institute for Experimental Mathematics

frey@exp-math.uni-essen.de

G.A.T.I
CIRM -May 12-16, 2003

1 Data security and Arithmetic

Problem:

$$A \qquad \overrightarrow{open} \qquad B$$

$$\uparrow$$

$$C$$

$$(A, m, B) \qquad \mapsto \qquad (B, m, A)$$

The transfer of the message has to be "secure".

This has (at least) 3 aspects:

- Reliability (engineers)
- Correctness (coding theory, engineers and mathematicians)
- Authenticity, privateness (cryptography, mathematicians, computer scientists, engineers)

Solutions have to be simple, efficient and cheap!

There was a basic decision some sixty years ago:
Messages are stored and transmitted as numbers.

This makes it possible to apply

Arithmetic

to data security.

We shall concentrate to the third aspect which uses

ENCRYPTION

provided by **cryptography.**

This is, in the true sense of the word, a classic discipline:
We find it in Mesopotamia and Caesar used it.

Encryption Devices

The devices shown are examples for **symmetric** procedures:
There is a common secret amongst the partners which enables them to de- and encrypt.

In principle they are used till today, in refined versions.
The new standard is called AES.

Typically the historical examples are involving secret services and military and the information is exchanged amongst a community in which each member is to be trusted.

This has changed dramatically because of electronic communication in public networks.
So data security has become a public challenge. There are millions of partners in nets.
Key exchange necessary for symmetric systems cannot be rely on personal trust and communication.

Solution:
PUBLIC KEY CRYPTOSYSTEMS
(Diffie-Hellman 1976)
Each member A of the network has **two** keys:

- a private key s_A produced by himself never leaving the private secure environment
- a public key p_A published in a directory.
  p_A is related to s_A by a (known) One-Way function.

For key exchange and for encryption/decryption A uses both keys (and the public key of the partner B if necessary).
There is no practically useable leakage of information about s_A, s_B !

BASIC IDEA:

One Way Functions

(Informal)**Definition:**
Let A and B be two finite sets of numbers and f a map from A to B.
f is a one way function if a computer can calculate $f(a)$ in ≤ 50 ms
but with very high probability $(1-10^{-30})$ it is impossible to find for given value $f(a)$ the argument a during the next 1000 years by using all known methods and all existing computers.

Here enters MATHEMATICS

- to construct candidates for one way functions
- to bring them in such a shape that computation is fast
- to analyze possible attacks

We shall concentrate us to systems based on the **Discrete Logarithm**

2 Abstract DL-Systems

Recall:
We want

- exchange keys
- sign
- authenticate
- (encrypt and decrypt)

with simple protocols
clear and easy to follow implementation rules
based on secure crypto primitives
with a well understood mathematical background.

Assume that $A \subset \mathbb{N}$ is finite
and that $B \subset End_{set}(A)$.

2.1 Key Exchange

Assume that the elements of B commute:
For all a and $b_1, b_2 \in B$ we have

$$b_1(b_2(a)) = b_2(b_1(a)).$$

Then we can use

$$A, B$$

for a key exchange system in the
following way:

We fix a
(publicly known) base point
$P_0 \in A$.
The members of the
crypto community
Q_i choose $s_i \in B$
and publish
$p_i := s_i(P_0)$.
Then
$s_i(p_j) = s_j(p_i)$
is the shared secret of
Q_i and Q_j.

The security depends (not only) on the complexity to find from the knowledge of randomly chosen $a \in A$ and given a_1, a_2 in $B \circ \{a\}$ **all** elements $b \in B$ with $b(a) = a_1$ modulo

$$Fix_B(a_2) = \{b \in B; b(a_2) = a_2\}.$$

The efficiency depends on the "size" of elements in A, B and on the complexity of evaluating $b \in B$.

2.2 Signature Scheme of El Gamal-Type

Again we assume that $B \subset End_{set}(A)$. In addition we assume that there are three more structures:

1. $$h : \mathbb{N} \to B,$$
   a hash function

2. $$\mu : A \times A \to C$$
   a map into a set C in which equality of elements can be checked fast

3. $$\nu : B \times B \to D \subset Hom_{set}(A, C)$$

with

$$\nu(b_1, b_2)(a) = \mu(b_1(a), b_2(a)).$$

Signature:

$a \in A$ is given (or introduced as part as the public key).

P chooses b and publishes $b(a)$.

Let m be a message.

P chooses a random element $k \in B$.

P computes

$$\phi := \nu(h(m) \circ b, h(k(a)) \circ k)$$

in D.

P publishes

$$(\phi, m, k(a)).$$

Verification:

V computes

$$\mu(h(m)(b(a)), h(k(a))(k(a)))$$

and compares it with $\phi(a)$.

2.3 The most popular realization

$A \subset \mathbb{N}$ a cyclic group
of prime order p
(with composition written multiplicatively.
with a numeration.

Choose a_0, a generator of A.
$B = Aut_{\mathbb{Z}}(A) \cong (\mathbb{Z}/p)^*$
identified with $\{1, ..., p-1\}$
by $b(a) := a^b$.

$C = A$ and $\mu =$ multiplication in A

$\nu =$ addition of endomorphisms
$h =$ a hash function
from $\mathbb{N}$ to $\{1, ..., p-1\}$.

We translate the

Signature scheme: to this situation: P chooses randomly and secretly, his **private key** $x \in \{1, ..., p-1\}$ and publishes his **public key** $Y := a_0^x$.

To sign a message m, P chooses a second random number k and computes

$$s := h(m)x + h(a_0^k)k \bmod p.$$

The signed message consists of

$$(m, a_0^k, s)$$

To check the authenticity of (P, m) one computes

$$S = a_0^s, T = Y^{h(m)}, H = a_0^{h(a_0^k)}.$$

and checks whether

$$S = T \circ H.$$

The security considerations
for the crypto primitive
boil down to the complexity of the computation of the
Discrete Logarithm:
For randomly chosen $a_1, a_2 \in G$ compute $n \in \mathbb{N}$ with

$$a_2 = a_1^n.$$

Challenge:
Construct
groups with numerations
of large prime order
such that the computation of the discrete discrete logarithm has the required complexity.

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 $\log(p)$.

2.4 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 $i = 0, ..., S \leq \sqrt{p}$ 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 ρ-Algorithm(probabilistic)[1]
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

$$x_i = P + x_{i-1} \text{ if } x_{i-1} \in T_1,$$
$$x_i = Q + x_{i-1} \text{ if } x_{i-1} \in T_2,$$
$$x_i = 2x_{i-1} \text{ if } x_{i-1} \in T_3.$$

There are efficient methods to detect collisions.

[1]Pollard's method is used for the "world record" w.r.t. Certicom challenge: Compute DL in an 108-bit elliptic curve.

Security hierarchy
We measure the complexity of a DL-system by the function

$L_p(\alpha, c) := exp(C(logp)^{\alpha}(loglogp)^{1-\alpha})$

with $0 \leq \alpha \leq 1$ and $c > 0$.

Best case: $\alpha = 1$:**Exponential complexity**.

Worst case: $\alpha = 0$: **Polynomial complexity**

The case between...: $0 < \alpha < 1$: The complexity is **subexponential**.

2.5 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 $\mathbb{Z}/p$:

$\alpha = 0$!

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. ζ is a primitive p-th root of unity).
Numeration:For $1 \leq i \leq p$ define
$z_i := [\zeta^i]_q$ and for $\overline{i} = i + p\mathbb{Z} \in G$

$$f(\overline{i}) := [z_i - z_1 + 1]_q.$$

Addition:
$a_i = f(x_i + p\mathbb{Z}) \in \{1, cdots, q-1\}$

$$a_1 \oplus a_2 = [[\zeta^{x_1+x_2}]_q - z_1 + 1]_q.$$

$$= [(a_1 + z_1 - 1)(a_2 + z_1 - 1) - z_1 + 1]_q$$

$$e(n, 1) = n \circ 1 = [z_1^n - z_1 + 1]_q.$$

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.
It usually is compared with factorization (this is no accident). Hence its security is to be compared with RSA.

Example 3:
A most important example:
Elliptic Curves

An elliptic curve E over a field K is a regular plane projective cubic with at least one rational point.

For simplicity we shall assume that $\mathrm{char}(K)$ is prime to 6. Then we find an equation

$$E: \; Y^2Z \; = \; X^3 + AXZ^2 + BZ^3$$

with $A, B \in K$ and $4A^2 + 27B^2 \neq 0$.

A very special property of elliptic curves is that their points form an abelian group.

Elliptic curve with addition

This addition is easily transformed into formulas:
Given

$$P_1 = (x_1, y_1) \ , P_2 = (x_2, y_2)$$

then

$$P_3 \ = (x_3, y_3) \ := \ P_1 \ \oplus \ P_2$$

with (in general):

$$x_3 \ = \ -(x_1{+}x_2){+}\ ((y_1{-}y_2)/(x_1{-}x_2))^2$$

To use elliptic curves E for DL-systems we have to solve the following diophantine problem:
Find $\mathbb{F}_q$ and an elliptic curve E such that the group of $\mathbb{F}_q-$ points has (almost) prime order of size $\approx 10^{60}$.

If we succeed we have to analyze attacks **using** the structures introduced during construction.

The state of the art :
For “generic” elliptic curves over “generic” finite fields the complexity of the computation of the Discrete Logarithm in the group of rational points is exponential.

But special elliptic curves are weak.

2.6 Numeration by Algebraic Groups

We generalize and systematisize 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.

2.6.1 Algebraic Groups

An algebraic group $\mathcal{G}$ 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)

$$m : \mathcal{G} \times \mathcal{G} \to \mathcal{G},$$

an inverse, i.e. a morphism

$$i : \mathcal{G} \to \mathcal{G},$$

and a neutral element, i.e. a morphism

$$e : \mathrm{Spec}(K) \to \mathcal{G},$$

satisfying the usual group laws:

$$m \circ (id_{\mathcal{G}} \times m) = m \circ (m \times id_{\mathcal{G}}) \text{ (associativity)},$$

$$m \circ (e \times id_{\mathcal{G}}) = pr_2$$

where pr_2 is the projection of $\mathrm{Spec}(K) \times \mathcal{G}$ to $\mathcal{G}$, and

$$m \circ (i \times id_{\mathcal{G}}) \circ \delta = j_e$$

where δ is the diagonal map from $\mathcal{G}$ to $\mathcal{G} \times \mathcal{G}$ and j_e is the map which sends $\mathcal{G}$ to $e(\mathrm{Spec}(K))$.

Down to earth:
For all extension fields L of K the set $\mathcal{G}(L)$ (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

$$0 := e(\mathrm{Spec}(K)) \in \mathcal{G}(K).$$

Example 1 corresponds to the additive group G_a (see below), Example 2 to the multiplicative group G_m, and Example 3 is an abelian variety of dimension 1.

3 DL-systems and orders

3.1 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 [2] 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.

[2] $A \subset O$ is an ideal of O if it is an $O-$module

How to compute A^k with
a numeration?

In general this will be not possible.
Here are some minimal assumptions:

I) O is **noetherian**:
Every A is a finitely generated $O-$module.
A generating system of the product of two ideals can be computed in finitely many steps from generators of the factors.

But these systems become longer and longer.

II)O can be embedded into a finitely generated algebra $\tilde{O}$ over an **euclidean** ring $\mathcal{B}$ such that the transition

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

preserves "enough" information. Then ideals A have a **base** over $\mathcal{B}$ (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 canonical basis for each ideal and $\mathcal{B}$ has a numeration. Then one can numerate ideals in O.

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,

$Pic(O)$

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?

So

1. Find a distinguished element in each class (resp. a finite (small) subset of such elements).
2. or: Find "coordinates" and addition formulas directly for elements of $Pic(O)$.

We need:

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 $Pic(O)$ 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 $Pic(O)$:

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

$$L_N(\alpha, c) := exp(c(logN)^{\alpha}(loglogN)^{1-\alpha})$$

mit $0 < \alpha < 1$ und $c > 0$ for a number N closely related to $\mid G \mid$.

3.2 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 $\mathbb{F}_p$.

3.2.1 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

$$g_K := 1/2log \mid \Delta_K \mid$$

(Δ_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 $Pic(O_K)$:
Uses analytic methods (L-series) in connection with most powerful tools from computational number theory.

There is a (probabilistic) estimate:
The order of $Pic(O_K)$ 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 $-D$.
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.

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 $ac - b^2 = D$, $-a/2 < b \leq a/2$, $a \leq c$ 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

$$O(L_D(1/2, \sqrt{2} + o(1))).$$

3.3 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 $Quot(O)$.

C is the desingularisation of the projective closure of the curve corresponding to O.
This relates $Pic(O)$ 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

We assume that O is not integrally closed.

The generalized Jacobian variety of C_p is an extension of J_C by linear groups.

Examples:

1. $Pic(\mathbb{F}_q[X,Y]/(Y^2-X^3)$ corresponds to the additive group.
2. $Pic(\mathbb{F}_q[X,Y]/(Y^2+XY-X^3)$ corresponds to G_m
   and (for a non-square d)

3. $Pic(\mathbb{F}_q[X,Y]/(Y^2+dXY-X^3)$ corresponds to a non split one-dimensional torus.

4. More generally we apply scalar restriction (se next lecture) to $G_m/\mathbb{F}_q$ and get higher dimension tori.

   Example:

   XTR uses an irreducible two-dimensional piece of the scalar restriction of $G_m/\mathbb{F}_{q^6}$ to $\mathbb{F}_q$.

   Though there is an algebraic group (torus) in the background the system XTR seems not to use it: It uses traces of elements instead of elements in the multiplicative group of of extension fields.

3.3.1 Work of Rubin-Silverberg

To understand what is going on Silverberg and Rubin analyse rational parametrisations of (non-)split tori, are able to explain related systems like LUC and give a new system CEILIDH.
In addition they come to interesting questions (conjectures) about tori (Vroskresenskii).
They also show limits of the method.

3.3.2 Security?

We can get tori by two different methods: By scalar restriction and by the Generalized Jacobian of curves of **geometric** genus 0 and **arithmetic** genus larger than 0.

Question:
Can this structure be used (as in the case of elliptic curves, see below) for attacks?

Curves without singularities

The corresponding curve C_a is an affine part of $C_p = C$.
The inclusion

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

corresponds to a morphism

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

which extends to a map

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

where $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$. The canonical map
$\phi : J_C(\mathbb{F}_q) \to Pic(O)$
is surjective but not always injective:
Its kernel is generated by formal combinations of degree 0 of points in $\pi^{-1}(\infty)$.

More precisely: $\mathbb{F}_q-$rational divisors of C are formal sums of points (over $\bar{\mathbb{F}}_q$) 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:

We find a representative D' in divisor classes c of the form
$D' = D - g\, P_\infty$ with $D = \Sigma_{i=1,\ldots g}\, a_i P_i$ with $a_i \geq 0$. Now map
$c \mapsto [\Pi_{P_i \in C_O}\, M_{P_i}^{a_i}]$.

Most interesting case: The kernel of ϕ is trivial.
Then we can use the ideal interpretation for computations and the abelian varieties for the structural background:

- 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 curves is done by using properties of abelian varieties resp. Jacobians of curves.

Example

Assume that there is a cover

$$\varphi : C \to \mathbb{P}^1;\ \deg \varphi = d,$$

in which one point (P_∞) 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 ϕ is an isomorphism.

Examples for curves having such covers are all curves with a rational Weierstraß point, especially C_{ab}-curves and most prominently **hyperelliptic curves** including **elliptic curves**
as well as superelliptic curves.

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

$$\mid J_C(\mathbb{F}_{p^n} \mid \sim \ p^{ng}.$$

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

4 Hyperelliptic curves

Definition[3]
Assume that C is a projective irreducible non singular curve of genus ≥ 1 with a generically étale morphism ϕ 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 ω denote the non trivial automorphism of this extension. It induces an involution ω on C with quotient $\mathbb{P}^1$.
The fixed points of ω are called **Weierstraß points**.

[3]Elliptic curves ($g = 1$) are included.

Assume that we have a $\mathbb{F}_q$-rational Weierstraß point P_∞.
We choose ∞ 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: $J_C(\mathbb{F}_q) = Pic(O)$.

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**.

Explicit formulas by T. Lange

Addition, $\deg u_1 = \deg u_2 = 2$	
Input	$[u_1, v_1], [u_2, v_2], u_i = x^2 + u_{i1}x + u_{i0}, v_i = v_{i1}x + v_{i0}$
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$

Step	Expression	Operations
1	compute resultant r of u_1, u_2: $z_1 = u_{11} - u_{21}$, $z_2 = u_{20} - u_{10}$, $z_3 = u_{11}z_1 + z_2$; $r = z_2z_3 + z_1^2u_{10}$;	1S, 3M
2	compute almost inverse of u_2 modulo u_1 ($inv = r/u_2 \bmod u_1$): $inv_1 = z_1$, $inv_0 = z_3$;	
3	compute $s' = rs \equiv (v_1 - v_2)inv \bmod u_1$: $w_0 = v_{10} - v_{20}$, $w_1 = v_{11} - v_{21}$, $w_2 = inv_0w_0$, $w_3 = inv_1w_1$; $s'_1 = (inv_0 + inv_1)(w_0 + w_1) - w_2 - w_3(1 + u_{11})$, $s'_0 = w_2 - u_{10}w_3$; if $s'_1 = 0$ see below	5M
4	compute $s'' = x + s_0/s_1 = x + s'_0/s'_1$ and s_1: $w_1 = (rs'_1)^{-1}(= 1/r^2s_1)$, $w_2 = rw_1(= 1/s'_1)$, $w_3 = s'^2_1w_1(= s_1)$; $w_4 = rw_2(= 1/s_1)$, $w_5 = w_4^2$, $s''_0 = s'_0w_2$;	I, 2S, 5M
5	compute $l' = s''u_2 = x^3 + l'_2x^2 + l'_1x + l'_0$: $l'_2 = u_{21} + s''_0$, $l'_1 = u_{21}s''_0 + u_{20}$, $l'_0 = u_{20}s''_0$	2M
6	compute $u' = (s(l + h + 2v_2) - k)/u_1 = x^2 + u'_1x + u'_0$: $u'_0 = (s''_0 - u_{11})(s''_0 - z_1 + h_2w_4) - u_{10} + l'_1 + (h_1 + 2v_{21})w_4 + (2u_{21} + z_1 - f_4)w_5$; $u'_1 = 2s''_0 - z_1 + h_2w_4 - w_5$;	3M
7	compute $v' \equiv -h - (l + v_2) \bmod u' = v'_1x + v'_0$: $w_1 = l'_2 - u'_1$, $w_2 = u'_1w_1 + u'_0 - l'_1$, $v'_1 = w_2w_3 - v_{21} - h_1 + h_2u'_1$; $w_2 = u'_0w_1 - l'_0$, $v'_0 = w_2w_3 - v_{20} - h_0 + h_2u'_0$;	4M
total		I, 3S, 22M

Special case $s = s_0$		
$4'$	compute s: $inv = 1/r$, $s_0 = s'_0inv$;	I, M
$5'$	compute $u' = (k - s(l + h + 2v_2))/u_1 = x + u'_0$: $u'_0 = f_4 - u_{21} - u_{11} - s_0^2 - s_0h_2$;	S
$6'$	compute $v' \equiv -h - (l + v_2) \bmod u' = v'_0$: $w_1 = s_0(u_{21} + u'_0) + h_1 + v_{21} + h_2u'_0$, $w_2 = s_0 + v_{20} + h_0$; $v'_0 = u'_0w_1 - w_2$;	2M
total		I, 2S, 11M

Doubling, $\deg u = 2$			
Input	$[u, v], u = x^2 + u_1x + u_0, v = v_1x + v_0$		
Output	$[u', v'] = 2[u, v]$		
Step	Expression	odd	even
1	compute $\tilde{v} \equiv (h + 2v) \bmod u = \tilde{v}_1x + \tilde{v}_0$: $\tilde{v}_1 = h_1 + 2v_1 - h_2u_1$, $\tilde{v}_0 = h_0 + 2v_0 - h_2u_0$;		
2	compute resultant $r = \mathrm{res}(\tilde{v}, u)$: $w_0 = v_1^2$, $w_1 = u_1^2$, $w_2 = \tilde{v}_1^2$, $w_3 = u_1\tilde{v}_1$, $r = u_0w_2 + \tilde{v}_0(\tilde{v}_0 - w_3)$;;	2S, 3M ($w_2 = 4w_0$)	2S, 3M (see below)
3	compute almost inverse $inv' = invr$: $inv'_1 = -\tilde{v}_1$, $inv'_0 = \tilde{v}_0 - w_3$;		
4	compute $k' = (f - hv - v^2)/u \bmod u = k'_1x + k'_0$: $w_3 = f_3 + w_1$, $w_4 = 2u_0$, $k'_1 = 2(w_1 - f_4u_1) + w_3 - w_4 - v_1h_2$; $k'_0 = u_1(2w_4 - w_3 + f_4u_1 + v_1h_2) + f_2 - w_0 - 2f_4u_0 - v_1h_1 - v_0h_2$;	1M	2M (see below)
5	compute $s' = k'inv' \bmod u$: $w_0 = k'_0inv'_0$, $w_1 = k'_1inv'_1$; $s'_1 = (inv'_0 + inv'_1)(k'_0 + k'_1) - w_0 - w_1(1 + u_1)$, $s'_0 = w_0 - u_0w_1$; If $s_1 = 0$ see below	5M	5M
6	compute $s'' = x + s_0/s_1$ and s_1: $w_1 = 1/(rs'_1) (= 1/r^2s_1)$, $w_2 = rw_1 (= 1/s'_1)$, $w_3 = s'^2_1w_1 (= s_1)$; $w_4 = rw_2 (= 1/s_1)$, $w_5 = w_4^2$, $s''_0 = s'_0w_2$;	I, 2S, 5M	I, 2S, 5M
7	compute $l' = s''u = x^3 + l'_2x^2 + l'_1x + l'_0$: $l'_2 = u_1 + s''_0$, $l'_1 = u_1s''_0 + u_0$, $l'_0 = u_0s''_0$;	2M	2M
8	compute $u' = s^2 + (h + 2v)s/u + (v^2 + hv - f)/u^2$: $u'_0 = s''^2_0 + w_4(h_2(s''_0 - u_1) + 2v_1 + h_1) + w_5(2u_1 - f_4)$; $u'_1 = 2s''_0 + w_4h_2 - w_5$;	S, 2M	S, M
9	compute $v' \equiv -h - (l + v) \bmod u' = v'_1x + v'_0$: $w_1 = l'_2 - u'_1$, $w_2 = u'_1w_1 + u'_0 - l'_1$, $v'_1 = w_2w_3 - v_1 - h_1 + h_2u'_1$; $w_2 = u'_0w_1 - l'_0$, $v'_0 = w_2w_3 - v_0 - h_0 + h_2u'_0$;	4M	4M
total		I, 5S, 22 M	I, 5S, 22 M
Special case $s = s_0$			
$6'$	compute s and precomputations: $w_1 = 1/r$, $s_0 = s'_0w_1$, $w_2 = u_0s_0 + v_0 + h_0$;	I,2M	I,2M
$7'$	compute $u' = (f - hv - v^2)/u^2 - (h + 2v)s/u - s^2$: $u'_0 = f_4 - s_0^2 - s_0h_2 - 2u_1$;	S	S
$8'$	compute $v' \equiv -h - (su + v) \bmod u'$: $w_1 = s_0(u_1 - u'_0) - h_2^2u'_0 + v_1 + h_1$, $v'_0 = u'_0w_1 - w_2$;	2M	2M
total		I, 3S, 13M	I, 3S, 14M

4.1 Non hyperelliptic curves of genus 3

Picard curves
or more generally
plane curves of genus 3
given by

$$Y^3 + f_1(X)Y = f(X)$$

with $deg(f) = 4$
have an efficient arithmetic too! (cf. e.g. work of Flon-Oyono).

4.2 Index-Calculus

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 $\mid D \mid$ 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.

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 $L_{1/2,q^g}[\frac{5}{\sqrt{6}}((1+\frac{3}{2t})^{1/2}+(\frac{3}{2t})^{1/2})]$.
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.

Principle:
Use prime divisors of small degree (e.g. 1) as factor base.

"Result": Orders related to curves with rational Weierstraß points of genus ≥ 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 (and even $g = 3$ is a little bit in danger)!

5 Galois Operation

5.1 Find a Curve!

The tasks are:
Find a finite field k, a curve C defined over k and a prime number p dividing $\mid Pic(O_C) \mid$, a point $P_0 \in Pic(O_C)$ such that we get a secure DL-system.
The determination of P_0 is not difficult if C is known.
To find (k, C) one uses the following strategy:

- Prove (e.g. by analytic number theory techniques) that good pairs occur with a reasonable large probability.
- Choose random (k, C) and count the elements in $Pic(O_C)$.

The second task is solved by determining the characteristic polynomial of the Frobenius automorphism Π acting on vector spaces related to the geometry of C and J_C:

Computation of the L-series of $C_{/k}$.

Examples for representation spaces are spaces of holomorphic differentials or more generally of differentials with prescribed poles and cohomology groups.

De Rham cohomology, étale cohomology and crystalline cohomology are especially interesting.

Methods:

- l-adic Methods:
  Use étale cohomology for small prime numbers l: (Schoof's algorithm)
- $\mathfrak{p}$-adic Methods: Use $\mathfrak{p}-$adic analysis and cohomology theories
  (Satoh, Gaudry-Harley-Mestre, Kedlaya, Lauder-Wan, Gerkmann)

Result: Efficient counting of
points on elliptic curves over all finite fields, points on hyper(super-)elliptic curves over fields of small characteristic and (!) on random curves of genus 2 (Gaudry) in cryptographic relevant ranges.

Counting on special curves

- Assume a curve is defined over a small field.
  Make a constant field extension, use naive counting methods or exponential algorithms to compute the L-series over the ground field.
  It is easy to determine it over extension fields.
- Reduction of global curves with real or complex multiplication.
  This method works very well for hyperelliptic curves genus 1,2,3.

5.1.1 Open Problems

1. Find an efficient algorithm to count points on random curves of genus 3 (not necessarily hyperelliptic) over random fields.
2. Does a computable global CM/RM-structure affect security?
3. Especially: Does the existence of endomorphisms with small norm allow attacks?

5.2 Scalar Restriction

One example to use the
extra structure:
Frobenius endomorphism
is the scalar restriction.
It is applied to curves which are not defined over prime fields.
It can be used to transfer DL's in many elliptic curves to DL's in Jacobians of curves for which the index-calculus method works.

It seems to be clear that it does not work for random curves or for extensions of large prime degree (which is not a Mersenne prime).

Principles:

Variant 1: Let L be a finite Galois extension of the field K.

Assume that C is a curve defined over L, D a curve defined over K and

$$\varphi : D \times L \to C$$

a non constant morphism defined over L.

Then we have a correspondence map

$$\phi : Pic^0(C) \to Pic^0(D)$$

$$\phi := Norm_{L/K} \circ \varphi^*.$$

Assumption: $ker(\phi)$ is small.

Then the (cryptographically relevant) part of $Pic^0(C)$ is mapped injectively into $Pic^0(D)$ and we have a transfer of the DL-problem in $Pic^0(C)$ into a (possibly easier) DL-problem.

It seems that this variant works surprisingly well if C is a (hyper-)elliptic curve not defined over K in characteristic 2.
cf. work of Galbraith, Smart, Hess, Gaudry,Diem,...
Key word: **GHS attack**

It relates the DL-problem to the highly interesting theory of fundamental groups of curves over non algebraically closed ground fields.

It certainly would be worth while to study this approach for non projective curves like curves of genus 0 with singularities.

Variant 2:
Again assume that C is defined over L. We apply scalar restriction from L to K to the (generalized) Jacobian variety of C and get a $[L : K]-$dimensional (group scheme) Abelian variety A over K.
Now we look for curves D in $K-$simple factors B of A.
As B is a factor of $Jac(D)$ we can hope to transfer the DL-problem from $Jac(C)$ to $Jac(D)$.

It is not clear whether this variant can be used in practise.

But it leads to interesting mathematical questions:

- Which group schemes have curves of small genus as sub schemes?
- Investigate the Jacobian of modular curves!
- Which curves have the scalar restriction of an abelian variety (e.g. an elliptic curve) as Jacobian?

To the last question: Bouw, Diem and Scholten have found families of such curves!

5.3 Bilinear Structures

We shall use properties of abelian varieties with Galois action to build up a bilinear structure related to our DL-system in special cases.

Assume that the DL-system $A, \circ$ is given and that there is a group A' in which we can compute "as fast" as in A.
Assume moreover that $(B, \circ)$ is another DL system and that a map

$$Q(a_1, a_2) : A \times A' \to B$$

is computable in polynomial time (this includes that the elements in B need only $O(log \mid A \mid)$ space
with

- for all $n_1, n_2 \in \mathbb{N}$ and random elements $a_1, a_2' \in A \times A'$ we have

  $Q(n_1 \circ a_1, n_2 \circ a_2') = n_1 \cdot n_2 \circ Q(a_1, a_2')$

- $Q(.,.)$ is non degenerate and hence for random $a' \in A'$ we have
  $Q(a_1, a') = Q(a_2, a')$ iff $a_1 = a_2$.

Then we call (A, Q) a DL-system with bilinear structure.

There are two immediate consequences:

- The DL-system $(A, \circ)$ is at most as secure as the system $(B, \circ)$.
- Assume moreover that $A = A'$.
  Given a (random) element a
  and $a_1, a_2, a_3 \in \mathbb{N} \circ a$ one can decide in polynomial time (in $log \mid B \mid$) whether (simultaneously)

  $a_1 = n_1 \circ a, a_2 = n_2 \circ a, a_3 = (n_1 \cdot n_2) \circ a$

  holds.

This are negative aspects of bilinear DL-systems but very interesting protocols due to Joux (tripartite key exchange) and Boneh-Franklin use such structures in a positive way.

6 Tate Duality of Abelian Varieties

In this section we shall discuss a bilinear structure on points of order p inside of the rational points of the Jacobian variety of a curve C with a rational point P_0 defined over a finite field k of characteristic l_0 with values in the **Brauer group** of a local field which can weaken our system in some cases.

We distinguish now two cases:
1.) $p = l_0$ and
2.) $p \neq l_0$
and begin our discussion with the first case. We follow closely a paper of Rück [Ru].

6.1 The Artin-Schreier case

We use the following result about algebraic function fields with positive characteristic(Serre 1956):

Proposition 1 *Let k be a field of characteristic p, C a projective curve of genus g defined over k and $\Omega^1(C)$ the $k-$vector space of holomorphic differentials on C. Then there is an isomorphismus from $Pic_0(C)[p]$ into $\Omega^1(C)$ given by the following rule:*
Choose a divisor D with $p \cdot D = (f)$ where f is a function on C. Then the divisor class $\bar{D}$ of D is mapped to the holomorphic differential df/f.(We have to use that char(K)= p!)

Next we describe differentials by their power series expansion at P_0.
Let t be a local parameter of C at P_0. Let $(a_0, a_1, ..., a_{2g-2})(f)$ be the tupel whose coordinates are first coefficients of the power series expansion of

$$(\partial f/\partial t)/f$$

at P_0. Hence we have to evaluate a function at a point. The problem is that the degree of f is very large.
The Riemann-Roch theorem implies that $(a_0, a_1, ..., a_{2g-2})(f)$ determines df/f completely . Hence

$$\Phi : Pic_0(C)[p] \to k^{2g-1}$$

given by

$$\bar{D} \mapsto (a_0, a_1, ..., a_{2g-2})(f)$$

is an injective map.

Hence: Φ transfers the DL- problem from $Pic_0(C)[p]$ into k^{2g-1} with its additive group structure. As remarked in example 1 this means that the DL-system is broken if the computation of Φ can be done in polynomial time.
We leave this as an open problem for a moment and go to the second case:

6.2 The Kummer case

We begin by discussing a more general situation.
Let K be a field with absolute Galois group G_K and A a principally polarized abelian variety over K, p prime to char(K).

By μ_p we denote the group of p-th roots of unity in the separable closure K_s of K (regarded as G_K module).
We have the exact sequence of G_K-modules (Kummer sequence)

$$0 \to A(K_s)[p] \to A(K_s) \stackrel{\cdot p}{\to} A(K_s) \to 0.$$

Application of Galois cohomology gives the exact sequence

$$0 \to A(K)/pA(K) \stackrel{\delta}{\to} H^1(G_K, A(K_s)[p])$$
$$\stackrel{\alpha}{\to} H^1(G_K, A(K_s))[p] \to 0.$$

Next we use that $A(K_s)[p]$ is as G_K-module self dual (since A is principally polarized) and so we can use the cup product to get the **Tate-pairing**

$$<,>_K: A(K)/pA(K)\times H^1(G_K, A(K_s))[p] \to H^2(G_K, \mu_p)$$

given by

$$< P+pA(K), \gamma >_K = \delta(P+pA(K))\cup\alpha^{-1}(\gamma).$$

$H^2(G_K, \mu_p)$ is a very important group for the arithmetic of K, it is isomorphic to $H^2(G_K, K_s^*)[p]$ and hence consists of the elements of order dividing p of the **Brauer group** $Br(K)$ of K.

The information we can get out of the Tate-pairing depends on the information given by the Brauer group and on its degree of non-degeneracy.

For instance if $K = k$ is a finite field the Brauer group is $\{0\}$.
The situation changes if we take K as an $\mathfrak{l}-$adic field with residue field k.

Theorem 1 (Tate)
$<,>_K$ *is non-degenerate.*

Hence for principally polarized abelian varieties over $\mathfrak{l}$-adic fields we have transferred the DL- problem in $A(K)[p]$ to the corresponding problem in $Br(K)[p]$ provided that we can evaluate the pairing in polynomial time.

This means especially that we can describe and compute in $H^1(G_K, A(K_s))[p]$ and $Br(K)[p]$.
Let us assume that K **contains the** $p-$**th root of unity** ζ_p,, i.e.
$p \mid (q-1)$.
Standard calculations with cohomology groups yield:
Let L_p be a ramified extension of K of degree p.

Corollary 1 *There is a non-degenerate pairing*

$$<,>: A(K)/p\cdot A(K) \times \mathrm{Hom}(G(L_p/K), A(K)[p]) \rightarrow Br(K)[p]$$

induced by the Tate pairing.

6.3 Application to Jacobian Varieties over Finite Fields

We continue to assume that k is a finite field of order $q = l_0^f$ and that$p$ is a prime dividing $q - 1$. Let C be a projective curve defined over k and let A be its Jacobian. We lift (C, A) to $(\tilde{C}, \tilde{A})$ over an $\mathfrak{l}$-adic field K with residue field k and apply Corollary 1 to $\tilde{A}$.

Now we invest what is known about the Brauer group of K. We use that $Br(K)[p]$ is cyclic of order p and that it is generated be cyclic algebras $(\sigma, a \cdot N_{L/K}(L^*)$(cf. second lecture) where L/K is a cyclic extension of degree p and σ is a generator of its Galois group.

Proposition 2 (Lichtenbaum) *Let τ be a generator of $G(L_p/K)$. Let P_1, P_2 be points of $\tilde{A}(K)$ with P_2 a point of order p. Let φ be the homomorphism of $G(L_p/K)$ to $J_C(k)[p]$ mapping τ to P_2. Represent $P_i - P_0$ by coprime divisors D_i in the divisor class group, and let f_2 be a function on $\tilde{C}$ with divisor $p \cdot D_2$.*
Then

$$< P_1 + p \cdot \tilde{A}(K), \varphi >= f_2(D_1) \cdot N_{L_p/K}/(L^*).$$

$\tilde{A}(K)[p]$ is isomorphic to $A(k)[p]$, $\tilde{A}(K)/p\cdot A(K)$ is isomorphic to $A(k)/p \cdot A(k)$ and $K*/N(L_p/K)(L_p^*)$ is isomorphic to k^*/k^{*p}, so:

Corollary 2 *There is a non-degenerate pairing*

$$<,>_k: A(k)/p\cdot A(k)\times A(k)[p]) \to k^*/k^{*p}$$

given by the the following rule:
Let P_1, P_2 be points of $\tilde{A}(k)$ with P_2 a point of order p. Represent $P_i - P_0$ by coprime divisors D_i in the divisor class group of C, and let f_2 be a function on C with divisor $p \cdot D_2$.
Then

$$< P_1+p\cdot J_C(k), P_2 >= f_2(D_1)\cdot k^*/k^{*p}.$$

As in the additive case we can transfer the DL-problem in $J_C(k)[p]$ to the discrete logarithm in a group related to k provided that we can compute $f_1(D_2)$ fast enough.
But there are two crucial differences: In the multiplicative case we end up in the *multiplicative group* of k, and in this group only sub exponential attacks are known, and secondly we can transform the original Tate duality pairing into a computable version only under the condition that *k contains the $p-$th roots of unity.* This last condition is rather difficult to satisfy (or easy to avoid).

6.4 Computation of the duality pairing

In both cases the computation of the Tate-Lichtenbaum pairing boils down to the evaluation of a function f on C at a divisor E of C. The problem is that the degree of the zero- resp. pole divisor of f and the degree of the negative (and positive) part of D are very large (about p) and so a direct approach to do this evaluation is not possible. The way out was found by V. Miller for elliptic curves (applied to the Weil pairing).

We use the theory of Mumford's Theta groups which explicitly describes extensions of (finite subgroups of) abelian varieties by linear groups.
We restrict ourselves to the multiplicative case.
The basic step for the computation is:
For given positive divisors A_1, A_2 of degree g find a positive divisor A_3 of degree g and a function h on C such that

$$A_1 + A_2 - A_3 - gP_0 = (h).$$

We can assume that this step can be done fast for otherwise we could not use J_C for DL-systems.
As measure for the complexity of our algorithm we shall take the needed amount of such steps.

We recall that we have a canonical birational morphism, ϕ_g, between the g-fold symmetric product of C and J_C.
Let S be a subset of $J_C(k)$. A divisor E of C is called prime to S if it is prime to all divisors in $\phi^{-1}(s); s \in S$.
Now assume that S is a finite subgroup of J_C, and that E is prime to S.
Define the following group law on $S \times k^*$:

$$(s_1, a_1) \circ (s_2, a_2) := (\phi_g(A_3), a_1 a_2 \cdot h(E))$$

where A_3, h are computed as above with $A_i = \phi^{-1}(s_i)$.
The assumption for E guarantees that $h(E) \in k^*$. The degree of h is at most g, and so the evaluation is polynomial in $g \cdot log \mid k \mid$.

We apply this in the following situation: $\bar{D}$ is an element of order p in $J_C(k)$ and $D \in \bar{D}$ is a divisor of the form $D = A - gP_0$ where A is a positive divisor of degree g on C. Furthermore E is a divisor of degree 0 on C which is prime to the group generated by $\bar{D}$ in $J_C(k)$.
Then the $p-$fold application of $\circ$ gives the result

$$(\underline{0}, f(E))$$

where f is a function on C with $(f) = pD$.

This is easily seen by induction for evaluating the application of $\circ\, l$ times gives

$$(\phi_g(A_{l-1}), h_{l-1}(E))$$

with a positive divisor A_{l-1} of degree g and a function h_{l-1} whose divisor is equal to

$$lA - A_{l-1} - (l-1)gP_0.$$

Since $\bar{D}$ is a $p-$torsion point A_{p-1} equals gP_0 and so h_{p-1} has the divisor $pA - lgP_0$.

Now we can use the group structure on $< \bar{D} > \times k^*$ and apply the square- and multiply algorithm to evaluate f at E in $O(log(p))$ addition steps.

CONSEQUENCE:
We can reduce the discrete logarithm in $A(K)/pA(K)$ to the discrete logarithm in $Br(K)_p$ with the costs $O(log(|\mathbb{F}_q(\mu_p)|)$.

Remark:
In general the conditions that K and hence the residue field $\mathbb{F}_q$ contains $p-$th roots of unity **and** that A has points of order p rational over $\mathbb{F}_q$ which are cryptographically interesting will not be satisfied at the same time.
For elliptic curves we can formulate this more precisely:

Proposition 3 *Let E be an elliptic curve defined over $\mathbb{F}_q$ and p a prime. Let π be the Frobenius automorphismus of $\mathbb{F}_q$.*
Then $\mathbb{Z}/p$ can be embedded into $E(\mathbb{F}_{q^f})$ iff the trace of π^f is congruent to $q^f + 1$ modulo p and the corresponding discrete logarithm in $E(\mathbb{F}_{q^f})$ can be reduced to the discrete logarithm in μ_p in the field $\mathbb{F}_{q^{fm}}$ where m is the smallest integer such that the trace of π^{fm} becomes congruent to 2 modulo p.

Sometimes one can enforce these conditions (after a small extension).

Corollary 3 *Assume that there is an endomorphism η of A with*

- $$< P_0 + pA(k), \eta(P_0) >= \zeta_p$$
- *η can be computed in polynomial time.*

Then the decision problem related to P, Q, R reduces in polynomial time to the equality test of $< R+pA(k), \eta(P_0) >$ and $< P + pA(k), \eta(Q) >$ in k.

Example 1 *Let E be a supersingular elliptic curve and assume that $\mathbb{F}_q$ has odd degree over $\mathbb{Z}/p$. Assume moreover that there is an endomorphism of E which is not contained in $\mathbb{Z} \cdot id_E$ and whose restriction to the points of order p can be computed in polynomial time (e.g. $E : Y^2 = X^3 - X$ and $\eta : X \mapsto -X, Y \mapsto \sqrt{-1}Y$). Then the conditions of the corollary are satisfied.*

7 Classical Discrete Logarithms: Computing in Brauer groups

7.0.1 Cyclic Algebras

$c \in Br(K)_p$ can be identified with algebras C over K which become isomorphic to the $p \times p-$matrices after tensorizing with some cyclic extension field L of degree p, i.e. we can determine c by a pair

$$(\sigma, a)$$

with $< \sigma >= G(L/K)$ and $a \in K^*/N_{L/K}L^*$: c is the class of $f_{\sigma,a} : G \times G \to L^*$, with

$$f_{\sigma,a}(\sigma^i, \sigma^j) = \begin{cases} a & : \quad i+j \geq p \\ 1 & : \quad i+j < p. \end{cases}$$

7.1 Local fields

7.1.1 Frobenius

Let K be complete with a discrete valuation v, a finite residue field k with $q = l_0^d$ elements and with Galois group G_K. For instance: $K = \mathbb{Q}_{l_0}$ and $k = \mathbb{Z}/l_0$.
Let π be the Frobenius automorphism of k.
Let L_u be the unique unramified extension of K of degree p. We can lift π in a canonical way to an element of the Galois group of L_u/K.

7.1.2 Invariants

The key results of local class field theory are:

1. Every element of c in $Br(K)[p]$ is equivalent to a cyclic algebra with respect to L_u/K.
2. Let c be given by (π, a). Then c is uniquely determined by $v(a)$ modulo p.

$v(a) \in \mathbb{Z}/p\mathbb{Z}$ is the
invariant $inv(c)$
of c.
Hence the computing in $Br(K)[p]$ would be trivial if we could compute invariants since then we transfer it to $\mathbb{Z}/p$.

For cyclic algebras two cases occur:
1)c is given by a pair (τ, a) and τ is another generator of $G(L_u)/K$. We have to determine n with

$$\tau^n = \pi.$$

2)c is given by (σ, a) with σ a generator of a ramified extension of degree p. We have to find an equivalent pair of the form (π, b).
(This is the case coming out of the Tate pairing.)
For both cases we have to solve discrete logarithms in finite fields.

7.2 Global fields

7.2.1 The Hasse-Brauer-Noether sequence

Let K be a global field (number field) with
localisations K_v and
with decomposition groups G_v.

We get the most important exact sequence

$$0 \to Br(K)[p] \overset{\oplus_{v' \in \Sigma_K} \rho_{v'}}{\longrightarrow} \bigoplus_{v' \in \Sigma_K} Br(K_{v'})[p] \overset{\Sigma_{v' \in \Sigma_K} inv_{v'}}{\longrightarrow} \mathbb{Z}/p \to 0.$$

where Σ_K is the set of equivalence classes of valuations of K.

7.3 Index-Calculus in Brauer groups

Assume that A_v is a cyclic algebra corresponding to $c_v \in Br(K_v)_p$.
Lift A_v to a cyclic algebra A defined over K and use the equation

$$-\Sigma_{v' \in \Sigma_K \setminus v} \; inv_{v'}(\rho_{v'}(A)) = inv_v(A_v).$$

to get relations.
For the lifting we need
existence theorems
for cyclic extensions of K with prescribed ramification delivered by
global class field theory
(in an explicit way e.g. by CM theory).

8 Example:$K = \mathbb{Q}$

The global class field theory of $\mathbb{Q}$ is completely determined by the theorem by Kronecker and Weber:

Theorem 2 (Kronecker–Weber) *Every abelian extension $K/\mathbb{Q}$ of $\mathbb{Q}$ is contained in a easily determined cyclotomic extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$.*
There exists an extension $K/\mathbb{Q}$ of degree l ramified exactly at p iff $l|p-1$ holds. If it exists it is uniquely determined.

We have a complete control of the decomposition laws of primes.

8.1 The Algorithm

Consider a global algebra A of the form $A = (K/\mathbb{Q}, \sigma, a)$. If a can be factored in the form $a = \prod p^{n_p}$ the theorem by Hasse–Brauer–Noether leads to a relation of the form

$$inv_p(a) + \sum_{q \neq p} f_q n_q \equiv 0 \bmod l. \quad (1)$$

Here the factors f_q are defined as follows:
Let $K_q/\mathbb{Q}_q$ denote the extension of local fields belonging to K/Q. We can identify $G(K_q, \mathbb{Q}_q)$ with the decomposition group G_q. Since G has prime order l, it is obvious that G_q is either trivial (if q splits completely in K) or is equal to G (if q is inert in K).

If $K_q/\mathbb{Q}_q$ is unramified (i.e. $q \neq p$) we can identify $G(K_q/\mathbb{Q}_q)$ with the Galois group $G(k_q/\mathbb{F}_q)$ of the extensions of residue class fields.

Let σ denote the fixed generator of G.

Define f_q by $\pi_q = \sigma^{f_q}$ (π_q the Frobenius at q) modulo l.

(1) can be seen as a linear equation relating the indeterminates $\{f_q, inv_p(a)$. Hence we have to produce enough equations of this form in order to apply linear algebra modulo l to compute "enough" factors f_q.

Definition 8.1 *A natural number* $n \in \mathbb{N}$ *is* M*–smooth iff the following holds:*

$$q \, prime, q|n \Rightarrow q \leq M.$$

Let $\psi(x, y)$ *denote the number of natural numbers* $n \leq x$ *which are* y*–smooth.*

Theorem 3 *Let* ε *be an arbitrary positive constant, then we have uniformly for* $x \geq 10$ *and* $y \geq (\log x)^{1+\varepsilon}$*:*

$$\psi(x, y) = xu^{-u+o(u)} \quad \textit{für} \, x \to \infty \tag{2}$$

where $u = (\log x)/(\log y)$.

8.1.1 One algorithm for $K = \mathbb{Q}$

Choose a smoothness bound M and compute the factor basis S consisting of the primes less or equal to M.

Let d be the smallest number $\geq \sqrt{p}$.
For $\delta \in L := [0, ..., l]$ take
$a_1(\delta) := d + \delta$.
$a_2(\delta) := c_0 + 2\delta \cdot d + \delta^2)$
$(\equiv a^2$ modulo $p)$
with $c_0 = d^2 - p$.
Assume that for $\delta \in L$ both $a_1(\delta)$ and $a_2(\delta)$ are $M-$smooth. Then we get a relation for the f_q for q in the factor base.
To find such $\delta \in L$ we can use sieves.

Having enough relations for a large enough factor base we can proceed as usual: For random a we take small powers of a and hope that modulo p such a power yields a smooth number. Then we can compute the invariant of the corresponding algebra and so the invariant of a and use this for computing discrete logarithms.

This approach unifies methods and results obtained by various authors (Coppersmith, ElGamal, Schirokauer,Adleman-Huang) using different and quite complicated methods for different cases. The most advanced amongst them are called number field sieve and function field sieve.
All these methods can be explained by Brauer groups and so class field theory of global fields is the right background for the DL in finite fields. That point of view could open new possibilities for more advanced attacks for instance by lifting from local Brauer groups to global Brauer groups in a more intelligent way.