Applications of Arithmetical Geometry to Cryptographic Constructions

Gerhard Frey *

Institut für Experimentelle Mathematik
Universität GH Essen, Ellernstr. 29, 45326 Essen (Germany)
email: frey@exp-math.uni-essen.de

Abstract. Public key cryptosystems are very important tools for data transmission. Their performance and security depend on the underlying crypto primitives. In this paper we describe one such primitive: The Discrete Logarithm (DL) in cyclic groups of prime order (Section 1).
To construct DL-systems we use methods from algebraic and arithmetic geometry and especially the theory of abelian varieties over finite fields. It is explained why Jacobian varieties of hyperelliptic curves of genus ≤ 4 are candidates for cryptographically "good" abelian varieties (Section 2).
In the third section we describe the (constructive and destructive) role played by Galois theory: Local and global Galois representation theory is used to count points on abelian varieties over finite fields and we give some applications of Weil descent and Tate duality.

1 Cryptographic Background

1.1 Aim

To ensure a safe environment for data exchange and data storage is a very complex task involving problems from quite different areas like engineering and computer science but also "human factors" and legal problems, and as a small but crucial component, mathematics. It is the task of mathematics to provide the particles called crypto primitives around which cryptographic protocols are developed. To estimate the security of these protocols is a difficult problem which is impossible if one cannot trust the primitives.

In the following paper we shall try to give an overview over one special but most important family of crypto primitives based on the discrete logarithm problem in groups. We shall describe how deep methods from arithmetical geometry and especially the interaction between Galois theory and algebraic

* I would like to thank the organizers for the opportunity to participate in the $\mathbb{F}_{q^5}$-conference which, because of their great expertise and warm hospitality, became a very interesting and inspiring event.

geometry over special fields can be used to construct them and to give estimates (or hints) for their reliability.

The basic ideas go back to Diffie and Hellman ([DH]). The main aim is the construction of a function f mapping the natural numbers $\mathbb{N}$ (or, in practice, a finite subset of $\mathbb{N}$) to a finite set A of $\mathbb{N}$ satisfying some "functional equations" and with the most important properties:

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

So we have to find functions f together with algorithms to evaluate them with a proven small complexity, and we have to estimate the probability for finding the inverse images by proposing possible "attacks". In contrast to the first task in almost all cases the second one cannot be solved in a satisfactory way. What we can get are estimates for this complexity from above which will lead to reject some functions f and the statement that " to our best knowledge" other functions are safe "at the moment".

Since the security of the whole crypto system depends on this rather vague statement we would feel much better if we could use for f a *one way function* in the sense of information theory, or a *trap door one way function* (for the definition cf. [MOV]).
But since we even don't know whether such functions exist we have to use what we have and to be very sensitive to new developments in technology (e.g. "quantum computers" (cf. [Sho])) and to new results in mathematics. We refer to the rather spectacular progress in recent years in factorizing numbers (by sieve methods in number fields), in counting points on elliptic curves over finite fields (cf. [Sch2] and the references therein) and in applying index-calculus methods to Discrete Logarithm Systems ([Ga] and [EG]).

Acknowledgment I would like to thank A. Enge and M. Müller for their help and the many valuable comments they gave.

1.2 Exponential and Discrete Logarithm Systems

Let A be a finite subset of $\mathbb{N}$. For normalization reasons we shall assume that $1 \in A$.
Let

$$e : \mathbb{N} \times A \to A$$

be a function satisfying a *functional equation*:
For all $n_1, n_2 \in \mathbb{N}$ one has

$$e(n_1, e(n_2, 1)) \;=\; e(n_1 \cdot n_2, e(1, 1)).$$

This is enough to organize a **key exchange:**
Two parties M_1, M_2 want to agree on a common *secret key* based on e. The communication uses a public channel.

Key exchange scheme: [1]

i) M_i chooses (as randomly as possible) a number n_i which never leaves the secure environment of M_i.
ii) M_i sends $y_i := e(n_i, 1)$.
iii) M_1 computes $e(n_1, y_2)$, M_2 computes $e(n_2, y_1)$.

Since

$$e(n_1, y_2) = e(n_1, e(n_2, 1)) = e(n_1 n_2, e(1, 1)) = e(n_2, e(n_1, 1)) = e(n_2, y_1)$$

M_1 and M_2 share the common key

$$S = e(n_1 n_2, e(1, 1)).$$

It is obvious that the secrecy of S depends on the secrecy of n_i and so on the difficulty to compute n_i from the knowledge of $y_i = e(n_i, 1)$.

So we *assume* that the function $e(n, a)$ as a function of the first variable behaves like a one way function. Then we call

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

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

For many applications one needs more "structure". For instance the *signature* of a message m can use a scheme of *ElGamal type* if we have a rapidly computable function

$$\oplus : A \times A \to A$$

which we require to be *associative*. In other words we require that A is a semigroup.

Using this associativity we define in the usual way for $n \in \mathbb{N}$ and $a \in A$

$$n \circ a$$

as the $n - 1$ fold application of $\oplus$ to a.

Remark 1.1. Of course the actual computation of $n \circ a$ uses the well known method of (for instance) developing n in the binary system and then "adding and doubling" accordingly. This bounds the number of compositions $\circ$ by 2 log n. Several variants can be used to accelerate and sometimes precalculations speed up even more.

[1] We do not go into details of how this protocol has to be refined in order to become as secure as its primitive, the function e.

Use this to define

$$e : \mathbb{N} \times A \to A$$

by

$$e(n, a) := n \circ a.$$

Obviously the function e satisfies the functional equation:
For all $n_1, n_2 \in \mathbb{N}$, $a \in A$ we have

$$e(n_1, e(n_2, a)) = e(n_1 n_2, a)$$

and especially

$$e(n_1, e(n_2, 1)) = e(n_1 n_2, e(1, 1)).$$

Signatures
Let e be as above.
e satisfies a second functional equation

$$e(n_1, a) \oplus e(n_2, a) = e(n_1 + n_2, a).$$

This equation is used for signature schemes of El Gamal type. We shall give one variant:

Aim: M wants to sign a message m in such a way that everybody can check the authenticity of m but no one can fake the contents of m or the name of M.

To *initialize* the system M chooses, again randomly and secretly, his **private key** $x \in \mathbb{N}$ and publishes his **public key** $Y := e(x, 1)$.
This number Y identifies M in public.

Signing a message M uses, in addition to the DL-system, a (publicly known) *hash function* h which maps $\mathbb{N}$ to a set of numbers of bounded size. It has to have properties similar to those of one way functions. Especially it has to be impossible in practice to construct a number z such that $h(z)$ is a given value. (For hash functions cf. [MOV].)

Signature 1.1. M chooses a second random number k and computes

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

The signed message consists of

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

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

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

Now the functional equations of e imply:

$$S = P \oplus H$$

if the signature is authentic. Otherwise it is rejected.

It is obvious that the security of the signature depends on the quality of $e(.,1)$ as one-way function, but it is easily seen that this is not enough.

Logarithms

Definition 1.2. The notation is as above.
For given a in A and $b \in \{n \circ a, n \in \mathbb{N}\}$ the **logarithm of b with respect to a** is a number $\log_a(b) := n_b \in \mathbb{N}$ with $n_b \circ a = b$.

Definition 1.3. The notation is as above. Let C be a positive real number.

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

is a **Discrete Logarithm System (DL-systems) of exponential security** C if for random elements $a, b \in A$ the computation of $\log_a(b)$ has (probabilistic) complexity [2] $\geq e^{C \cdot \log(|A|)}$.

So DL-systems with exponential security C with C not too small give rise to exponential systems. Our aim is to construct DL-systems which are candidates for exponential security 1/2.

1.3 Algebraic DL-Systems

Let $(G, \times)$ be a finite group.
For our purposes the way how to present the group elements and the composition law is essential.

Definition 1.4. A **numeration** (A, f) of G is a bijective map

$$f : G \to A$$

where A is a finite subset of $\mathbb{N}$ containing 1.
A **presentation** of an abstract finite group G is an embedding of G into a group with numeration.

[2] In the whole paper the measure for complexity is the number of needed bit-operations.

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

Define
$$\oplus : A \times A \to A$$
by
$$a_1 \oplus a_2 := f(f^{-1}(a_1) \times f^{-1}(a_2)).$$
Then for $n \geq 1$ we have
$$e(n, a) = f(n \circ f^{-1}(a))$$
as one sees easily by induction.
Especially we get: $e(n, 1) = f(n \circ g_0)$.

We want to make one thing completely clear: We require that $\oplus$ is rapidly computable *without* the knowledge of f^{-1} and that we can think of G as an abstract group (i.e. we look at it up to isomorphisms) but the security and the efficiency of the DL-System based on $\oplus$ will depend crucially on f.

We can refine our signature scheme 1.1:

Signature 1.2. Let n be the order of G. Let (A, f) be a numeration of G and $e(.,.)$ as above. The signature procedure of a sender M and a message m is as described in Subsection 1.2 except that we replace in the equation of 1.1 all numbers by their smallest positive residue modulo n:
The signature of m given by M is $(m, e(k, 1), s)$ with
$$s \equiv h(m)x + h(e(k, 1))k \bmod n$$
and $x, k, s, h(.) \in \{0, \cdots, n-1\}$.

Example 1:

We take a prime number p and the set $G := \mathbb{Z}/p$ together with its addition. Hence we deal with "the" group with p elements.
As numeration we take the map
$$f : G \to \{1, \cdots, p\}$$
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.

What about security? We can assume that $a \in \{1, \cdots, p-1\}$ and $b = e(n,a) = [na]_p$. To determine n we have to solve the equation

$$b = na + kp$$

with $k \in \mathbb{Z}$. But by using the *Euclidean algorithm* this task is done in $O(\log(p))$ operations in $\mathbb{Z}$ and so n is computed very rapidly. Hence we do not get a Discrete Logarithm System of exponential security.

Example 2: Again we take $G = \mathbb{Z}/p$. In addition we choose a prime q such that p divides $q-1$. As it is well known this implies the existence of an element $\zeta \neq 1$ in $\mathbb{Z}/q$ with $\zeta^p = 1$ (i.e. ζ is a primitive p-th root of unity). Now define for $1 \leq i \leq p$ the number $z_i := [\zeta^i]_q$ and for $\bar{i} = i + p\mathbb{Z} \in G$

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

Then f defines an injection of G into $\{1, \cdots q\}$ with $f(1 + p\mathbb{Z}) = 1$. Let A denote the image of f.

Using the addition in G we get for $a_i = f(x_i + p\mathbb{Z}) \in A$

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

As stressed above it is important that one can compute $a_1 \oplus a_2$ without knowing x_1 and x_2. For this purpose we use the rules for addition and multiplication in $\mathbb{Z}/p$ and get:

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

and

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

What about security in this system? For fixed a and random $b \in A$ we have to find n in $\mathbb{N}$ with

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

Essentially this means that 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. This explains the name "discrete logarithm" introduced above.
Indeed to our knowledge at present a system based on this numeration is quite safe though for all constants C there is a number p_0 such that for all primes $p \geq p_0$ the corresponding DL-system it not of exponential security C. The best known method to compute the discrete logarithm is "subexponential" (cf. [Od]). The suggested size of p is at least 1024 bits.

1.4 Generic Systems

In the examples in the last subsection we already had more structure available than necessary for us: The set A was the image of the numeration f of a *finite cyclic group* G. This will be so in the following sections, too.

This seems to be reasonable: The part of the numeration we use for key exchange and signatures is given by the numeration of the group generated by $f^{-1}(1)$. But it would be interesting to study whether one can win security by generating this numeration by a more complicated group like a general matrix group.

Next we used in the signature scheme 1.2 the order of G. There are crypto systems which are based on the assumption that one cannot compute this order or that one can compute it only by using a secret trapdoor function (RSA-like systems). In this paper we do not enter into these very interesting discussions but assume that the order of G and even its prime factorization are given.
An easy application (by some people called "Pohlig-Hellman attack") of the Chinese remainder theorem and p-adic expansion shows that the security of the discrete logarithm attached to G and so a fortiori of the cryptographic schemes is reduced to the difficulty to compute the DL in the subgroups of G with prime order. Hence we have to restrict ourselves to cyclic groups of order p where p is a prime number which is sufficiently large.

We can formulate the mathematical task to be solved more precisely now:
We have to find numerations f of groups $\mathbb{Z}/p$ with p large enough which satisfy:

- Time needed (probabilistically) for the computation of the logarithm in $f(\mathbb{Z}/p)$ is **exponential in** $\mathbf{log}(p)$**.**
- Time needed to write down the elements and to execute the composition $\oplus$ is **polynomial in** $\mathbf{log}(p)$**.**

But having decided to use the algebraic structure "group" in the construction of the crypto primitive "DL" we have added a lot of structure to our system. So it is important which methods are available to attack crypto systems

which use “just” groups and the resulting DL-problems. For a very interesting discussion of different types of information which can weaken the protocols we refer to [MW].
Of course the worst case is that the discrete logarithm can be computed.
Here the amazing fact is that we can do much better than brute force attacks: The Baby-Step-Giant-Step method of Shanks as well as the ρ- and λ-methods of Pollard work in every finite group. All of them have time-complexity $O(p^{1/2})$ and the methods of Pollard need very little storage space (for more details cf. [MOV]).

These attacks give a first upper bound for the optimal exponential complexity of the Discrete Logarithm in finite groups: The constant $C = 1/2$ is the best one can hope for, and so we are forced to choose p of a size near to 10^{60} instead of 10^{30}.

Our aim is to construct groups of the necessary size for which no attacks of lower complexity than these generic attacks are known.

1.5 The Index-Calculus Attack

In reality we shall have to use a concrete presentation of our group. In many examples there are elements in G which are easier to deal with, and this gives rise to the index-calculus attack.

The principle of index-calculus methods in abelian groups G is to find a “factor base” consisting of relatively few elements and to 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.
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. Typically successes give rise to algorithms for the computation of the DL in G which have **subexponential** complexity and so, for large enough order of G, the DL-systems have a poor exponential security.

The effectiveness of this approach is the reason for the large numbers of bits required for safe RSA-systems and for DL-systems based on the multiplicative group of finite fields (Example 2 in the Subsection 1.3).

In the second section we shall see more applications of this method, and in [EG] one finds a very nice discussion of the index-calculus attack in a rather general frame. The results found there explain why it is so effective in many cases.

2 Numeration by Algebraic Groups

To find the numerations we shall use algebraic groups defined over finite fields $\mathbb{F}_q$ where q is a power of a prime l_0.

2.1 Algebraic Groups

We begin by a short description of algebraic groups defined over fields K.

First of all an algebraic group $\mathcal{G}$ is an algebraic scheme with special properties: It is reduced, non-singular, noetherian, defined over K and hence can be covered by finitely many affine subvarieties (open w.r.t. the Zariski topology which is used in the following): Locally it is "given" by a system of equations of polynomials. This means that we can cover $\mathcal{G}$ by open subvarieties U_i, $i \in I$, on which we can choose coordinate functions $X_1, \cdots, X_{n_i}$ satisfying the relations

$$(F_1(X_1, \cdots, X_{n_i}) = 0, \cdots, F_{m_i}(X_1 \cdots, X_{n_i}) = 0)$$

with $F_j \in K[X_1, \cdots, X_{n_i}]$ ($m_i = 0$ is allowed) which can be glued together along $U_i \cap U_j$. One should keep in mind that the choice and the number of coordinate functions and of relations is not canonically determined by U_i.
If U_i is irreducible (w.r.t. the Zariski topology) the polynomials in the coordinate functions generate an integral domain. Its quotient field $F(U_i)$ depends only on U_i. Its transcendence degree d_i over K is the dimension of U_i.
$\mathcal{G}$ is the disjoint union of irreducible schemes called connected components. It is connected if there is only one connected component. Open non-empty subvarieties inside of one component are dense in this component. All components have the same dimension $d := \dim(\mathcal{G})$.

For extension fields L of K let $\mathcal{G}(L)$ be the set of L-rational points of $\mathcal{G}$, i.e. the set of morphisms from $\mathrm{Spec}(L)$ to $\mathcal{G}$. These points can be described explicitly in the following way:

$$\mathcal{G}(L) = \bigcup_{i \in I} U_i(L)$$

(here one has to identifiy points on different open subschemes U_i according to the glueing).
For U_i with chosen coordinate functions $X_1, \cdots, X_{n_i}$ and relations $F_1, \cdots, F_{m_i}$ we get:

$$U_i(L) = \{x \in L^{n_i},\ F_1(x) = \cdots = F_{m_i}(x) = 0\}.$$

Next there is 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

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

such that these morphisms satisfy the usual group laws. So we get

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

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

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 this means that for all extension fields L of K the set $\mathcal{G}(L)$ 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

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

Because of the Noetherian property of $\mathcal{G}$ it follows that it has only finitely many connected components, and it is a fact that the set of these components forms a finite group Z with $\mathcal{G}_0$ as neutral element. We see easily that the unique connected component of $\mathcal{G}$ which contains 0 is a subgroup scheme of $\mathcal{G}$ denoted by $\mathcal{G}_0$.

There are several reasons (both security and complexity are bad) for the fact that Z is of little interest for our cryptographic purposes, and so we shall assume from now on that $\mathcal{G}$ is connected.

Now choose an affine open subvariety U of $\mathcal{G}$ with coordinate functions $X_1, \cdots, X_n$. The morphism m induces a morphism

$$m_U : U \times U \to \mathcal{G}$$

and its image contains a non-empty open subset $V \subset U$. Take W as the inverse image of V in $U \times U$. Then m induces a map from W to V which can be written as:

$$m_W : W \to V$$

sending pairs of L-rational points $(x_1, \cdots, x_n) \times (y_1, \cdots, y_n)$ in W to

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

with $R_i \in K(X_1, \cdots, X_n, Y_1, \cdots, Y_n)$.

Remark 2.1. This is a birational description of the addition law which is enough for all cryptographic applications. (The set of points where this map is not defined is of small dimension and hence with high probability one will not run into it by chance.)
For the performance of the cryptosystem the choice of (W, m_W) is crucial; we require small n and low degree of R_i.

If we can take $U = \mathcal{G}$ then $\mathcal{G}$ is an **affine group scheme**.
The other important kind of group schemes are projective, i.e. they can be embedded into a projective space $\mathbb{P}^n/K$ and are closed in it.
They are called **abelian varieties** and will be in the center of our interest. Abelian varieties have many special properties which are not at all clear from the definition. For instance their addition law has to be **commutative**.
(This and much more of the fascinating theory of abelian varieties can be found in [Mu2].)

2.2 One-dimensional examples

1. The **additive group** G_a is the affine line. We can take one variable X as coordinate function, the relation set is empty. m is given by the function $R(X, Y) = X + Y$, $i(X) = -X$ and $e(\mathrm{Spec}(K)) = 0_K$.
   The set of $L-$rational points is L, the group structure is given by the field addition.
2. For the **multiplicative group** G_m we choose two variables X_1, X_2 and the relation $X_1X_2 - 1 = 0$. So as variety G_m is a curve in the affine plane. The "addition" m is given by
   $$(R_1(X_1, X_2; Y_1, Y_2) = X_1Y_1, R_2(X_1, X_2; Y_1, Y_2) = X_2Y_2),$$
   $i(X_1, X_2) = (X_2, X_1)$ and $e(\mathrm{Spec}(K)) = (1_K, 1_K)$. The group of L-rational points is isomorphic to L^*.
3. **Elliptic curves** E
   They are the simplest examples for abelian varieties and at the same time, the most important ones in theory and applications today. Only for the sake of simplicity we shall assume here that $\mathrm{char}(K)$ is not equal to $2, 3$ (see [Si] for the general case).
   Like in 2.) we use a curve as underlying scheme. But this time it is a curve in the projective plane given by one cubic equation.
   If we use homogeneous coordinates (X, Y, Z) the relation is
   $$R(X, Y, Z) = Y^2Z \;-\; X^3 \;- AXZ^2 \;- BZ^3$$
   with $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$. As an affine open set we can take U_f given by the inequality $Z \neq 0$. Taking $Z = 1$ in U_f and (ab-)using X, Y as affine coordinates we get the affine equation
   $$Y^2 \;=\; X^3 + AX + B$$

for U_f.
The birational version of the addition $m =: \oplus$ is given by the well known addition formulas for elliptic curves: For

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

we get

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

with (in general):

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

and y_3 such that $(P_1, P_2, (x_3, -y_3))$ are collinear. The inversion is defined by $i(x, y) = (x, -y)$. The neutral element is not inside of U_f: We get in homogeneous coordinates: $e(\mathrm{Spec}(K)) = (0, 1, 0) =: \infty$, this is the one point in $E(K) \setminus U_f(K)$.

2.3 Birational Numeration

We come back to our task of finding "good" numerations of $\mathbb{Z}/p$. We want to use algebraic groups $\mathcal{G}$ over finite fields $\mathbb{F}_q$. So we first choose (and fix) a numeration of elements of $\mathbb{F}_q$ which provides a numeration of $\mathbb{F}_q^n$ (for instance by the lexicographical order). Next we choose coordinate functions for open affine subvarieties U of $\mathcal{G}$ as described above and get numerations of $U(\mathbb{F}_q)$ depending on these functions. If we want we can use a covering of $\mathcal{G}$ by affine parts U_i to get a numeration of $\mathcal{G}(\mathbb{F}_q)$ but for most applications this will not be necessary (cf. Remark 2.1). Again we stress that there is no canonical way to get such a numeration and a big part of the implementation of a DL-system consists of finding a good numeration (even for $\mathbb{F}_q$).
Now let

$$\alpha : \mathbb{Z}/p \to \mathcal{G}(K)$$

be a non-trivial homomorphism. Then α induces a numeration f_i of $\mathbb{Z}/p \cap \alpha^{-1}(U_i(\mathbb{F}_q))$ in a natural way and the related map $\oplus_i =: \oplus$ is given by the rational functions defining the group law of $\mathcal{G}$ on U_i. The *existence* of α is equivalent with the existence of $\mathbb{F}_q-$rational points P on $\mathcal{G}$ with order p, and one such α can be explicitly given if one point P_0 of order p is known.

From now on we take $\mathcal{G}$ as connected and commutative.

Remark 2.2. It may be be worthwhile to look for other possibilities, e.g. matrix groups, but then structural properties of such groups like the theorem of Maschke about semi-simplicity of representations of groups with order prime to $char(\mathbb{F}_q)$ have to be taken into account.

A well known structure theorem about commutative and connected algebraic groups yields that without loss of generality we can assume that $\mathcal{G}$ is either an affine group or an abelian variety. Moreover affine connected algebraic commutative groups can be built up by unipotent groups and tori. Unipotent groups have composition factors isomorphic to G_a, and tori are up to twists products of copies of G_m. So essentially we can try to use copies of G_m and G_a and abelian varieties for our purposes.
It is easily seen that G_a leads to Example 1 and G_m to Example 2 in Subsection 1.3 . So we shall concentrate in the following on discussing numerations induced by abelian varieties.

2.4 Admissible Abelian Varieties

It is now clear that we have the

Aim 2.1. Construct **explicitly** abelian varieties $A/\mathbb{F}_q$ satisfying simultaneously

1. A (large) prime p divides $|A(\mathbb{F}_q)|$ and
$$\log p \approx \log(|A(\mathbb{F}_q)|) \approx \dim(A) \cdot \log q (cf. \text{Theorem } 3.3).$$
2. To store a point $P \in A(\mathbb{F}_q)$ one needs only $c_1(\log(p))$ bits of space and to compute $\oplus$ only $c_1(\dim(A)^k)$ operations in $\mathbb{F}_q$ with c_1, c_2, k small (e.g. $c_1 = 1 + \epsilon, k = 2$).
3. All **known** algorithms for the computation of the discrete logarithm in $A(\mathbb{F}_q)$ have a large enough probabilistic exponential complexity.

In practice we require that $p \geq 10^{60}$ and the exponential constant is $1/2$.

We call abelian varieties satisfying these conditions **"admissible"**.

The embedding of $\mathbb{Z}/p$ into $A(\mathbb{F}_q)$ induces a lot of additional structure from arithmetic geometry in the corresponding DL-system: We can use

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

and, most importantly, **Galois theory** related to these objects.

These theories give tools for constructions, but also for possible (or at least conceivable) attacks.

2.5 Manageable Abelian Varieties

The first task to solve is to describe (birationally) abelian varieties and the addition laws in a time and space saving way.
This seems to be hopeless as long as we work with **general** abelian varieties A: The number of coordinate functions and the degree of the addition formulas both grow exponentially with the dimension of the abelian variety (cf. results of Mumford [Mu1] and Lange-Ruppert [LR]) and so we have to use **special** abelian varieties.
The first specialisation is to take A as Jacobian variety J_C of a curve C.
The big advantage is that both the coordinates and the addition can use objects defined by C since

$$(C \times \ldots \times C)/S_g \quad (g = \text{genus}(C),\ S_g \text{ the symmetric group in } g \text{ letters})$$

is birationally isomorphic to J_C and the points of J_C correspond to divisor classes of degree 0 of the function field of C. We can assume that we have an $\mathbb{F}_q-$rational point P_∞ on C. The theorem of Riemann-Roch implies that we find "standard " representatives in divisor classes of the form $D - g\,P_\infty$ with D a positive $\mathbb{F}_q-$rational divisor of degree g (i.e. a formal sum of g points of C).
The addition in J_C is induced by the addition of divisors and the task is to find in the class of the sum of two divisors standard representatives either by formulas or by an algorithm involving the coordinates of the points occurring in the added divisors. So we need an effective (and very fast) version of the Riemann-Roch theorem.
We consider the following situation: We assume that there is a cover

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

in which a non singular point (P_∞) is totally ramified and induces the place $(X = \infty)$ in the function field $\mathbb{F}_q(X)$ of $\mathbb{P}^1$.
It is an easy exercise to show:

Proposition 2.3. *Let S be the normal closure of $\mathbb{F}_q[X]$ in the function field of C, $J(S)$ its ideal class group. Then:*

$$J(S) \cong J_C(\mathbb{F}_q)$$

This allows to present points on $J_C(\mathbb{F}_q)$ by ideals in S and hence as d-tuples of polynomials in $K[X]$ whose degree is bounded by g. The addition on J_C is reduced to linear algebra and interpolation. The space needed to write down elements of $J_C(\mathbb{F}_q)$ is $O(d \cdot g)$.
There are promising examples of curves with $d = 3$, but here we restrict ourselves to $\mathbf{d = 2}$, i.e. to **hyperelliptic curves**.

Corollary 2.4. *Assume that C is a hyperelliptic curve over $\mathbb{F}_q$ having an $\mathbb{F}_q$−rational Weierstraß point P_∞. Let C be given by a separable, monic polynomial $f(X,Y)$ of degree 2 in Y such that $(X)_\infty = 2P_\infty$.*
Then $J_C(\mathbb{F}_q)$ is isomorphic to the ideal class group of $S = \mathbb{F}_q[X,Y]/f$.
The isomorphism is canonical if we fix P_∞ and the birational morphism from $(C \times \cdots \times C)/S_g$ to J_C.

Artin has generalized Gauß 's theory of ideal classes of imaginary quadratic number fields to hyperelliptic function fields connecting ideal classes of S 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**. In both cases we need an efficient arithmetic in polynomial rings over $\mathbb{F}_q$ (and nothing more).

Implementations of both variants and data concerning the performance can be found in [Sp] (for $g = 2$) and in [Kr] in general. It is not surprising that for elliptic curves the formulas are faster than the algorithm, for genus 2 both methods seem to be equivalent, and for higher genus the algorithm is the only feasible variant.
Using these algorithms it turns out that the computing time for an addition grows like twice the genus of C and so elliptic curves are optimal. But this assertion is a little bit unfair: For $g = 1$ a lot of work has been invested to get a "best implementation", for $g \geq 2$ we did not optimize the algorithm. Moreover we shall see below that the bit size of $J_C(\mathbb{F}_q)$ grows linearly with the genus and so we can realize a large group over a relatively small field and so we may take advantage of special features of the hardware configuration.

2.6 The Index-Calculus Attack on Hyperelliptic Curves

But we have to pay a price: We have left the abstract realm of abelian varieties and we use the ideal class groups of orders S over the polynomial ring in one variable for the DL-system. This approach is well known in the analogous situation in number theory, and there exists a subexponential attack based on the index-calculus principle.

So it is not surprising that we are confronted with the same kind of attack in the geometric situation, too.

The general principle of the index-calculus attack was described in Subsection 1.5. One of the essential parts of it is the choice of a factor base.

The ideal classes of S can be represented by polynomials of degrees bounded by $g = g(C)$. This suggests a rather natural way of choosing a factor base for the index-calculus attack: Take the ideal classes which can be represented by polynomials of small degrees as factor base!

It is to be expected that (for fixed field $\mathbb{F}_q$) this method becomes more and more effective with increasing g. And indeed Adleman, DeMarrais and Huang ([ADH]) proposed an index-calculus algorithm for hyperelliptic curves with subexponential complexity in g. This was made precise in [MST] and [E] and finally settled by a smoothnessness result in [ES]:

Proposition 2.5. *([E]) 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 $L_{q^g}[\frac{5}{\sqrt{6}}((1+\frac{3}{2t})^{1/2}+(\frac{3}{2t})^{1/2})]$.*

For the definition of the subexponential function L we refer to [E] and we do not go into more details since this result predicts the behaviour of the DL-systems for fairly large g which is not in the center of our (practical) interest.
But we notice that because of this result (and, by the way, because of the difficulty of finding hyperelliptic curves for which we can count points on their Jacobian) we have to restrict ourselves to small g (≤ 7 in the range of security parameters used today) if we want to have secure DL-systems.
In a new paper of Gaudry (cf. [Ga]) things become more serious for practical use: For hyperelliptic curves of relatively small genus (in practice: $g \leq 8$) with known structure and order of the group of $\mathbb{F}_q$−rational points of their Jacobian variety one can proceed in a much simpler way: It is "easy" (with complexity $O(q\log(q))$ to decide whether a positive divisor of degree $\leq g$ is a sum of divisors of degree 1 (i.e. of $\mathbb{F}_q$−rational points of C) and if this is the case one gets the explicit expression of this sum with the same time complexity (probabilistically). (One has to factorize polynomials of degree g over $\mathbb{F}_q$.) On the other side such an event occurs with probability $\approx 1/g!$. Using this Gaudry (cf. [Ga]) succeeds to prove:[3]

Theorem 2.6. *Assume that C is a hyperelliptic curve of genus $g \leq 8$ defined over $\mathbb{F}_q$ such that $|J_C(\mathbb{F}_q)|$ is known.*
Then the DL in $J_C(\mathbb{F}_q)$ can be computed with complexity $O(q^2(\log(q))^\gamma)$, with "reasonable small" constants.

Of course by this result only a specific presentation of $\mathbb{Z}/p$ as subgroup of the group of rational points of J_C is attacked, but since we do not know a different manageable presentation till now we get the

[3] A more precise formulation of the result and examples can be found in the paper of Gaudry, for a general point of view cf. [EG].

Result: The Jacobian varieties attached to hyperelliptic curves of genus ≤ 4 or closely related abelian varieties [4] are the only known candidates for admissible abelian varieties.

Remark 2.7. It is obvious that Gaudry's method works in all situations in which we embed $\mathbb{Z}/p$ into the ideal class group of an order over a polynomial ring in which addition is made effective by a "reduction theory".

3 Galois Theory

3.1 Counting Points

In order to use manageable abelian varieties A of dimension d for DL-systems 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. We can exploit a rich theory due to Hasse, Weil, Tate and others.

The absolute Galois group G_q of $\mathbb{F}_q$ is topologically generated by the **Frobenius automorphism** π_q which maps elements of $\overline{\mathbb{F}}_q$ to their $q-$th power.

Let n be a natural number. For all numbers n π_q acts on the points $A(\overline{\mathbb{F}}_q)[n]$, the group of elements of $A(\overline{\mathbb{F}}_q)$ whose order divides n. Hence it induces a linear map on $A(\overline{\mathbb{F}}_q)[n]$ which is, if n is prime to char(K), as $\mathbb{Z}/n$–module isomorphic to $(\mathbb{Z}/n)^{2d}$.

Fact (Weil):
The characteristic polynomial of π_q w.r.t. this action is the reduction modulo n of a monic polynomial with integer coefficients of degree $2d$. This polynomial is independent of n and is called the **L-series** $L_A(T)$ of A over $\mathbb{F}_q$.

Since $A(\mathbb{F}_q)$ is the kernel of the map $\pi_q - id$ we get by elementary linear algebra:

Proposition 3.1. $|A(\mathbb{F}_q)| =| L_A(1) |$.

A trivial but crucial consequence is:

Corollary 3.2. *$\mathbb{Z}/p$ is embeddable into $A(\mathbb{F}_q)$ iff $L_A(1) \equiv 0 \, mod p$.*

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

[4] for instance factors or abelian varieties constructed by Weil descent (cf. Section 3.2)

Theorem 3.3.

$$\dim A \cdot \log q \approx \log |A(\mathbb{F}_q)|.$$

Conclusion: Task 2. of Aim 2.1 can be solved if we can find enough manageable abelian varieties A of dimension d for which we can

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

The second item can be discussed by **global Galois theory** using analytic and algebraic number theory. These theories provide tools like effective versions of Chebotarev's density theorem and conjectures about the distribution of traces of Frobenius elements (Lang-Trotter) and about the distribution of class groups generalizing heuristics of Cohen-Lenstra. Recent interesting work on these topics can be found in [Mur].

We shall present some methods to solve the first item. They all use more or less sophisticated properties of L-series and Frobenius automorphisms.

1.) 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 [5]. 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_q 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 3.4. *Let the notation be as above.*
Let p be a prime larger than $\mid A(\mathbb{F}_{q_0}) \mid$. Then $\mathbb{Z}/p$ is embeddable into $A(\mathbb{F}_q)$ iff p divides

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

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

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

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.

So mostly the method of constant field extensions is used only for very small q_0 and large prime m. The typical examples are Koblitz curves defined over fields with 2-power order (cf. [Ko]).

In Subsection 3.2 we shall present another method to construct admissible abelian varieties using constant field extensions in the situation that q_0 is as big as possible and m small. It uses the observation stated in

Proposition 3.5. *Let $A_0(\mathbb{F}_q)$ denote the subgroup of $A(\mathbb{F}_q)$ annihilated by the trace map*

$$Tr_{\mathbb{F}_q/\mathbb{F}_{q_0}} = \sum_{j=0,\cdots,m-1} \pi_{q_0}^j.$$

Then

$$|A_0(\mathbb{F}_q)| = \prod_{i=1,\cdots,2d} (1-\omega_i^m)(1-\omega_i)^{-1}.$$

The proof of the proposition uses the fact that the trace map is a surjective homomorphism from $A(\mathbb{F}_q)$ to $A(\mathbb{F}_{q_0})$.

2.)Schoof's Algorithm:
Remember: $L_A(T)$ is a polynomial with integral coefficients which simultaneously for all natural numbers n is the characteristic polynomial of π_q acting on torsion points of order n of A. Since it has integral coefficients (of size depending on q and $\dim(A)$ only) it is determined by this action for small n.

This is the starting point of Schoof's algorithm (cf. [Sch1]) 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 (cf. [Si], p.105).

Theorem 3.6. (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 (cf. [Ka]) 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* (cf. [Si] p.100 ff)). 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. We recall as the most spectacular result the proof of Fermat's Last Theorem by Wiles which was obtained by proving the Taniyama conjecture for elliptic curves.
Our interest are 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 ([Mo]):

Proposition 3.7. *(cf. [Mo]) 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
$O((l^2 \cdot \log(q))^{1+\epsilon})$ *operations in $\mathbb{F}_q$.*

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 3.7 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 the Generalised Riemann Hypothesis (GRH) it can be proved[6] that the bound $O((\log(q))^2)$ (with explicitly computable constants) is big enough.
So we get

Theorem 3.8. *Assume that GRH is true. Let ϵ be a positive real number. Let E be an elliptic curve defined over $\mathbb{F}_q$.*

[6] We thank K. Murty and R. Murty for the communication of this result (e-mails February 2000).

The order of $E(\mathbb{F}_q)$ can be computed with (probabilistic) complexity $O((\log(q))^\delta)$ with $\delta \leq 6+\epsilon$ and conjecturally $\delta \leq 4+\epsilon$ operations in $\mathbb{F}_q$.

Using this theorem and taking into account the predictions on the structure of $E(\mathbb{F}_q)$ we can solve Task 1. and Task 2. of Aim 2.1 for **random** elliptic curves in a range which is sufficient for cryptography.

Real and Complex Multiplication
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.

1.) We use the arithmetic theory of the Galois groups of special number fields K (called **CM-fields**) which are totally imaginary quadratic extensions of totally real number fields.

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)** ([ST]):
We can determine (in principle explicitly, see examples) 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 $A_K \bmod \mathfrak{q}$ 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 Task 1. and Task 2. of Aim 2.1 are solved. 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 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 (cf. [Si], pp.338 ff) was proposed by Atkin and 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 uses

1. *class field theory* of fields of degree 2 over real quadratic fields (non-Galois over $\mathbb{Q}$), [7]
2. *Invariant theory* which is explicit and "easy" (cf [Ig]) 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, cf. [Me]).

The implementation of the algorithm is relatively easy, it works efficiently. We give one example computed by Spallek in 1993:

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

$$(7550700989929, 49, 31694823907497262594, 86028807748921141745)$$

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

$$l = 6457086864793418655053917441267 9.$$

For $g \geq 3$ 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 (cf. [Mu3]). But a principally polarized abelian variety of dimension ≥ 4 need not to be the Jacobian of a curve (Schottky problem) and even if so, the chance of finding a *hyperelliptic* curve becomes dramatically smaller if the genus increases.
In his thesis (Essen 1995)(cf. [We]) Weber used results of Mumford and Poor and succeeded in overcoming the computational difficulties for $g \leq 5$. He implemented an algorithm which decides whether a given period matrix belongs to a hyperelliptic curve and if so, computes the equation of the curve. He applied his algorithm to abelian varieties with real multiplication (see below) and found, as expected, many examples with $g = 3$, some with $g = 4$ and only one with $g = 5$ (which is a modular curve) [8].

[7] to avoid non-necessary automorphisms

[8] In view of Gaudry's result 2.6 this is sufficient for cryptographic applications.

2.) 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 $\mathbb{Q}$ (cf. [Sh]) 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.
By methods of Basmaji (thesis Essen 1996) [Ba] and M. Müller this can be done for $N \leq 10000$ and $l \leq 10^{11}$.

Example (Weber) Take $N = 284$. The *new part* of $J_0(284)$ has dimension 6 and splits into two simple factors of dimension 3, one of them, A_f, corresponds to the cusp form f determined by

$$f = q + \beta q^3 + (-\beta^2 - 3\beta - 1)q^5 + \ldots$$

with $\beta^3 + 3\beta^2 - 3 = 0$.
A_f is the Jacobian of the curve

$$Y^2 = X^7 + 3X^6 + 2X^5 - X^4 - 2X^3 - 2X^2 - X - 1.$$

This curve has good reduction modulo primes l which do not divide N and so the same is true for A_f. We denote this reduction by $A_f^{(l)}$. Using Basmaji's algorithm one can compute the Hecke operator T_l and so the order of $A_f^{(l)}(\mathbb{Z}/l)$ for primes up to 10^{11}. The size of this group is $\approx 10^{33}$ which is too small for DL-systems. But we hope that we can combine this construction with Weil descent methods (Subsection 3.2) to find interesting candidates for DL-systems.

3.2 Weil Restriction

We recall that one of the methods to determine the L-series of abelian varieties A of dimension d was related to constant field extensions. More generally one can look at the situation that $q = l_0^f$ with $f \leq 2$. Hence we have the Frobenius automorphism π_{l_0} acting non-trivially on $\mathbb{F}_q$. One may ask what *geometric* consequences this has for abelian varieties A defined over $\mathbb{F}_q$ and whether there are hidden structures which weaken the DL.

In [Fr] I have suggested that one should study the geometric method of restricting scalars (Weil-descent) at least in special cases.

Scalar Restriction Here is a short description of this procedure (for a detailed exposition and the strict geometric construction cf. [Na]):

Take a field K and a finite separable field extension L/K. Let V be a quasi-projective variety (i.e. V can be embedded into a projective space) defined over L.
Then there is a quasi-projective variety W_V defined over K with
$W_V(K) = V(L)$ and $W_V \times L \simeq V^{[L:K]}$.

The recipe for the construction of W_V for affine V is:
Choose coordinate functions $X_1, \cdots, X_n$ of V over L and a basis $(u_1, \cdots, u_m)$ of L/K. Define the $n \cdot m$ variables $Y_{i,j}$ by

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

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

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

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

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

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

So the DL-problem on $A/\mathbb{F}_{q^m}$ is equivalent with the DL-problem on the $m \times d-$dimensional abelian variety W_A over $\mathbb{F}_q$. But W_A has more geometric structure: We find $\mathbb{F}_q$-rational subvarieties like curves and hypersurfaces on W_A which are not on A.

It seems that "in general" these subvarieties are rather complicated. For instance take an elliptic curve E. Then "in general" one expects that the minimal genus of curves on W_E is $\approx 2^m$ and so at least till now we cannot apply this additional information (positively or negatively) to the DL-problem if m is large. But for small m or special fields $\mathbb{F}_q$ one has to expect a different picture.

Here is one such example. It is due to Gaudry, Hess and Smart (cf. [GHS]).

Theorem 3.9. *Take $q = 2^n$ and m prime to n. Let E be an elliptic curve defined over $\mathbb{F}_{q^m}$ and assume that E is not defined over a proper subfield of $\mathbb{F}_{q^m}$. Assume that $\mathbb{Z}/p$ can be embedded into $E(\mathbb{F}_{q^m})$.*
Then there is an (explicitly given) embedding of $\mathbb{Z}/p$ into the Jacobian variety of a hyperelliptic curve C of genus $\leq 2^{m-1}$ defined over $\mathbb{F}_q$ such that the discrete logarithm problems (corresponding to these embeddings) of $\mathbb{Z}/p$ in $E(\mathbb{F}_{q^m})$ and in $J_C(\mathbb{F}_q)$ are equivalent.

The proof of this theorem uses Weil descent applied to E from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ and constructs on (an affine part of) W_E a hyperelliptic curve by using a convenient basis of $\mathbb{F}_{q^m}/\mathbb{F}_q$ and hyperplane sections.

Typically for our present knowledge about Weil descent are the applications of this result:

1.) If m is too large (e.g. ≥ 7) the resulting objects (here the hyperelliptic curves) are too complex to be used.

2.) If m is small (here $m \leq 3$) we can use the Weil descent to produce new admissible abelian varieties, here Jacobians of hyperelliptic curves C: By construction we know that the group of $\mathbb{F}_q-$rational points on J_C contains a subgroup of order p if the elliptic curve E we begin with has such a subgroup in $E(\mathbb{F}_{q^m})$.

3.) In a medium range ($4 \leq m \leq 6$) the discrete logarithm system attached to E is weakened.
This follows from Theorem 2.6 at least for $m \geq 5$. Numerical experiments made in [GHS] rise the suspicion that the same is true for $m = 4$.

The work of Gaudry, Hess and Smart is a clear signal to designers of DL-systems based on elliptic curves:

The degree d of the finite field over its prime field over which the numeration of $\mathbb{Z}/p$ is realized should be equal to $k \cdot l$ where l is a large prime and $k \leq 3$.

In Theorem 3.9 it is assumed that E is not defined over a proper subfield. One reason for this is the following fact:

Proposition 3.10. *Assume that A is a simple abelian variety defined over $\mathbb{F}_{q^m}$. In general A is defined over a proper subfield of $\mathbb{F}_{q^m}$ iff W_A is not a simple abelian variety over $\mathbb{F}_q$.*
Here "in general" means that we can give (for any dimension of A and given m) a complete list of the exceptions.

For details and the explicit discussion of the case that A is an elliptic curve we refer to [Na].

Trace-0-Variety Assume now that A **is** defined over $\mathbb{F}_q$. We continue to assume that A is simple. Again in general W_A has two (over $\mathbb{F}_q$) irreducible abelian subvarieties. One of them is isomorphic to A, we call the other one B.

B has dimension $d(m-1)$ and is the kernel of the **trace projection** morphism which is the sum of the first m powers of the Frobenius automorphism. Its L-series over $\mathbb{F}_q$ is equal to the L-series of $A \times \mathbb{F}_{q^m}$ divided by the L-series of A over $\mathbb{F}_q$ and so (up to points of order dividing m) we get rid of points of A with coordinates in $\mathbb{F}_q$.
Of course this procedure is closely related to the method of constant field extensions we described in Subsection 3.1. But we have set the right geometric context for this method by interpreting the points of $A(\mathbb{F}_{q^m})$ lying in the kernel of the trace map as $\mathbb{F}_q$−rational points of an abelian variety B defined over $\mathbb{F}_q$.

As one positive consequence we can reduce the key length.
There is a second advantage: The addition on B is induced by the group law of $A/\mathbb{F}_{q^m}$ but multiplication by numbers k have shorter expressions if developed w.r.t. powers of the Frobenius automorphism (cf. analogous advantages of Koblitz curves).
This speeds up the addition considerably and so one can expect that for small m we find new admissible abelian varieties of higher dimension by using "small" abelian varieties over $\mathbb{F}_q$ which are manageable but not secure. Below we describe in detail an example.

Example The Weil descent of elliptic curves with $m = 4$ was worked out by Galbraith and Smart in [GS].

We take $m = 3$ and $A = E$ an elliptic curve given by the equation

$$Y^2 = X^3 + AX + B.$$

We are interested in the case that q is odd.
We assume that $q \equiv 1 \mod 3$. So we can use Kummer theory to describe $\mathbb{F}_{q^3}$: Let μ be an element of $\mathbb{F}_q$ which is no third power and ζ be an element of $\mathbb{F}_{q^3}$ with $\zeta^3 = \mu$. So $(1, \zeta, \zeta^2)$ is a basis of $\mathbb{F}_{q^3}/\mathbb{F}_q$.

We choose coordinates for the Weil descent

$$Y = y_0 + y_1\zeta + y_2\zeta^2$$

$$X = x_0 + x_1\zeta + x_2\zeta^2$$

and plug this into the equation of the elliptic curve E:

$$(y_0 + y_1\zeta + y_2\zeta^2)^2 =$$

$$= (x_0 + x_1\zeta + x_2\zeta^2)^3 + A(x_0 + x_1\zeta + x_2\zeta^2) + B.$$

This produces three equations over $\mathbb{F}_q$:

$$y_0^2 + 2\mu y_1 y_2 = x_0^3 + \mu x_1^3 + \mu^2 x_2^3 + 6\mu x_0 x_1 x_2 + Ax_0 + B,$$

$$2y_0 y_1 + y_2^2\mu = 3x_1^2 x_2 \mu + 3x_0^2 x_1 + 3x_0 x_2^2 \mu + Ax_1$$

and

$$2y_0 y_2 + y_1^2 = 3x_1 x_2^2 \mu + 3x_0^2 x_2 + 3x_0 x_1^2 + Ax_2$$

which describe an open affine part of W_E.

Now we want to determine the subvariety B given by the condition

$$\mathrm{Trace}(\pi_q) = 0.$$

We find on B the relations:

$$3x_0 = \left(\frac{y_1}{x_1}\right)^2 = \left(\frac{y_2}{x_2}\right)^2 = \frac{y_1 y_2}{x_1 x_2}.$$

Hence we get one equation:

$$(3x_1 x_2 \mu + 3x_0^2 + A)^2$$

$$= 12x_0(x_1^3\mu + x_2^3\mu^2 + x_0^3 + Ax_0 + B).$$

which together with the relation

$$y_0^2 = x_0^3 + \mu x_1^3 + \mu^2 x_2^3 + Ax_0 + B$$

describes an open affine part of B.
We find curves on B by intersecting by hyperplanes, e.g. we choose $x_0 =$ const.
In general these curves will have genus ≥ 4 but for the special choice

$$x_0 = 0$$

we find a hyperelliptic curve with equation:

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

with $y = y_0 x_1^2$.

This curve[9] has genus 3. Its Jacobian has a factor which is isogenous to B and hence is manageable if $E/\mathbb{F}_q$ is manageable. In [Na] one finds choices of E, q which lead to rather good DL-systems.

Next assume that q is a power of 3. Take $m = 3$ and an elliptic curve given by

$$E : Y^2 = X^3 + AX^2 + B.$$

We generate $\mathbb{F}_{q^3}$ by an element α satisfying the equation

$$\alpha^3 - \alpha = a.$$

By analogous computations as above Diem finds the curve

$$y_0^2 = A^{-3}x_1^6 + ax_1^3 + Ax_1^2 - A^2x_1 + aA^3 + A^{-1} + B$$

on $B/\mathbb{F}_q$ which has genus 2.

One could speculate that as in the case exposed in [GHS] Weil descents of degree $m \geq 5$ can weaken DL-systems over $\mathbb{F}_{q^m}$.

[9] This curve as well as the next one have been found by C. Diem.

3.3 Tate Duality and Brauer Groups

The Tate Pairing In the last subsections we have already seen how the operation of Galois groups plays a key role (constructively and partly destructively) for the realization of discrete logarithm systems. In the center (even in the global constructions via CM-theory or modular varieties) were the Frobenius automorphisms.

In this subsection we shall describe a duality structure intrinsically related to abelian varieties over local and global fields for which ramified extensions play an essential role, too. Applications of this duality can be seen as prototypes of "lifting attacks". Typically we shall not only lift abelian varieties and points on them from finite fields to $\mathfrak{l}-$adic fields and global fields but also use Galois cohomology groups related to these liftings which become trivial over finite fields.

We begin with the general setting. Let K be a field and A a (principally polarized) abelian variety over K, n prime to char(K). Let M be a $\mathbb{Z}-$module. By $M[n]$ we denote the subgroup of M consisting of the elements of order dividing n.
Let K_s be the separable closure of K and $G_K = \mathrm{Aut}(K_s/K)$ the absolute Galois group of K.
G_K acts continously on $A(K_s)$ and we have the exact sequence of G_K-modules (Kummer sequence)

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

Application of Galois cohomology gives the exact sequence

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

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

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

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

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

For computational reasons it is important that **Lichtenbaum** [Li] gave a definition of $<,>_K$ in the case that A is the Jacobian of a curve C which uses functions and points on C for the computation of $<,>_K$ (see 3.3).

The group $H^2(G_K, \mu_n)$ is very important for the arithmetic of K: It consists of the elements of order dividing n of the **Brauer group** $Br(K)$ of K. 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.

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

If K is an $\mathfrak{l}-$adic field (i.e. K is a finite algebraic extension of the field of $l-$adic numbers $\mathbb{Q}_l$) the Brauer group of K is canonically isomorphic to $\mathbb{Q}/\mathbb{Z}$, the isomorphism is given by the so called **invariant map** inv_K. This and the explicit determination (called Artin's reciprocity law) of the invariant are the key to **local class field theory** (cf. [Ne]): One can describe the Brauer group of K by using cocycles defined by cyclic extensions L of K of degree n in the following way:

Theorem 3.11. *Let K be an $\mathfrak{l}-$adic field with normed valuation $v_{\mathfrak{l}}$. Let L/K be a cyclic extension of degree n and let τ be a generator of its Galois group.*

i) $Br(K)[n] = H^2(G(L/K), L^*)$.

ii) $H^2(G(L/K), L^*)$ is generated by the cohomology classes of the 2-cocycles γ defined by

$$\gamma(\tau^i, \tau^j) = a \in K^* \text{ if } i + j \geq n$$

and

$$\gamma(\tau^i, \tau^j) = 1 \text{ otherwise.}$$

iii) Two cocycles γ and γ' are in the same class iff the corresponding elements a and a' satisfy:

$$a \cdot a'^{-1} \in N_{L/K}(L^*).$$

iv) Let L/K be unramified of degree n and let τ be the automorphism of L/K which induces the Frobenius automorphism of the residue field extension. Then

$$\mathrm{inv}(c) = v_{\mathfrak{l}}(a)/n \bmod \mathbb{Z}.$$

There are two problems if one wants to use Theorem 3.11 to compute the invariant function in the Brauer group of K:

1.) In general a cohomology class in $Br(K)[n]$ is not given as a cocycle of an unramified extension. We shall see below that in the cases of interest for us we have to deal with ramified cyclic extensions L/K.
2.) Even if c is given by an unramified field extension L/K the given generator of $G(L/K)$ need not be the Frobenius automorphism.

In both cases one checks that in order to compute $\mathrm{inv}(c)$ we have to compute discrete logarithms in the residue field of L. (Details of these considerations will be found in [Ng]). Hence there is a close connection between the discrete logarithm in this residue field and $Br(K)[n]$ which is especially easy in the following case:

Proposition 3.12. *Assume that n is a number prime to the characteristic of the residue field k of K and that L/K is a totally ramified Galois extension of degree n. Then $Br(K)[n]$ is isomorphic to $H^2(G(L/K), L^*)$ and the DL-problem in the group $k^*[n] = \mu_n$ is equivalent with the DL-problem in $H^2(G(L/K), L^*)$ and hence with the computation of the invariant.*

Proof: L/K is tamely ramified by assumption and hence by Hilbert theory (cf. [Ne]) it is a cyclic extension and the $n-$th roots of unity are contained in k. Hence there is an element π in K with $v_{\mathfrak{l}}(\pi) = 1$ such that $L = K(\pi^{1/n})$ and so π is in the image of the norm map from L to K. By this and Hensel's lemma we see that $N_{L/K}(L^*)$ is isomorphic to k^*/k^{*n}. Now use Theorem 3.11 to get the result.

Remark 3.13. Let l_0 be the characteristic of k and take $n = l_0$. By using Artin-Schreier theory in power series fields over k it is not difficult to get results for extensions of degree l_0 analoguous to the results in Theorem 3.11.

Tate Duality over Local Fields Let K be an $\mathfrak{l}-$adic field with residue field characteristic l_0 and let A be a principally polarized abelian variety defined over K.

Theorem 3.14. **(Tate**, *cf.[Li])*
$<,>_K$ is non-degenerate.

Now assume that n is prime [10] to l_0 and that A has good reduction modulo $\mathfrak{l}$.

[10] For $n = l_0$ cf. [Rü].

What about $H^1(G_K, A(K_s))[n]$?
Let π be an element in K with $v_{\mathfrak{l}}(\pi) = 1$ and let ζ_n be a primitive $n-$th root of unity. Let L_n be equal to $K(\zeta_n, \pi^{1/n})$. The Galois group G_n of $K(\zeta_n)/K$ acts on the Galois group of $L_n/K(\zeta_n)$ by conjugation.
The field $K_n := K(A(K_s)[n])$, the smallest field containing the coordinates of all points of order n of A, is an unramified cyclic extension of K containing ζ_n. Hence the Galois group of $K(\zeta_n)/K$ has a canonical lifting to the Galois group U_n of K_n/K and so U_n acts on $A(K_s)[n]$ and on $G(L_n/K(\zeta_n))$.

Using standard arguments from Galois cohomology and the fact that abelian varieties are cohomologically trivial over finite fields we get:

Lemma 3.15. *In the situation above*

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

Hensel's lemma implies that $A(K)/nA(K) \simeq A(K)[n]$.
Hence by Theorem 3.14 we get a non-degenerate pairing

$$\overline{<,>_K} : A(K)[n] \times \mathrm{Hom}_{U_n}(G(L_n/K(\zeta_n), A(K_s)[n]) \to Br(K)[n] \stackrel{\mathrm{inv}_K}{\to} \mathbb{Z}/n\mathbb{Z}.$$

If we could compute $\overline{<,>_K}$ we would have solved the computation of the discrete logarithm in $A(K)[n]$.

In the special case that $\zeta_n \in K$ we get from Theorem 3.14 the

Corollary 3.16. *Assume that $\zeta_n \in K$ (or equivalently that $\mid k^* \mid \equiv 0 \bmod n$). There is a non-degenerate pairing*

$$<,>_K : A(K)[n] \times \mathrm{Hom}(G(L_n/K), A(K)[n]) \to Br(K)[n]$$

induced by the Tate pairing.

We describe the pairing in the simplest case: Assume that n is a prime and that there is no point of order n^2 in $A(K)$. Let P_1 be a point of order $n \in A(K)$ and $Q_1 \in A(K_s)$ with $nQ_1 = P_1$. Let π be the generator of the Galois group of the maximal unramified extension of K which induces the Frobenius automorphism modulo $\mathfrak{l}$. Let τ be a generator of the Galois group of L_n/K and ϕ_{P_2} the homomorphism of $G(L_n/K)$ to $A(K)[n]$ given by $\phi_{P_2}(\tau) = P_2$. Then $< P_1, \phi_{P_2} >_K$ is the cohomology class of the 2-cocycle γ of the group generated by τ and π given by

$$\gamma(\tau^i \cdot \pi^r, \pi^j \cdot \tau^s) = i \cdot P_2 \cup (\pi^j(Q_1) - Q_1).$$

Application to Jacobian Varieties over Finite Fields We shall assume that p is a prime dividing $q-1$.
Let A be defined over $\mathbb{F}_q$.
We lift A to an abelian variety $\tilde{A}$ over an $\mathfrak{l}$-adic field K with residue field $\mathbb{F}_q$, assume the same notations as above and apply Corollary 3.16 to $\tilde{A}$.
Since Hensel's lemma implies that $\tilde{A}(K)[p]$ is canonically isomorphic to $A(\mathbb{F}_q)[p]$ we get a non-degenerate pairing

$$<,>_{\mathbb{F}_q}: A(\mathbb{F}_q)[n] \times \mathrm{Hom}(G(L_n/K), A(\mathbb{F}_q)[n]) \to Br(K)[n].$$

It remains to give a definition of this pairing which makes its computation fast. For this we assume in addition that A is the Jacobian J_C of a curve C and lift the pair (C, J_C) to K.

Proposition 3.17. (Lichtenbaum) *Let P_1, P_2 be points of order n of $J_C(\mathbb{F}_q)$. Represent P_i by coprime divisors D_i in the divisor class group, and let f_1 be a function on C with divisor $n \cdot D_1$.*
Then $< P_1, P_2 >_{\mathbb{F}_q}$ is the cohomology class c represented by the cocycle

$$\gamma(\tau^i, \tau^j) := f_1(D_2)\ if\ i + j \geq n$$

and

$$\gamma(\tau^i, \tau^j) = 1 \textit{ otherwise.}$$

We call this version of the pairing the Tate-Lichtenbaum pairing.

Since γ represents c modulo the image of the norm map from L_n to K and because of the divisibility of the principal units of K by n we get (with the notation of Proposition 3.17)

Corollary 3.18. *The Tate-Lichtenbaum pairing induces a non-degenerate pairing*

$$<,>: J_C(\mathbb{F}_q)[n] \times J_C(\mathbb{F}_q)[n] \to \mu_n(\mathbb{F}_q)$$

given by

$$< P_1, P_2 >:= f_1(D_2)^{\frac{q-1}{n}}.$$

One finds in [FR] how this pairing can be computed in $O(\log(q))$ addition steps and so it reduces the discrete logarithm in $J_C(\mathbb{F}_q)[n]$ to the discrete logarithm in $\mu_n(\mathbb{F}_q)$.

In general the conditions that $\mathbb{F}_q$ contains $p-$th roots of unity **and** a manageable abelian variety 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:

Corollary 3.19. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and p a prime. Let π_q 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_q^f is congruent to q^f+1 modulo p. In this case 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_q^{fm} becomes congruent to 2 modulo p.

Hence to satisfy Task 3. of Aim 2.1 we have to make sure that f is rather large. This excludes supersingular elliptic curves and very few others.

We end this subsection by remarking that analogous arguments make it even easier to compute the DL if $p = \mathrm{char}(\mathbb{F}_q)$.

Outlook There are two natural
Questions:

1. Can one compute $\overline{<,>}$ rapidly?
2. Can one compute $<,>$ without using the condition that K contains all n-th roots of unity?

To answer these questions (positively or negatively) we need much more information about the arithmetic inside of Brauer groups.

We recall that to use the Tate pairing we had to lift the abelian variety from finite fields to $\mathfrak{l}-$adic fields. **Hasse's** results on Brauer groups make it possible, at least in theory, to lift the problem to global fields (i.e. number fields and function fields in one variable over finite fields) and it may well be that his celebrated sequence for global fields K and their completions $K_{\mathfrak{l}}$:

$$0 \to Br(K) \to \bigoplus_{\mathfrak{l}} Br(K_{\mathfrak{l}}) \overset{\oplus \mathrm{inv}_{\mathfrak{l}}}{\to} \mathbb{Q}/\mathbb{Z} \to 0$$

can play an important role.

References

[ADH] L. Adleman, J. DeMarrais and M. Huang, A Subexponential Algorithm for Discrete Logarithm over the Rational Subgroup of the Jacobians of Large Genus Hyperelliptic Curves over Finite Fields, *Algorithmic Number Theory – Proceedings of the First International Symposium, ANTS–I*, Springer Verlag (1994), 28–40.

[Ba] J. Basmaji, Ein Algorithmus zur Berechnung von Hecke-Operatoren und Anwendung auf modulare Kurven, *Dissertation Essen* (1996).

[DH] W. Diffie and M. Hellman, New directions in cryptography, *IEEE Trans. Inform. Theory* **22** (1976), 644–654.

[E] A. Enge, Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time, *CORR* **99-04**, *Univ. of Waterloo*, (Febr. 1999), to appear in *Math. Comp.*

[ES] A. Enge and A. Stein, Smooth Ideals in Hyperelliptic Function Fields, *CORR* **2000-08**, *Univ. of Waterloo*, (Febr. 2000).

[EG] A. Enge and P. Gaudry, A General Framework for Subexponential Discrete Logarithm Algorithms, Manuscript 19 pp (Febr. 2000).

[Fr] G. Frey, Weil Restriction , *ECC Waterloo* (1998).

[FMR] G. Frey, M. Müller and H.-G. Rück, The Tate Pairing and the Discrete Logarithm Applied to Elliptic Curve Cryptosystems, *Trans. on Inf. Th., IEEE*, **45** (1999), 1717-1719.

[FR] G. Frey and H.-G. Rück, A Remark Concerning m-Divisibility and the Discrete Logarithm in the Divisor Class Group of Curves, *Math. of Comp.*, **62** (1994), 865-874.

[Ga] P. Gaudry, A variant of the Adleman–DeMarrais–Huang algorithm and its application to small genera, *Laboratoire d' Informatique* Preprint LIX/RR/99/04 (1999).

[GHS] P. Gaudry, F. Hess and N. Smart, Constructive and Destructive Facets of Weil Descent on Elliptic Curves, Preprint (2000).

[GS] S. Galbraith and N. Smart, A cryptographic application of Weil descent, in: *Codes and Cryptography, M. Walker ed., Springer LNCS* **1746** (1999), 191–200.

[Ig] J.-I. Igusa, The arithmetic variety of genus two, *Ann. Math.* **72** (1960), 612–649.

[Ka] W. Kampkötter, Explizite Gleichungen für Jacobische Varietäten hyperelliptischer Kurven, *Dissertation Essen* (1991).

[Ko] N. Koblitz, Hyperelliptic Cryptosystems, *J. Cryptology* **1** (1989),139–150.

[Kr] U. Krieger, signature.c–Anwendungen hyperelliptischer Kurven in der Kryptographie, *Diplomarbeit Essen* (1997).

[LR] H. Lange and W. Ruppert, Complete systems of addition laws on abelian varieties, *Invent. Math.*, **79** (1985), 603-610.

[LV] A.K. Lenstra and E.R. Verheul, Selecting Cryptographic Key Sizes, manuscript, (Oct.1999).

[Li] S. Lichtenbaum, Duality Theorems for Curves over p-adic fields, *Inv. math.*, **7** (1969), 120-136.

[Me] J.-F. Mestre, Construction de courbes de genre 2 à partir de leurs modules, in: *Progress in Math.*, **94**, Birkhäuser Verlag (1991), 313–334.

[Mo] F. Morain, Calcul du nombre de points sur une courbe elliptique dans un corps fini: aspects algorithmiques, *J. Th. des Nombres de Bordeaux*, **7** (1995), 111-137.

[MOV] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press (1995).

[MST] V. Müller, A. Stein and A. Thiel, Computing discrete logarithms in real quadratic congruence function fields, *Math. Comp.*, **68** (226) (1999), 807–822.

[Mu1] D. Mumford, On the equations defining abelian varieties I, *Invent. Math.*, **1** (1966), 287–354.

[Mu2] D. Mumford, *Abelian Varieties*, Oxford University Press (1974).

[Mu3] D. Mumford, *Tata lectures on Theta I,II + III*, Birkhäuser Verlag (1982).

[Mur] R. Murty, Exponents of Class Groups of Quadratic Fields, in: *Proc. Conf. Number Th. and Arith. Geom. 19977, ed. G.Frey*, Preprint **14** (1998), IEM, Essen.

[MW] U. Maurer and S. Wolf, Lower Bounds on Generic Algorithms in Groups, in: *Advances in Cryptology-EUROCRYPT 98, K.Nyberg ed., Lecture Notes in Computer Science* **1403**, Springer Verlag (1998), 72-84.

[Na] N. Naumann, Weil-Restriktion Abelscher Varietäten, *Diplomarbeit Essen* (1999).

[Ne] J. Neukirch, *Algebraische Zahlentheorie*, Springer (1992).

[Ng] K. Nguyen, Brauer Groups of Local and Global Fields and Discrete Logarithms, in preparation.

[Od] A.M.Odlyzko, Discrete Logarithms and Smooth Polynomials, in *Finite Fields: Theory, Applications and Algorithms, G.L.Mullen and P. Shiue,eds. Cont. Math.* **168** *AMS* (1994), 269-278.

[Rü] H.-G. Rück, On the Discrete Logarithm in the Divisor Class Group of Curves, *Math. Comp.*, **68** (1999), 1233-1241.

[Sch1] R. Schoof, Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.*, **43** (1985), 483–494.

[Sch2] R. Schoof, Counting Points on elliptic curves over finite fields, *J. de Th. des Nombres de Bordeaux*, **7** (1995), 219–254.

[Sh] G. Shimura , *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press (1971)

[ST] G. Shimura and Y. Taniyama, *Complex Multiplication of Abelian Varieties and its applications to Number Theory*, Publ. Math. Soc. Japan (1961).

[Sho] P. W. Shor, Quantum Computing, *Doc.Math.J.DMV Extra Volume ICM I* (1998), 467–486.

[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer Verlag (1992).

[Sp] A. M. Spallek, Kurven vom Geschlecht 2 und ihre Anwendungen in Public–Key–Kryptosystemen, *Dissertation Essen* (1994).

[We] H. J. Weber, Hyperelliptic Simple Factors of $J_0(N)$ with dimension at least 3, *Experimental Math.*, **6** (1997), 273-287.