Lectures on Cryptography
Heraklion 2003
Gerhard Frey
IEM, University of Duisburg-Essen

Part II
Discrete Logarithm Systems

1 Algebraic Realization of Key exchange and Signature

1.1 Key exchange and signature

The following is a repetition of facts explained in the first part of the lectures.

Take A as cyclic group of prime order p embedded into $\mathbb{N}$, i.e. a group G **with a numeration.**
In the sequel we shall assume that f is fixed and given and we shall identify A with G.
The group automorphisms of G are identified with elements in $\{1, ..., p-1\}$ by $\varphi_k(g) := g^k$.

One fixes a publicly known generator $g_0 \in G$.

1.1.1 Key exchange

Each partner P_i chooses a (random) number $s_i \in \{1, ..., p-1\}$ as secret (and not the group order as in RSA schemes) and publishes $p_i := g_0^{s_i}$.
It is obvious but has to be emphasized that there is know leakage of security if everyone knows everything about the group G.
If P_1 wants to share a secret with P_i he powers p_i by s_1. The security considerations boil down to the complexity of the computation of the **Discrete Logarithm:** How difficult is it to compute for randomly chosen $g_1, g_2 \in G$ a number $n \in \mathbb{N}$ with

$$g_2 = g_1^n?$$

1.1.2 Signature:

The person S who wants to sign a message chooses a secret $x \in \{1, ..., p-1\}$ and publishes $y := g_0^x$.

In addition it is publicly known that he uses a *hash function* h which maps G to $\{1, ..., p-1\}$.
Recall that it has to be impossible in practice to construct a number z such that $h(z)$ is a given value.

S chooses a second random number k and does the (for him since he knows k and x) easy computation

$$s := h(m)x + h(g_0^k) \cdot k \ \ \mathbf{mo\underline{d}ulo}\ p.$$

The signed message consists of

$$(m, g_0^k, s).$$

To check the authenticity of m V computes

$$S = g_0^s, P = y^{h(m)}, H = (g_0^k)^{h(g_0^k)}.$$

Now the properties of exponentiation imply:

$$S = P \oplus H$$

if the signature is authentic. Otherwise it is rejected.
Again the security depends crucially on the difficulty to compute the discrete logarithm in G.
In fact one can change the two protocols such that under strong attack models the security is equivalent with the hardness of the discrete logarithm.

1.2 Hardness

Since we have used the algebraic structure "group" we cannot avoid "generic" attacks like Shanks' Baby-Step-Giant-Step Method and Pollard's ρ-Algorithm and hence the complexity of computing discrete logs is bounded from above by $\approx \sqrt{p}$.
It can be shown that in black box groups attacks to the discrete logarithm problem cannot be better than these generic attacks.
So we have to find numerated groups of order $p \approx 10^{180}$ for which no (known) attacks of smaller complexity than $p^{1/2}$ exist.

To be more precise we introduce a **Security hierarchy.**
We measure the complexity of a DL-system by the function

$$L_x(\alpha, c) := exp(c(logx)^{\alpha}(loglogx)^{1-\alpha})$$

with $0 \leq \alpha \leq 1$, $c > 0$ and x closely related to p.

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

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

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

1.3 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 easily computed from the knowledge of r_i.
Security?
For given b with $b = e(n, a) = [na]_p$ solve

$$b = na + kp$$

with $k \in \mathbb{Z}$.
The *Euclidean algorithm* does this in $O(\log(p))$ operations in $\mathbb{Z}/p$ hence $\alpha = 0$!
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 $\bar{i} = i + p\mathbb{Z} \in G$

$$f(\bar{i}) := [z_i]_q.$$

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

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

$$= [a_1 a_2]_q$$

Security?
For two randomly chosen p-th roots of unity in the multiplicative group of $\mathbb{Z}/q$ one has to determine the exponent needed to transform one of them to the other. 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:**
is most important. It is an **Elliptic Curve.**
Recall:
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 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.
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):

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

and y_3 such that $\{(x_1, y_1), (x_2, y_2), (x_3, -y_3)\}$ is collinear.
In contrast to the first examples we have to solve a difficult diophantine oroblem if we want to use elliptic curves E for DL-systems:
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.

Consequence for key length:

- Additive subgroups of fields are weak for any group size.

- Multiplicative subgroups of fields have to be contained in fields with at least 1024 or better 2048 bits.
- Groups on random elliptic curves need a size of 180 bits.

1.4 Digression:Numeration by Algebraic Groups

We generalize and systematize the examples.
We use numerations induced by embedding $\mathbb{Z}/p$ into the group of rational points of **algebraic groups** over finite fields $\mathbb{F}_q$ where q is a power of a prime l_0.
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 ratinal functions 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.
If we restrict ourselves to connected commutative algebraic groups we have found essentially all types: Any $\mathcal{G}$ is composed by factors which correspond to tori (higher dimensional analogue of G_m), unipotent linear groups (analogue of G_a) and projective group schemes called **abelian varieties**. Elliptic curves are the one-dimensional abelian varieties.

So for cryptography tori and abelian varieties are interesting.

2 Ideal Class Groups

The concept of algebraic groups gives a nice frame for discrete logarithms but to work in this generality in practice would be hopeless. One has to use very special algebraic groups which represent well known objects in commutative algebra.

2.1 The Picard group

Let O be a (commutative) ring with unit 1 without zero divisors.
Two ideals [1] A, B of O can be multiplied:

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

Clearly $\cdot$ is associative. So ideals form a semi group.
In order to make this multiplication constructive we shall assume from now on that O is noetherian, i.e. that every ideal of O has a finite generating set.
We generalize the notion of ideals of O slightly:
Let K be the quotient field of O.
Let A be a subset of K such that there exists $f \in K^*$ with $f \cdot A \subset O$ an ideal of O. Then A is a (broken) ideal of O.

Next we introduce an equivalence relation:

Definition 2.1 *Let A_1, A_2 be two ideals of O.
$A_1 \sim A_2$ iff there is an element $f \in K$ with*

$$A_1 = f \cdot A_2.$$

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.

There is an immediate computational problem: The equivalence classes contain infinitely many ideals. How to describe the elements in $Pic(O)$ for the computer? So we have to be able

1. to find a distinguished element in each class (resp. a finite (small) subset of such elements) by an "reduction algorithm"

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

2. or: find “coordinates” and addition formulas directly for elements of $Pic(O)$. For this we can hope to use the geometric background of $Pic(O)$ which leads to **group schemes** ; i.e. the Pic functor of extension algebras of O can be represented by a group scheme.

Most interesting cases are those for which both methods can be used!

We want to embed $\mathbb{Z}/p$ into $Pic(O)$ in a bit-efficient way:
For this 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.

Thirdly we have to discuss and, if possible, **exclude attacks.**

2.2 Index Calculus Attacks

There is a **”generic attack”** for DL-systems based on $Pic(O)$:
We have distinguished ideals, the prime ideals.
We have to have a very special arithmetic structure of O in order to be able to do the reduction step. So we have a notion of “small” ideals.
Hence we are in a very similar situation as in the section about factorization of numbers and we can try to develop a analogous attack.
Principle:
We work in a group G .
Find a “factor base” consisting of relatively few small elements (i.e. in our case: classes which contain small prime ideals) and compute G as a $\mathbb{Z}-$module given by the free abelian group generated by the base elements modulo relations.
Then one has to 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 with small exponents.
The rest is linear algebra.
The important task is, as in the factorization algorithms, 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.
If successful the expected complexity of this attack is **subexponential**.

2.3 Existing Systems

What is used today? There are only two types:

- O is an order or a localization of an order in a number field, i.e. O is a subring of the ring of integers of an algebraic extension K of $\mathbb{Q}$ of degree n which is a $\mathbb{Z}$-module of rank n.

- O is the ring of holomorphic functions of a curve defined over a finite extension field of $\mathbb{F}_q$ and hence O is a **polynomial order** over $\mathbb{F}_q[X]$.

2.3.1 The 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

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

(Here Δ_K is the discriminant of $O_K/\mathbb{Z}$.)
The mathematical 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.

The most difficult part is the computation of the order of $Pic(O_K)$:
One 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 $exp(g_K)$ (but in a very erratic way).

One big **disadvantage** is that 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 split into two components:
The degree $n := [K : \mathbb{Q}]$ and the ramification locus of $K/\mathbb{Q}$.

If n is large the arithmetic in O_K is very complicated. Key words are computation of fundamental units, integral basis, lattice reduction ...).
So it is to be expected that the most practical examples have small degree.
We shall discuss the simplest case: K is an imaginary quadratic field of discriminant $-D$.
So $K = \mathbb{Q}(\sqrt{-D})$. The expected size of $Pic(O)$ is $\approx \sqrt{D}$.
By the **theory of Gauß** of quadratic forms $Pic(O_K)$ corresponds to classes of binary quadratic forms with discriminant D.
The multiplication of ideals corresponds to the composition of quadratic forms.
The 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 $a = c$.
So we can compute in $Pic(O_K)$ very efficiently.
But the great disadvantage is: The index-calculus-attack works very efficiently: Under assumption of the GRH one gets: The complexity to compute the DL in $Pic(O_K)$ is

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

2.3.2 The geometric case

O is the ring of holomorphic functions of a curve defined over a finite extension field $\mathbb{F}_q$ of $\mathbb{F}_{l_0}$.
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 C_P of the curve corresponding to O.

This relates $Pic(O)$ closely with the points of the Jacobian variety J_C of C. J_C is a **projective** group scheme and hence an abelian variety which represents the functor Pic^0 of **divisor classes** of degree 0 on C which is the projective analog of ideal classes of coordinate rings of affine curves. Hence the important role of abelian varieties in crypto systems used today becomes obvious.
First case:**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. Hence additive groups and tori appear as composition factors.
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 to $G_m/\mathbb{F}_q$ and get higher dimensional 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.

More of this and interesting mathematical problems related with tori can be found in recent papers of Rubin-Silverberg (cf. their web site) .
From now on we restrict ourselves to the case of **curves without singularities**.
The corresponding curve C_a 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

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

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 $J_C(\mathbb{F}_q)$ are the divisor classes of $\mathbb{F}_q-$rational divisors of degree 0 of C.
The theorem of Riemann-Roch implies that

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

(with S_g the symmetric group in g letters) is birationally isomorphic to J_C:
We find a representative D' in the divisor class c of the form $D' = D - g\,P_\infty$ with $D = \Sigma_{i=1,\cdots g}\, a_i P_i$ with $a_i \geq 0$ and $\Sigma_i\, a_i = g$. The rationality of D implies that the coefficients a_i depend only on the class of the points under the Galois operation.
Choose in any such class one point P_{j_i} and define $M_{P_{j_i}}$ as the ideal of functions

in O which vanish in P_{j_i}. Then $c \mapsto \Pi_{P_{j_i}} M_{P_{j_i}}^{a_i}$ induces the map ϕ.

The most interesting case is that 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

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

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. We can choose

1. l_0 = characteristic of the base field
2. n = degree of the ground field of $\mathbb{Z}/l_0$
3. $g_C = g$ = the genus of the curve C resp. the function field $Quot(O)$.

There are (asymptotically with l_0 growing) about $l_0^{3g \cdot n}$ curves of genus g over $\mathbb{F}_{l_0^n}$.
We have the result of Hasse-Weil:

$$\mid J_C(\mathbb{F}_{l_0^n} \mid \sim\ l_0^{ng}.$$

Using the ideal theoretic interpretation (and a rather obvious data compression) we get a **key length** of size $n\, log(p) \cdot g$ which is near to the group order.

3 Hyperelliptic curves

Definition 3.1 [2]
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 that 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 the Weierstraß points of C.

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

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**.
Of course the formulas become very involved as the genus grows.
Surprisingly it turns out for curves of genus 2 and genus 3 that in certain computer environments the formulas are faster than the algorithm and that scalar multiplication (with group order fixed) is even faster than on elliptic curves.

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

3.1 Explicit Formulas

Here are the best known formulas for genus 2 found by Tanja Lange:

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

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: $w_1 = (rs'_1)^{-1}(= 1/r^2s_1)$, $w_2 = rw_1(= 1/s'_1)$, $w_3 = {s'}_1^2w_1(= s_1)$; $w_4 = rw_2(= 1/s_1)$, $w_5 = w_4^2$, $s''_0 = s'_0w_2$;	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 Output	$[u,v], u = x^2 + u_1x + u_0, v = v_1x + v_0$ $[u', v'] = 2[u,v]$		
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 =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: $w_1 = 1/(rs'_1)(= 1/r^2s_1),\ w_2 = rw_1(= 1/s'_1),\ w_3 = {s'}_1^2w_1(= s_1)$; $w_4 = rw_2(= 1/s_1),\ w_5 = w_4^2,\ s''_0 = s'_0w_2$;	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 $u' = s^2 + (h + 2v)s/u + (v^2 + hv - f)/u^2$: $u'_0 = {s''_0}^2 + w_4(h_2(s''_0 - u_1) + 2v_1 + h_1) + w_5(2u_1 - f_4)$; $u'_1 = 2s''_0 + w_4h_2 - w_5$;	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

3.2 Index-Calculus

As in the analogous situation in number theory there exists a subexponential attack based on the index-calculus principle.
As in the number field case the subexponential function is a function in the order of the class group and so in q^g.
But in all known index-calculus algorithms one cannot look at q and g as independent variables. For instance if $g = 1$ is fixed then we do not get a subexponential attack for $q \to \infty$!.

This is obvious if one takes a closer look at the attack. In general the ideal classes of S can be represented by two polynomials in X of degrees g resp. $g-1$. One chooses as factor base for the index-calculus attack the ideal classes which can be represented by polynomials of smaller degrees.
So it was no surprise that the attack is most efficient if the genus is large compared with q.
The best result in this direction is due to **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 $L_{1/2,q^g}[\frac{5}{\sqrt{6}}((1+\frac{3}{2t})^{1/2}+(\frac{3}{2t})^{1/2})]$.

However it came as a surprise when Gaudry presented an **exponential** attack for relatively small genus (in practice: $g \leq 9$) based on the same principle. He chooses as factor base the classes which correspond to rational points on the curve. Their number is about q. Due to linear algebra his algorithm has complexity

$$O(q^2(\log(q))^\gamma)$$

with "reasonable small" constants.
If the genus of the curve is at most 3 the group order is bounded by $O(q^3)$ and hence the attack is weaker than a generic one.
The break even point is $g = 4$ and in fact Gaudry can show that in this case the complexity of computing the discrete logarithm is bounded by $O(q^{8/5}$!
So the present state of the art is: 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.

4 Counting Points

4.1 The Local L-series

In this section we use the structural properties of Jacobians being abelian varieties A of dimension g. We have to determine the order of the Mordell-Weil group $A(\mathbb{F}_q)$. Since the desired size of $|A(\mathbb{F}_q)|$ is at least 10^{60} we cannot count directly. Instead we shall use the **Galois group** of $\mathbb{F}_q$ and the known properties of its action on torsion points of abelian varieties.
The absolute Galois group $G_q = Aut(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ is topologically generated by the **Frobenius automorphism** $\pi_q =: \Pi$ which maps elements of $\overline{\mathbb{F}}_q$ to their $q-$th power.
For all natural numbers n Π 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 char(K), as $\mathbb{Z}/n$–module isomorphic to $(\mathbb{Z}/n)^{2g}$.

Theorem 4.1 (Weil)
The characteristic polynomial of Π *w.r.t. this action is the reduction modulo* n *of a polynomial with integer coefficients of degree* $2g$. *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 $\Pi - id$ we get by elementary linear algebra:

Proposition 4.1 $|A(\mathbb{F}_q)| = | L_A(1) |$.

A trivial but crucial consequence is:

Corollary 4.1 $\mathbb{Z}/p$ *is embeddable into* $A(\mathbb{F}_q)$ *iff* $L_A(1) \equiv 0 \, mod p$.

Hence we are looking for abelian varieties for which we can

1. compute $L_A(1)$ rapidly, and
2. prove that with a not too small probability a prime of size $\approx q^g$ 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.
We shall present some methods to solve the first item. They all use more or less sophisticated properties of L-series and Frobenius automorphisms.

4.2 Constant Field Extensions

This approach is the simplest method: We begin with a small field $\mathbb{F}_{q_0}$ and A defined over this field such that we *can* count the $\mathbb{F}_{q_0}-$rational points of A [3]. We use this to compute the zeroes ω_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 Π is the m-th power of π_{q_0}. Hence the zeroes of the L-series of $A \times \mathbb{F}_q$ are the $m-$th powers of ω_i and so the order of $A(\mathbb{F}_q)$ can be computed easily.

There is one obvious disadvantage: The group $A(\mathbb{F}_{q_0})$ is embedded into $A(\mathbb{F}_q)$ and so the maximal prime p dividing $|A(\mathbb{F}_q)|$ and useful for DL-systems divides $|A(\mathbb{F}_q)|/|A(\mathbb{F}_{q_0})|$. We summarize:

Proposition 4.2 *Let the notation be as above.*
Let p *be a prime larger than* $| A(\mathbb{F}_{q_0}) |$. *Then* $\mathbb{Z}/p$ *is embeddable into* $A(\mathbb{F}_q)$ *iff* p *divides*

$$\Pi_{i=1,\cdots,2g} \; (1-\omega_i^m)(1-\omega_i)^{-1}$$

and so the size of p *is at most* $\approx q_0^{g(m-1)}$.

[3] to give a rough idea: small means that $q^g \leq 10^{10}$

This means that the size of the DL-system compared with the key length and the time needed for an addition (roughly proportional to $\log(q)$) is not optimal.
Moreover one has to be careful with the degree of the extension since there is an attack related to scalar restriction ("Weil descent").
So mostly the method of constant field extensions is used only for very small q_0 and large prime m which is not a Mersenne prime. The typical examples are Koblitz curves defined over fields with 2-power order.

4.3 Schoof's Algorithm:Étale Cohomology

Remember: $L_A(T)$ is a polynomial with integral coefficients which simultaneously for all natural numbers n is the characteristic polynomial of Π 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.
This is the starting point of Schoof's algorithm for computing the number of points of elliptic curves over $\mathbb{F}_q$. It is made effective by another ingredient: It is well known that there is a linear recurrency between the n-division polynomials of elliptic curves.

Theorem 4.2 (Schoof)
For elliptic curves E the complexity to compute $L_E(T)$ is bounded by a polynomial function in $\log(q)$.

One can try to generalize this idea to arbitrary abelian varieties. One main task is to find a way of computing division polynomials. Kampkötter has done this in the case of Jacobians of hyperelliptic curves proving that for fixed g the computation of the L-series has polynomial complexity (similar results are due to Pila).
But Schoof's algorithm is too slow for practical applications, and the same is true in a much worse way for Kampkötter's algorithm.
For **elliptic curves** things have become much better by observations and refinements due to Atkin and Elkies. Instead of using the kernel of the multiplication by small n on elliptic curves E one can use the kernel of endomorphisms of small norm and determine $L_E(T)$ modulo ideals in the endomorphism ring of E (which is an *order R_E in an imaginary quadratic field or in a quaternion algebra*).
This explains why the determination of $L_E(T)$ modulo l is easier if the prime l splits in R_E.
For the actual computation one has to find convenient methods to describe isogenies of elliptic curves. Here enter the *modular curves $X_0(l)$*. These curves parametrize pairs of elliptic curves with cyclic isogenies of degree l. Their rich theory is the key to many of the important new results in arithmetic geometry.

Remark:
We are interested in (hyper-)elliptic curves over finite fields. To handle them we are led in a natural way to **global** objects in number theory: Orders in number

fields, modular curves and corresponding Galois representations!

Based on these considerations Schoof's algorithm for elliptic curves E has been refined.

Proposition 4.3 *Let ϵ be a positive real number.*
Let E be an elliptic curve over $\mathbb{F}_q$ and l a prime which is split in R_E.
Then $L_E(T)$ modulo l can be computed with probabilistic complexity
$O((\log(l)^2 \cdot \log(q))^{1+\epsilon})$.

To determine $L_E(T)$ one uses the information modulo different primes l and applies the Chinese remainder theorem. The estimates due to Hasse-Weil imply that $O(\log(q))$ different primes l are sufficient.
To use Proposition 4.3 we want to use split primes only and so we need bounds which ensure that we have found enough of them.
An easy check decides whether E is supersingular (and then $L_E(T)$ is known). So assume that E is not supersingular. We observe that q is a non-trivial norm with respect to $R_E/\mathbb{Z}$ and so the size of the discriminant of R_E is bounded by $O(\mid q \mid)$.
This implies conjecturally (and in practice) that it is enough to use primes l up to a bound of size $O(\log(q))$. Under the assumption of (GRH) it can be proved that the bound $O(\log(q))^2)$ (with explicitly computable constants) is big enough.

Theorem 4.3 *Assume that (GRH) is true. Let ϵ be a positive real number. Let E be an elliptic curve defined over $\mathbb{F}_q$.*
The order of $E(\mathbb{F}_q)$ can be computed with (probabilistic) complexity $O((\log(q))^\delta)$ with $\delta \leq 5 + \epsilon$ and conjecturally $\delta \leq 4 + \epsilon$.

By these results (and their practical implementation) we are able to count points on elliptic curves in all cryptographically interesting situations quite efficiently.
The situation is completely different for hyperelliptic curves of genus 2 and 3 though by a new paper of Gaudry and Schost at least for random curves of genus 2 there is remarkable progress.
Nevertheless one has to look for and to rely on different technics.

4.4 Lifting strategies

Strictly spoken we have used in the last remark already a global argument: The theory of complex multiplication and points on modular curves.
Of course it would be much more efficient to lift the whole situation to characteristic 0 and determine a lifting of the Frobenius automorphism explicitly.
Note: Π acts in two manners: As Galois automorphism **and** as endomorphism!
It is not difficult to lift Π as Galois group element but quite difficult to do this as

endomorphism.In general such liftings of A do even not exist. We need **canonical liftings.**
The theorem is:
Assume that A is a simple abelian variety with a commutative ring of endomorphisms $End(A)$. Then there is a lift of A to an abelian variety $\mathcal{A}$ defined over a number field K which has the same ring of endomorphisms. I.e. there is a prime $\mathfrak{p}$ of K such that $\mathcal{A}$ modulo $\mathfrak{p}$ equals A and $End_K(\mathcal{A}$ modulo $\mathfrak{p})$ is canonically isomorphic to $End_{\mathbb{F}_q}(A)$.
Take for instance $A = E$ an elliptic curve. It may happen that the Π induces the multiplication with an integer. Then E is supersingular and the center of its ring of endomorphisms is isomorphic to $\mathbb{Z}$ over all extension fields.
In this case E together with its ring of endomorphisms is either not liftable or the lifting does not give non-trivial information.
(Fortunately it is very easy to determine the L-series of E for supersingular elliptic curves.)
But assume that E is not supersingular and so $End(E)$ is an order O in an imaginary quadratic field. Then (theorem of **Deuring**) there is a uniquely determined elliptic curve defined over the ring class field of O.
In practice this does not help for randomly chosen elliptic curves for the order O will have a discriminant of a size $\sim 10^{60}$ and so E is defined over a number field of degree $\sim 10^{30}$!

4.5 $p-$adic Methods

Since a lifting to a number field is hopeless in general we replace number fields by their $\mathfrak{l}_0-$adic completions. Note that at least nowadays it seems to be not avoidable that the prime number l_0 (characteristic of the residue field) occurs exponentially in the complexity but the degree n contributes as a small power factor: so this idea works (surprisingly good) for **small** l_0 (and so for large n).
Change of notation: To coincide with the usual language we call the prime number l_0 now p (and do not confuse it with group orders!).

4.5.1 Elliptic Curves: Work of Satoh

We shall give a very short sketch. Take p small, let E be an elliptic curve over $\mathbb{F}_{p^n}$. We can assume that E is not supersingular. A consequence of class field theory is that the minimal polynomial of the j-invariant of the canonical lifting $\mathcal{E}$ has (all) zeroes in the extension $W(\mathbb{F}_{p^n}) =: K_p$ of degree n of $\mathbb{Q}_p$ which is unramified with residue field $\mathbb{F}_{p^n}$.
In the first step one determines the j-invariant of $\mathcal{E}$ (in a sufficiently good $p-$adic approximation) and so $\mathcal{E}$.
Then we know that Π has a lifting to $End_{K_p}(\mathcal{E})$.

Now comes the trick: We have to compute how Π operates on torsion points (or another nice representation space). And so we can use the p-power torsion points of $\mathcal{E}$ which are in the kernel of the reduction map, i.e. which are in the formal group of $\mathcal{E}$. In this formal group we can use p-adic power series to do this (Newton-type iteration).
The only problem is that the Frobenius automorphisms is not acting in a non-trivial way on this group. But there is the dual map called **Verschiebung** which acts nicely (separably) and which has the same trace as Π (and this is all we need).
Practical remarks:

- By the theorem of Hasse we know the order of $E(\mathbb{F}_{p^n})$ up to an error term of size $2 \cdot p^{n/2}$ and so it is enough to compute everything with (easy to estimate) p-adic precision.
- In fact one does not use Π but the action of the Frobenius automorphism of $\mathbb{F}_p$ on the Weil restriction of E, and since p is small one uses explicit formulas for isogenies.
- The complexity of this algorithm is (for p fixed) of size $O(n^2)$ (needed space) and $(O(n^{5+\epsilon})$ (needed time).

  For $p = 2$ Satoh's method was re interpreted by Mestre and led to the so called AGM-method. It can be generalized to hyperelliptic curves of genus 2 and 3. It gives the most efficient way to count points on hyperelliptic curves in fields of characteristic 2.

4.5.2 Monsky-Washnitzer Cohomology

There is a theoretically more involved method which is surprisingly easy to be implemented. It was first found by Kedlaya. Related methods (relying on Dwork's theory) are published by Lauder-Wan.
A general frame can be found in the thesis of Gerkmann (2003, Essen)
The method avoids to lift abelian varieties canonically but uses a $p-$adic version of de Rham cohomolgy to find a representation space for Π. The background is the work of Monsky-Washnitzer on Lefschetz fixed points formulas on these spaces. Till now we have only discussed the case that we want to count points on abelian varieties. Now we shall count on an **affine** curve, from this it is easy to get the number of points of corresponding projective curves and then by using properties of Zeta-functions of curves and their relations to class group numbers on gets the result for the Jacobian of the projective curve.

Note: To do this for curves of genus g one has to count the points on the curve over $\mathbb{F}_{p^{gn}}$.

We assume that C is an affine curve defined over a field K of characteristic 0 with ring of coordinate ring A (e.g. $A = K[X, Y]$). If we remove finitely many points from C we get again an affine curve C_1 with coordinate ring A_1.
Let Ω_1 be the the A_1-module of holomorphic differentials on C_1. Inside of Ω_1 there is the module of exact differentials, i.e. the image of A_1 under "differentiation", denoted by B_1.

$$H^1(C_1) := \Omega_1 / B_1$$

is the first de Rham cohomology of C_1.One knows that it is a finite dimensional $K-$vectorspace.

The relevant example

Let C' be a projective hyperelliptic curve of genus g with a rational Weierstraß point which we choose as point at infinity. Let C be given as the affine part, an equation is

$$Y^2 = f(X)$$

where f is a polynomial of degree $2g + 1$.
Let C_1 be the subcurve obtained by removing the zeroes of Y.
Then

$$A_1 = K[X, Y, Y^{-1}]/(Y^2 - f(X))$$

and we can give an explicit base of $H^1(C_1)$:

$$H^1(C_1) = < X^i dX/Y; i = 0, \cdots, 2g - 1 >$$
$$\oplus < X^i dX/Y^2; i = 0, \cdots, 2g - 1 >$$

(we get a decomposition under the action of the hyperelliptic involution). Now assume that $K = K_p$ (for simplicity p odd), change notation $C \mapsto \mathcal{C}$ and assume that C is the reduction modulo p of $\mathcal{C}$.
If Π would act on $H^1(\mathcal{C}_1)$ as endomorphism we would have a good chance to use fixed point formulas of Lefschetz type to count the number of points on $C_1(\mathbb{F}_{p^n})$. This will be not possible in general but we always have an obvious action if we replace A_1 by its formal p-adic completion A_∞.
Reason: The map

$$X \mapsto X^{p^n}$$

extends to

$$Y \mapsto$$
$$Y^{p^n}((1 + (f(X)^{\Pi} - f(X)^{p^n})/f(X)^{p^n})^{1/2}$$

as series converging in the p-adic topology very rapidly.
This induces an action (explicitly given) on the de Rham cohomology of A_∞.

S. Kedlaya proved that this formal cohomology is finitely generated with the same set of generators as $H^1(\mathcal{C}_1)$.
By the Theorem of Monsky-Washnitzer we get: The fixed point theorem for Π holds on this formal cohomology group, and we are done.

4.6 Real and Complex Multiplication

We have still a gap in our counting methods. We cannot handle Jacobians of hyperelliptic curves of genus 2 and 3 over fields with "large" (i.e. p at least 11) characteristic.
The following 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.

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.

The simplest and well known case deals with **elliptic curves with complex multiplication** whose endomorphism ring is an order in a field $K = \mathbb{Q}(\sqrt{d})$ with $d < 0$.
More generally: **Class field theory** relates endomorphisms of special abelian varieties A_K to elements in orders $\mathcal{O}_K$ in CM-fields K **(Shimura - Taniyama)**.
We can determine (in principle explicitly, see example) an abelian variety A_K defined over a known finite field extension L of $\mathbb{Q}$ such that the reduction of A_K modulo (suitably chosen) prime ideals $\mathfrak{q}$ in the ring of integers of L leads to abelian varieties defined over the residue field of $\mathfrak{q}$ with known L-series. The necessary computations can be done (after a precalculation) in K!
So the calculation of A_K modulo $\mathfrak{q}$ and of $L_{A_K} \bmod \mathfrak{q}(T)$ is very fast and one variety A_K gives rise to many abelian varieties over finite fields for which we know the number of points. Even after Morain's results this method remains interesting for elliptic curves (for instance for statistical studies about the behavior of class groups), and for higher dimensions and not very small characteristic it is the most effective method known till now.

One can object that this method produces very special abelian varieties with an explicitly known lifting to a $CM-$variety over a number field. So it may be wise to make A_K complicated enough, e.g. by using only fields K whose class number is between 200 and 1000.
Examples:
1.) $g = 1$: *Class field theory* of imaginary fields applied to elliptic curves and especially to the j-invariant was implemented by *A. M. Spallek 1992* (diploma thesis) and is used in practice till today. It works very efficiently, the hardest

computational problem is the factorization of polynomials of degree ≤ 1000 over $\mathbb{F}_q$.
2.) $g = 2$: This is implemented by A.M. Spallek in her thesis, Essen 1994 , and much more efficiently, by Annegret Weng (Thesis 2001), and uses

1. *class field theory* of fields of degree 2 over real quadratic fields (non-Galois over $\mathbb{Q}$), [4]

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

3. either elimination theory to solve a system of three polynomial equations in 6 variables of degree > 1 over the ring of integers of a number field or

4. *much better:* Mestre’s method intersecting invariant forms (with one of them a conic).

The implementation of the algorithm is relatively easy, it works efficiently. We give one example:
As CM field take $\mathbb{Q}(\sqrt{-2-\sqrt{2}}$. The resulting curve is

$$C : Y^2 = X^5 - 140X^3 + 240X^2 + 3810X - 6928.$$

Reduce modulo

$$p = 153946287550700989943 \approx 1.5 \cdot 10^{20}.$$

The point

$$(7550700989929, 49, 316948239074972625 94, 860288077489211417 45)$$

on $(J_C)(\mathbb{F}_p)$ has order

$$l = 6457086864793418655053917 4412679.$$

For $g = 3$ things become more complicated.
First the invariant theory is not so well understood and the determination of the equation of the curve from the knowledge of the invariants is too complicated. The way out is to use the period matrix of the Jacobian from the beginning and Mestre’s method.
The given CM-field can be used to compute the period matrix of an abelian variety. It can be tested whether it is principally polarized and hence is the Jacobian of a curve. But the chance of finding a *hyperelliptic* curve becomes dramatically smaller if the genus increases.
One can enforce this by taking K as composite field of $\mathbb{Q}(\sqrt{-1})$ with a totally real cubic field. This is done in the thesis of Weng.

[4] to avoid non-necessary automorphisms

In future it would be nice to go away from hyperelliptic curves and to handle more general curves of genus 3.

Let us end with an an outlook which is in the moment only of theoretical interest. As explained above the main task in the construction of curves is to find the period matrix of an abelian variety which is a candidate to be the Jacobian of a hyperelliptic curve. As first source we used CM-Theory.

A second source uses **Real multiplication** (i.e. the ring of endomorphisms of A contains an order of a totally real field K with $[K : \mathbb{Q}] = \dim(A)$) and its relation with modular forms: Over $\mathbb{Q}$ the conjecture of Taniyama (proved for elliptic curves) says that we should work with abelian varieties A which are factors of the Jacobian of modular curves $X_0(N)$. For these factors we know by work of Shimura how their period matrices are related to cusp forms.

To use the Jacobians of the constructed curves for cryptography one needs their L-series over residue fields. In other words one needs the **local factors** of the global L-series. Again the theory of cusp forms and their relation to representations of the Galois group of $\mathbb{Q}$ becomes crucial:

For all prime numbers l not dividing N there are special endomorphisms, Hecke operators T_l, of A, and knowing T_l is as good as knowing the Frobenius π_l because of the **Eichler-Shimura relation**:

$$\pi_l^2 + T_l \pi_l + l = 0.$$

So the fast computation of T_l is crucial both for the computation of the period matrix and for the local L-series of A. In fact the computation of the period matrix is not difficult for $N \leq 10000$ but the complexity to compute T_l is $O(l \cdot log(l)$ and so one does not reach cryptographically interesting regions directly.