Séminaires & Congrès
11, 2005, p. 41–73

MATHEMATICAL BACKGROUND OF PUBLIC KEY CRYPTOGRAPHY

by

Gerhard Frey & Tanja Lange

Abstract. — The two main systems used for public key cryptography are RSA and protocols based on the discrete logarithm problem in some cyclic group. We focus on the latter problem and state cryptographic protocols and mathematical background material.

***Résumé* (Éléments mathématiques de la cryptographie à clef publique). —** Les deux systèmes principaux de cryptographie à clef publique sont RSA et le calcul de logarithmes discrets dans un groupe cyclique. Nous nous intéressons aux logarithmes discrets et présentons les faits mathématiques qu'il faut connaître pour apprendre la cryptographie mathématique.

1. Data Security and Arithmetic

Cryptography is, in the true sense of the word, a classic discipline: we find it in Mesopotamia and Caesar used it. Typically, the historical examples involve secret services and military. Information is exchanged amongst a limited community in which each member is to be trusted. Like Caesar's chiffre these systems were entirely symmetric. Thus, the communicating parties needed to have a common key which is used to de- and encrypt. The key exchange posed a problem (and gives a marvellous plot for spy-novels) but the number of people involved was rather bounded. This has changed dramatically because of electronic communication in public networks. Since

2000 *Mathematics Subject Classification*. — 11T71.
***Key words and phrases*. —** Elliptic curve cryptography, mathematics of public key cryptography, hyperelliptic curves.

The authors would like to thank the organizers of the conference for generous support, an interesting program and last but not least for a very inspiring and pleasant atmosphere.
The second author acknowledges financial support by STORK `http:\\www.stork.org`. The information in this document reflects only the author's views, is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

each pair of participants needs a secret key, a network of n users needs $n(n-1)/2$ keys. Besides the storage problem, one cannot arrange a key exchange for each pair of participants for the huge number of users in today's networks. The solution to this problem came in 1976 with the ground breaking paper by Diffie and Hellman [**16**]. They propose *public key cryptosystems*. This way, parties can agree on a joint secret key over an insecure channel. This key is then used with modern symmetric ciphers like AES [**13**]. The concept of public key cryptography relies heavily on *one way functions*. We give an informal definition:

Definition 1.1. — Let $\mathcal{A}$ and $\mathcal{B}$ be two sets and f a map from $\mathcal{A}$ to $\mathcal{B}$. f is a *one way function* if one can "easily calculate" $f(a)$ but for "essentially all" elements $b \in \mathrm{Im}(f)$ it is "computationally infeasible" to find an $a \in \mathcal{A}$ such that $f(a) = b$.

In a *public key cryptosystem*, each member A of the network has *two* keys: a *private key* s_A produced by himself, never leaving the private secure environment and a *public key* p_A published in a directory. p_A is related to s_A by a (publicly known) one way function. In a protocol, A uses both keys (and the public key of the partner B if necessary). One has to ensure that the function to derive p_A from s_A is one way, and the protocols have to be designed in a manner that there is no usable leakage of information about s_A, s_B from the publicly accessible values.

Today, messages are stored and transmitted as numbers. This makes it possible to apply *Arithmetic* to construct candidates for one way functions, to bring them in such a shape that computation is fast, and to analyze possible attacks.

We shall concentrate on systems based on the *Discrete Logarithm (DL)*. For a general overview of applied cryptography including protocols see [**42**]. In this exposition we can only outline the methods and mathematical facts used for designing secure and efficient DL-Systems. Much more details both for the mathematical background, the basic algorithms and their efficient implementation and the realisation of DL-systems in hardware can be found in [**4**].

2. Abstract DL-Systems

To give mathematical sound definitions we first describe DL-systems in an abstract setting. We give the minimal requirements needed for key exchange and signatures. For the remainder of this section we assume that $\mathcal{A} \subset \mathbb{N}$ [1] and that $\mathcal{B} \subset \mathrm{End}_{\mathrm{set}}(\mathcal{A})$, the set of endomorphism of $\mathcal{A}$. Hence, for any $a \in \mathcal{A}$ and any $b \in \mathcal{B}$ we have $b(a) \in \mathcal{A}$.

[1] This is also important for practical application as one can represent a natural number as a string of bits on a computer.

2.1. Key Exchange. — Assume that the elements of $\mathcal{B}$ commute: for all $a \in \mathcal{A}$ and $b_1, b_2 \in \mathcal{B}$ we have

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

Then we can use $\mathcal{A}, \mathcal{B}$ for a key exchange system in the following way:

We fix a (publicly known) base point $P_0 \in \mathcal{A}$. Each participant S_i chooses an $s_i \in \mathcal{B}$ and publishes $p_i := s_i(P_0)$. Then $s_i(p_j) = s_j(p_i)$ is the shared secret of S_i and S_j.

The security depends (not only) on the complexity to find for any randomly chosen $a \in \mathcal{A}$ and $a_1, a_2 \in \mathcal{B} \circ \{a\}$ *all* elements $b \in \mathcal{B}$ with $b(a) = a_1$ modulo $\mathrm{Fix}_{\mathcal{B}}(a_2) = \{b \in \mathcal{B} : b(a_2) = a_2\}$.

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

2.2. Signature Scheme of El Gamal-Type. — In addition we assume that there are three more structures:

(1) $h : \mathbb{N} \to \mathcal{B}$, a cryptographic hash function[2]

(2) $\mu : \mathcal{A} \times \mathcal{A} \to \mathcal{C}$ a map into a set $\mathcal{C}$ in which equality of elements can be checked fast

(3) $\nu : \mathcal{B} \times \mathcal{B} \to \mathcal{D} \subset \mathrm{Hom}_{\mathrm{set}}(\mathcal{A}, \mathcal{C})$

with $\nu(b_1, b_2)(a) = \mu(b_1(a), b_2(a))$ for all $a \in \mathcal{A}, b_i \in \mathcal{B}$.

Signature. — Let a base point $P_0 \in \mathcal{A}$ be given (or introduced as part as the public key). Like before, each participant S_i has his private key $s_i(P_0)$ and publishes his public key p_i.

To sign a message m, the signer S_i chooses a random element $k \in \mathcal{B}$ and computes $\phi := \nu(h(m) \circ s_i, h(k(P_0)) \circ k) \in \mathcal{D}$ using the knowledge of his private key s_i. Then he sends $(\phi, m, k(P_0))$ as the signature of the message m.

Verification. — The verifier V looks up $s_i(P_0)$, computes

$$\mu\Big(h(m)(s_i(P_0)), h(k(P_0))(k(P_0))\Big),$$

and compares it to $\phi(P_0)$.

The signature is valid if the results are equal.

2.3. The Most Popular Realization. — In practice we often encounter the following situation: Let p be a prime and consider an injective map $(\mathbb{Z}/p, +) \xrightarrow{f} \mathbb{N}$. Let $\mathcal{A} = \mathrm{Im}(\mathbb{Z}/p)$ be the image of f. $\mathcal{A}$ becomes a group with the composition $\oplus$ by the rule:

$$a_1 \oplus a_2 := f(f^{-1}(a_1) + f^{-1}(a_2)).$$

[2] We require h to be one way and collision resistant.

Note that in general $\oplus$ does not coincide with the usual addition in $\mathbb{N}$. For an element $P \in \mathcal{A}$ we define

$$kP = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k \text{ times}}.$$

We require $\oplus$ to be computable in $\mathcal{A}$, *i.e.* without going back to $\mathbb{Z}/p$. Then $\mathcal{A}$ with the operation $\oplus$ is called a *group with numeration.*

We show how this matches with our previous definitions.

Choose $f(0 + p\mathbb{Z}) \neq P_0 \in \mathcal{A}$. The set $\mathcal{B} = \mathrm{Aut}_{\mathbb{Z}}(\mathcal{A}) \cong (\mathbb{Z}/p)^*$ is identified with $\{1, \ldots, p-1\}$ via $b(P) := bP$. We let $\mathcal{C} = \mathcal{A}$, $\mu =$ operation $\oplus$ in $\mathcal{A}$, $\nu =$ addition of endomorphisms, and $h =$ a hash function from $\mathbb{N}$ to $\{1, \ldots, p-1\}$.

Signature scheme. — We translate the abstract scheme to this situation: S chooses randomly and secretly, his *private key* $s \in \{1, \ldots, p-1\}$ and publishes his *public key* $P_S := sP_0$. This key pair is used for many messages.

To sign a message m, S chooses a random number k, which is only used for this one message, and computes

$$r := h(m)s + h(kP_0)k \mod p.$$

The signed message consists of (m, kP_0, r).

To check the authenticity of the message one looks up S's public key and computes

$$R = rP_0, T = h(m)P_S, \quad H = h(kP_0)kP_0.$$

and checks whether

$$R = T \oplus H.$$

The security considerations *for the crypto primitive* boil down to estimating the complexity of computing *Discrete Logarithms:*

The *Discrete Logarithm Problem (DLP)* is as follows: For a given cyclic group with numeration $\mathcal{A}$ and for randomly chosen $P, Q \in \mathcal{A}$ compute $k \in \mathbb{N}$ with $Q = kP$.

We need to construct groups with numerations of large prime order p, which are secure and efficient. Note, that these aims can be contradictory. One requires that the time *or* space needed (probabilistically) to compute discrete logarithms is *exponential* in $\log(p)$. But time *and* space needed to write down the elements and to execute a group composition must be polynomial in $\log(p)$.

2.4. Generic Attacks. — We have motivated that for some protocols it is useful to use the algebraic structure "group". However, every additional structure opens the door to attacks. Assuming no special properties of $\mathcal{A}$, *i.e.* dealing with a so-called *black-box group* allows "generic" attacks. Shoup [**55**] proved that such a black-box group has security at least $\sqrt{|\mathcal{A}|}$. We present two algorithms having this complexity.

To solve the DLP on input $Q = kP$, both aim at retrieving an equality between multiples of P and Q. From $m_1 Q = m_2 P$ one obtains $k \equiv m_2/m_1 \bmod p$. Since these algorithms are inevitable we say that a group is suitable for cryptographic applications, if only these algorithms (or ones with similar running-time) apply. As one is able to find such suitable instances, one should avoid using groups with more powerful attacks unless they offer special advantages like easier implementation or faster algorithms, but a careful security analysis is needed.

Shanks' Baby-Step-Giant-Step Method. — This method is a deterministic algorithm to solve the DLP, first proposed by Shanks [**54**].

– *Baby step:* For $i = 0, \ldots, m \leqslant \sqrt{p}$ compute $(i \cdot P, i)$. These values are stored in a list ordered by the first argument.

– *Giant step:* For $j = 0, \ldots, m \leqslant \sqrt{p}$ compute $(Q - jm \cdot P, j)$.

Then one compares the two lists looking for matching pairs. (In practice only one list is stored and each result of the giant step is compared to this.) If $i \cdot P = Q - jm \cdot P$ then $k = i + jm$ and we have solved the DLP. This algorithm has *complexity* $O(\sqrt{p})$ but there is a *disadvantage* – it needs $O(\sqrt{p})$ space.

Pollard's ρ-Algorithm. — Pollard's algorithm [**48**] is a probabilistic algorithm in the sense that the output is always correct but the computations involve random choices and thus the complexity analysis involves probability assumptions.

The principle behind this algorithm is that for randomly drawn elements of G the expected number of draws before an element is drawn twice is $\sqrt{\pi p/2}$ due to the birthday paradox. To get information out of this we use a controlled random walk, which we now present in the simplest version: The result x_i of the i-th step should depend only on x_{i-1}. So partition the group "randomly" into three sets T_j of size $\approx p/3$ and take

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

There are efficient methods to detect collisions. Like Shanks' method this algorithm has complexity $O(\sqrt{p})$ but requires far less memory.(3)

Security hierarchy. — To have a more precise statement on the complexity of algorithms we measure it by the function

$$L_p(\alpha, c) := \exp(c(\log p)^{\alpha}(\log\log p)^{1-\alpha})$$

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

The *best case* for a cryptosystem is $\alpha = 1$ – then one has *exponential complexity*, this means that the complexity of solving the DLP is exponential in the binary length of the group size $\log p$. The *worst case* is when $\alpha = 0$ – then the system only has *polynomial complexity*. For $0 < \alpha < 1$ the complexity is called *subexponential*.

(3) Using such generic low storage methods the current "world record" w.r.t. Certicom challenge was solved: Compute DL in an 109-bit elliptic curve over a prime field.

2.5. Very Special Examples. — We now describe some groups and analyze their security. In all cases we take numerations based on $(\mathbb{Z}/p,+)$ as cyclic group but the image space $\mathcal{A}$ of the numeration and therefore the induced operation $\oplus$ differs.

Example 1. — The numeration $f : \mathbb{Z}/p \to \{1,\ldots,p\}$ is given by $f(r + p\mathbb{Z}) := [r]_p$ where $[r]_p$ is the smallest positive representative of the class of r modulo p.

The function $\oplus$ is given by

$$r_1 \oplus r_2 = [r_1 + r_2]_p$$

which is easy to compute from the knowledge of r_i.

Security?

We are given b with $b = [na]_p$ and have to solve

$$b = na + kp$$

with $k \in \mathbb{Z}$. The *Euclidean algorithm* solves this in $O(\log(p))$ operations in $\mathbb{Z}/p$, therefore, $\alpha = 0$! We do *not* get a secure DL-system.

Example 2. — 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). We represent elements of $\mathbb{Z}/q$ by their smallest representative in $\{1,\ldots,q\}$. The numeration is given by $f(i + p\mathbb{Z}) := [\zeta^i]_q$. Denote the group of p-th roots of unity by μ_p.

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

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

Security?— For fixed root of unity $a \in \mu_p$ and random $b \in \mu_p$ find k in $\mathbb{N}$ with $b = [a^k]_q$. The best known methods to compute this discrete logarithm are *subexponential* in q [**1, 12, 51**].

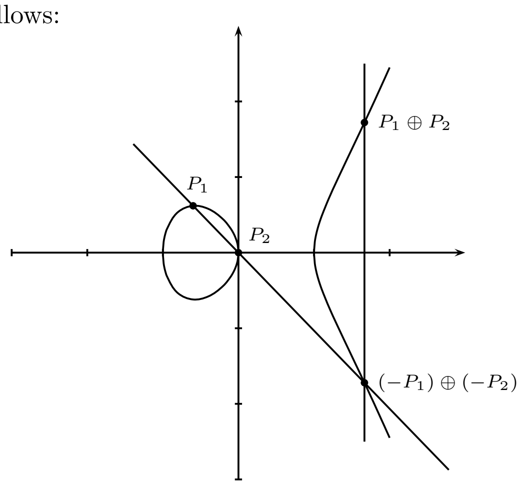
In practice, one starts with a prime q and searches for large prime divisors $p|q-1$ since finding primes q such that $q \equiv 1 \bmod p$ for a given prime p is a hard task. This way it is very easy to find appropriate parameters p and q. An obvious generalization is to work in extension fields with $q = l_0^n, p|l_0^n - 1$ for l_0 prime. To represent the finite field $\mathbb{F}_{l_0^n}$ one fixes an irreducible polynomial $h(x) \in \mathbb{F}_{l_0}[x]$ and uses the isomorphism $\mathbb{F}_{l_0^n} \cong \mathbb{F}_{l_0}[x]/h(x)$ to get an enumeration of $\mathbb{F}_q$, and hence of $\langle\zeta\rangle$ in $\mathbb{N}$.

Example 3. — The most important examples for us are *Elliptic Curves*. An elliptic curve E over a field K is a regular plane projective cubic with at least one rational point. For simplicity we shall assume that $\mathrm{char}(K)$ is prime to 6. Then we find an equation

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

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

A very special property of elliptic curves is that their points form an abelian group. We normalize the points by dividing through the Z-coordinate $(X : Y : Z) \mapsto (x,y) := (X/Z, Y/Z)$. Thereby we loose the point $(0 : 1 : 0)$, which corresponds to the neutral element P_∞. For an elliptic curve over $\mathbb{R}$ the group law on these affine points can be visualized as follows:



This addition is easily transformed into formulas valid over any field. Given $P_1 = (x_1, y_1), P_2 = (x_2, y_2) \neq \pm P_1$ on E their sum $P_3 = P_1 \oplus P_2$ is given by

$$x_3 = \lambda^2 - x_1 - x_2,\ y_3 = \lambda(x_1 - x_3) - y_1,\ \text{where } \lambda = \frac{y_1 - y_2}{x_1 - x_2}. \tag{1}$$

For $P_1 = P_2$ we have the doubling formula

$$x_3 = \lambda^2 - 2x_1,\ y_3 = \lambda(x_1 - x_3) - y_1,\ \text{where } \lambda = \frac{3x_1^3 - A}{2y_1}. \tag{2}$$

Consider an elliptic curve over a finite field $K := \mathbb{F}_q$. Using the numeration of $\mathbb{F}_q$ we can enumerate $\mathbb{F}_q \times \mathbb{F}_q$, *e.g.* using the lexicographical ordering, and therefore the points of $E(\mathbb{F}_q) \smallsetminus \{P_\infty\}$. Choose any number n_∞ which is not used for the enumeration of $E(\mathbb{F}_q) \smallsetminus \{P_\infty\}$ and use it as label for P_∞. Let $P = (x, y) \in E(\mathbb{F}_q)$ be a point of prime order p, then it is obvious that $\langle P \rangle$ is a group with numeration isomorphic to $\mathbb{Z}/p$, the operation induced by $\oplus$.

Elliptic curves are called "good" for cryptographic applications if the group order of the $\mathbb{F}_q$-rational points is almost prime, *i.e.* equal to a prime times a small co-factor. To find such curves is a hard problem. We have to solve the following Diophantine problem:

Find a finite field $\mathbb{F}_q$ with q elements and an elliptic curve E such that the group of $\mathbb{F}_q$-points has (almost) prime order.

Security?— The state of the art is as follows: 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 (see Section 5).

2.6. Numeration by Algebraic Groups. — We now generalize and systematisize the examples, namely, we consider numerations by *algebraic groups* over finite fields $\mathbb{F}_q$ where $q = l_0^n$ is a power of a prime l_0.

Definition 2.1. — An (absolutely irreducible) *algebraic group $\mathcal{G}$ over a field K* is an (affine or projective) absolutely irreducible variety defined over K together with three additional ingredients:

(i) the addition, *i.e.* a morphism

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

(ii) the inverse, *i.e.* a morphism

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

(iii) the neutral element, *i.e.* a K-rational point

$$0 \in \mathcal{G}(K),$$

satisfying the usual group laws:

$$m \circ (\mathrm{id}_{\mathcal{G}} \times m) = m \circ (m \times \mathrm{id}_{\mathcal{G}}) \text{ (associativity)},$$

$$m_{|\{0\}\times\mathcal{G}} = \mathrm{pr}_2,$$

where pr_2 is the projection of $\mathcal{G} \times \mathcal{G}$ on the second argument, and

$$m \circ (i \times \mathrm{id}_{\mathcal{G}}) \circ \delta_{\mathcal{G}} = c_0,$$

where $\delta_{\mathcal{G}}$ is the diagonal map from $\mathcal{G}$ to $\mathcal{G} \times \mathcal{G}$ and c_0 is the map which sends $\mathcal{G}$ to 0.

Let L be an extension field of K. Let $\mathcal{G}(L)$ denote the set of L-rational points. Then $\mathcal{G}(L)$ is a group in which the sum and the inverse of elements are computed by evaluating morphisms which are defined over K, which do not depend on L, and in which the neutral element is the point 0. From now on, we require m to be *commutative*. We now describe how to explicitly compute in algebraic groups.

By definition $\mathcal{G}$ can be covered by affine open subvarieties U given by coordinate functions $X_1, \ldots, X_l$ (l depending on U) which satisfy polynomial relations

$$\{f_1(X_1, \ldots, X_l) = 0, \ldots, f_k(X_1, \ldots, X_l) = 0\}.$$

The L-rational points $U(L) \subset \mathcal{G}(L)$ are the elements $(x_1, \ldots, x_l) \in L^l$, where the polynomials f_i vanish simultaneously. The morphism m induces a morphism

$$m_U : U \times U \longrightarrow \mathcal{G}.$$

For generic points of $U \times U$ the image of m_U is again contained in U. The map can be described via rational functions $R_i \in K(X_1, \ldots, X_l; Y_1, \ldots, Y_l)$ sending pairs of L-rational points $(x_1, \ldots, x_l) \times (y_1, \ldots, y_l)$ in $U \times U$ to

$$(R_1(x_1, \ldots, x_l; y_1, \ldots, y_l), \ldots, R_l(x_1, \ldots x_l; y_1, \ldots, y_l)).$$

This is a birational description of the addition law which is true outside proper closed subvarieties of $U \times U$*. 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. But it can happen that we use pairs of points on purpose (e.g. lying on the diagonal in* $U \times U$*) for which we need an extra description of* m*.*

Now let K and L be finite fields and use a numeration of L to get a numeration of the L-rational points of the affine parts U of $\mathcal{G}$. Then we get a partial numeration of $(\mathcal{G}, m)$. In many cases this is enough for cryptographic applications. For the performance of the cryptosystem the choice of (U, m_U) is crucial. To have short representations and fast to compute group operations we require small l and low degree of the relations f_i as well as of the R_i defining the group operation.

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*.

Example 1 corresponds to the additive group G_a. The scheme is the affine line with coordinate function X and no relations. $G_a(L)$ can be identified with L and $R(X, Y) := X + Y$. Hence, G_a as group is isomorphic to the additive group of L.

Example 2 corresponds to the multiplicative group G_m given by coordinate functions X_1, X_2 with relation $X_1 \cdot X_2 = 1$. The group law is given by

$$R_1(x_1, x_2; y_1, y_2) = x_1 y_1, \quad R_2(x_1, x_2; y_1, y_2) = x_2 y_2.$$

$G_m(L)$ can be identified with L^*.

Both are affine group schemes.

Example 3 is an abelian variety of dimension 1. Choose $U = E \smallsetminus \{P_\infty\}$ with coordinate functions X, Y and relation $Y^2 - X^3 - AX - B$. The addition formulae given above are a birational description for points $(x_1, y_1), (x_2, y_2)$ with $x_1 \neq x_2$. On the diagonal in $U \times U$ we need a special addition law given by the doubling formula (2).

2.7. Manageable Algebraic Groups. — Having this abstract background in mind we now look for instances that can actually be applied. The first task to solve is to describe (birationally) algebraic groups and the addition laws in a time and space efficient way.

Since we have assumed that $\mathcal{G}$ is connected and commutative we can use a classification theorem which yields that $\mathcal{G}$ is an extension of an abelian variety by an affine group scheme. So, for cryptographic purposes we can assume that $\mathcal{G}$ is either affine or an abelian variety.

Affine group schemes have composite factors which (after finite ground field extensions) are isomorphic to copies of G_a and G_m. Since G_a leads to totally insecure systems (see Example 1) we can assume that only copies of G_m occur. Hence, $\mathcal{G}$ is a *torus*. In some cases we find an efficient way to present higher dimensional tori and the addition law on it.

In the center of our interest are abelian varieties. In general it seems to be hopeless to present affine parts and the addition law on them:

Results of Mumford and Lange-Ruppert show that the number of coordinate functions and the degree of the addition formulas both grow exponentially with the dimension of the abelian variety. Therefore, we have to use special abelian varieties.

The first specialization is to take A as Jacobian variety J_C of a curve C or closely related objects. The elliptic curve in Example 3 was a first instance of this strategy. The next section takes a different approach, starting from ideal class groups of orders, and establishes a relation to Jacobians of curves. The (combined) treatment is continued there.

3. DL-systems and Orders

3.1. Ideal Class Groups of Orders. — Let O be a commutative ring with unit 1 without zero divisors. Two ideals[4] A, B of O different from 0 can be multiplied:

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

Clearly $\cdot$ is associative. To be able to compute A^k efficiently we need some minimal assumptions. We require O to be *Noetherian*, *i.e.* every A is a finitely generated O-module. A generating system of the product of two ideals should be computable in finitely many steps from generators of the factors. (Note that in general these systems tend to become longer and longer...) Furthermore, O should be a finitely generated algebra over an *Euclidean* ring $\mathcal{B}$. Then ideals A have a *basis* over $\mathcal{B}$, and by linear algebra over $\mathcal{B}$ one can compute a basis of a product of ideals. But there are *infinitely many* possible choices of bases. Thus we require that there is a canonical basis for each ideal and $\mathcal{B}$ has a numeration. Then one can numerate ideals in O. But to come to a structure usable for DL-systems we have to go one step further and consider *isomorphism classes of projective rank-1-modules* $\mathrm{Pic}(O)$ and factor- or subgroups, respectively.

Definition 3.1. — Let A_1, A_2 be two O-modules in the quotient $\mathrm{Quot}(O)$ of O. We define an equivalence relation by $A_1 \sim A_2$ if there is an element $f \in \mathrm{Quot}(O)^*$ with $A_1 = f \cdot A_2$.

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

$\mathrm{Pic}(O)$ is the set of equivalence classes of invertible ideals of O. It is an abelian group, where the group operation $\oplus$ is inherited from the multiplication of ideals.

To apply systems based on $\mathrm{Pic}(O)$ there has to be a very fast algorithm to find distinguished elements in ideal classes. This is possible if we have "reduction algorithms",

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

or we can use the geometric background of $\mathrm{Pic}(O)$ which leads to *group schemes and abelian varieties* (*cf.* Section 2.6). The most interesting cases are those for which both methods can be used!

We want to embed $\mathbb{Z}/p$ into $\mathrm{Pic}(O)$ in a bit-efficient way. To this end we need a fast method for the computation of the order of $\mathrm{Pic}(O)$ to know which values of p can be used and (at least) a heuristic that with reasonably high probability this order is almost a prime, hence, p is large.

Above all, we need to *exclude attacks.*

"Generic attack". — There is a kind of generic attack for DL-systems based on $\mathrm{Pic}(O)$. It uses the structure introduced by this special choice. We stress that this approach need not be successful in reducing the complexity of the problem. So, there are instances of the DLP based on $\mathrm{Pic}(O)$ for which the best known attacks are the generic attacks described in Section 2.4, and it will be an important task to discuss this carefully.

By the choice of $\mathrm{Pic}(O)$ we have introduced additional structure. We have distinguished ideals in O, namely the prime ideals, and we have the arithmetic structure of $\mathcal{B}$. Since we have to be able to define reduced elements (*i.e.* ideals) in classes, we have in all known cases a notion of "size" which behaves reasonable with respect to addition. Such a setting is always susceptible to *Index-Calculus.*

The abstract principle behind this attack is that we find a "factor base" B consisting of relatively few elements and compute in the group as a $\mathbb{Z}$-module given by the free abelian group generated by the elements of the factor base modulo relations. One needs to prove that with reasonable high probability every element can be written (fast and explicitly) as a sum of elements in the factor base. Such elements are called smooth with respect to B.

The important task in this method is to balance the number of elements in the factor base to make the linear algebra over $\mathbb{Z}$ manageable and to "guarantee" smoothness of enough elements with respect to this base.

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

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

with $0 < \alpha < 1$ and $c > 0$ for a number N closely related to $|\,\mathrm{Pic}(O)|$, but it is only practical under the assumption that one can actually balance the size of B and find a means to express elements over this factor base.

Existing Systems. — All DL-Systems used today fit into the following two classes:

– $\mathcal{B} = \mathbb{Z}$, and O is an order or a localization of an order in a number field

– $\mathcal{B} = \mathbb{F}_{l_0}[X]$, and O is the ring of holomorphic functions of a curve defined over a finite extension field of $\mathbb{F}_{l_0}$.

3.2. The Number Field Case. — Orders O in number fields were proposed very early in the history of public key cryptography by Buchmann and Williams [**10**]. 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 $\mathrm{Pic}(O_K)$ 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. How small the (logarithmic) norm is depends on

$$g_K := \log\left(2^{-r_1-r_2}\pi^{-r_2}w\sqrt{|\Delta_K|}\right),$$

where Δ_K is the discriminant of $O_K/\mathbb{Z}$, r_1 is the number of real embeddings of K, r_2 is the number of complex embeddings of K, and w is the number of roots of unity contained in K (see [**65**], p.238). Due to the analogy with the geometric case (see below), g_K is referred to as the *genus of* K.

The background is the "Geometry of numbers" (Minkowski). By lattice techniques it is possible to compute an ideal of small norm in each class, and for such an ideal one finds a "small" basis.

The most difficult part is to compute the order of $\mathrm{Pic}(O_K)$. One uses analytic methods (L-series) in connection with most powerful tools from computational number theory.

Remark 3.2. — There is a (probabilistic) estimate. The order of $\mathrm{Pic}(O_K)$ behaves (in an erratic way) exponentially in g_K.

This system suffers from the disadvantages that for given g there are not many fields with $g_K = g$ and that to have a large group $\mathrm{Pic}(O_K)$ the genus of K has to be large. The parameter g_K can be split into two components: the degree $n := [K : \mathbb{Q}]$ of the extension field and the ramification locus of $K/\mathbb{Q}$. If n is large the arithmetic in O_K is complicated (it is hard to deal with fundamental units, the lattice dimension grows, ...), therefore large g_K should be obtained by large ramification.

Theory of Gauß. — The most practical example of $\mathrm{Pic}(O_K)$ is when K is an imaginary quadratic field of discriminant $-D$. Then $K = \mathbb{Q}(\sqrt{-D})$. The expected size of $\mathrm{Pic}(O)$ is $\approx \sqrt{D}$.

To perform the arithmetic in $\mathrm{Pic}(O_K)$ one uses a result due to Gauß, namely that $\mathrm{Pic}(O_K)$ corresponds to classes of binary quadratic forms with discriminant D. Hence, multiplication of ideals corresponds to composition of quadratic forms. Reduction of ideals corresponds to the (unique) reduction of quadratic forms: In each class we find (using Euclid‘s algorithm) a uniquely determined *reduced* quadratic form

$$aX^2 + 2bXY + cY^2$$

$ac - b^2 = D$, $-a/2 < b \leqslant a/2, a \leqslant c$ and $0 \leqslant b \leqslant a/2$ if $a = c$.

Remark 3.3. — These systems bear a big disadvantage: The index-calculus-attack works very efficiently! Assuming the generalized Riemann hypothesis, the complexity to compute the DL in $\mathrm{Pic}(O_K)$ is

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

This is no worse than the complexity of solving the DLP in finite fields but for the additional structure there was almost no gain in return.

3.3. The Geometric Case. — Now let $\mathcal{B} = \mathbb{F}_p[X]$, and O is the ring of holomorphic functions of a curve C_O defined over a finite extension field $\mathbb{F}_q$ of $\mathbb{F}_p$. Intrinsically behind this situation is a regular projective absolutely irreducible curve C defined over $\mathbb{F}_q$ whose field of meromorphic functions $F(C)$ is given by $\mathrm{Quot}(O)$. C is the desingularization of the projective closure of the curve C_O. This relates $\mathrm{Pic}(O)$ closely to the points of the Jacobian variety J_C of C and explains the role of abelian varieties in cryptosystems used today.

Curves with singularities. — We assume that O is not integrally closed and hence C_O is a singular curve. The generalized Jacobian variety of the projective closure of C_O is an extension of J_C by linear groups. Examples of groups based on singular curves (or which can also be obtained this way although they were introduced in the different context) contain the following:

(1) $\mathrm{Pic}(\mathbb{F}_q[X,Y]/(Y^2 - X^3))$ corresponds to the additive group G_a of $\mathbb{F}_q$.

(2) $\mathrm{Pic}(\mathbb{F}_q[X,Y]/(Y^2 + XY - X^3))$ corresponds to G_m, the multiplicative group.

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

(4) More generally, we apply scalar restriction to $G_m/\mathbb{F}_{q^k}$ and get tori of higher dimension. An example of this construction, which is actually used in practice, is *XTR* [**40**]. XTR uses an irreducible two-dimensional piece of the scalar restriction of $G_m/\mathbb{F}_{q^6}$ to $\mathbb{F}_q$. Although 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 extension fields and even the variant [**62**] working in $\mathbb{F}_{q^6}$ does not use the geometric background. A further example of this family is LUC [**59**].

To understand what is going on in 4., Silverberg and Rubin [**57**] analyze rational parameterizations of (non-)split tori. They are able to explain systems like LUC and related ones and present a new system called CEILIDH. In addition they come to interesting questions (conjectures) about tori (Vroskresenskii). They also show limits of the method, *i.e.* they analyze for which degrees k a field extension $\mathbb{F}_{q^k}$ allows to work efficiently in a subgroup defined via norm conditions.

Security?— We can get tori by two different methods: by scalar restriction and as generalized Jacobian of curves of *geometric* genus 0 and *arithmetic* genus larger than 0.

This raises the question, whether this structure can be used (as in the case of non singular curves, see below) for attacks?

Curves without singularities. — Assume that C is a projective curve over $\mathbb{F}_q$ without singularities. Let the corresponding curve C_O be an affine part of C with ring of holomorphic functions O which is integrally closed in $F(C) := \mathrm{Quot}(O)$. 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 $\mathbb{A}^1$ is the affine line and $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ is the projective line. For simplicity of our presentation we shall assume that there is a $\mathbb{F}_q$-rational point P_∞ in $\pi^{-1}(\infty)$.

The $\mathbb{F}_q$-rational divisors of C are formal sums of points (over $\overline{\mathbb{F}_q}$) of C which are invariant under $G_{\mathbb{F}_q} := \mathrm{Aut}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. The degree of a divisor D is the sum of the multiplicities of the points occurring in it and is denoted by $\deg(D)$. A divisor is effective if all multiplicities are non negative. Two divisors are in the same class iff their difference consists of the zeroes and poles (with multiplicity) of a function $f \in F(C)$, *i.e.* they differ only by the principal divisor (f) attached to f. The $\mathbb{F}_q$-rational points of the Jacobian variety of C, $J_C(\mathbb{F}_q)$, correspond to the $\mathbb{F}_q$-rational divisor classes of degree 0 of C.

J_C is an abelian variety. The following result makes it possible to describe it (with addition law) by objects like points and functions of C. The reason behind is the *Theorem of Riemann-Roch* (see *e.g.* [**30**]) which rules the arithmetic of curves and their function fields.

One consequence of this theorem is:

Lemma 3.4. — *Let $D = \sum n_i P_i$ be a $\mathbb{F}_q$-rational divisor of C of degree $\geqslant g$. Then there is a function $f \in F(C)$ which has poles of order at most n_i (hence zeroes of order at least $-n_i$ if $n_i < 0$) in the points P_i and no poles elsewhere. In other words: the divisor $D + (f)$ is effective.*

This yields

Lemma 3.5. — *In every $\mathbb{F}_q$-rational divisor class of degree 0 of C there exists a divisor $D - g \cdot P_\infty$ with $D = \sum_{i=1}^k n_i P_i$ with $n_i \in \mathbb{N}$ and $\sum n_i = g$.*

Proof. — Take a divisor class c of degree 0 and any divisor $D' \in c$. We can split $D' = D_1 - D_2$ as difference of two effective $\mathbb{F}_q$-rational divisors. In the first step we choose l large enough such that $l - \deg(D_2) > g$ and by Lemma 3.4 a function f_1 such that $-D_2 + (f_1) + l \cdot P_\infty$ is effective.

By replacing D' by $D' + (f_1)$ we can assume that $D' = D - k \cdot P_\infty$ with D effective and $k = \deg(D)$. If $k > g$ (otherwise we are done) we apply Lemma 3.4 to the divisor $D - (k - g) \cdot P_\infty$ and find a function f such that $D - (k - g) \cdot P_\infty + (f) := D_0$ is effective and therefore $D + (f) - k \cdot P_\infty = D_0 - gP_\infty$ is an element of c of the required form. □

In geometric language this is the

Theorem 3.6. — *The Jacobian J_C of C is birationally isomorphic to*

$$(C \times \cdots \times C)/S_g, \tag{3}$$

where g is the genus of C and S_g is the symmetric group in g letters.

A surjective map φ from $(C \times \cdots \times C)/S_g(\mathbb{F}_q)$ to $J_C(\mathbb{F}_q)$ is given by the following rule: Take natural numbers $n_1, \ldots, n_k$ with $\sum_{i=1}^{k} n_i = g$ and points $P_i \in C(\overline{\mathbb{F}_q})$ such that the divisor $D := \sum_{i=1}^{k} n_i P_i$ is $\mathbb{F}_q$-rational. Then $\varphi(D)$ is the divisor class of $D - g \cdot P_\infty$.

By Lemma 3.5 φ is surjective.

To describe a relation between points on J_C and elements of $\mathrm{Pic}(O)$, we first relate ideals of O to divisors. We shall use that O is a Dedekind ring. This implies that every ideal $\neq (0)$ is a product of powers of maximal ideals M in a unique way and that to every maximal ideal M there corresponds a unique normed discrete valuation v_M such that M is the intersection of the valuation ideal with O. Moreover O is the intersection of all valuation rings related to maximal ideals and every discrete valuation of F is either equivalent to v_M for some M or to an extension of the infinite valuation on $\mathbb{A}^1$ to C.

Let $B \subset F(C)$ be a projective O-module of rank 1. For a maximal ideal $M \subset O$ define $v_M(B) := \max\{k \in \mathbb{Z} : B \subset M^k\}$. Then

$$B = \Pi_{M \text{ maximal in } O}\ M^{v_M(B)}$$

and $B \subset O$ iff all $v_M(B) \geqslant 0$. The classes of two O-ideals B_1 and B_2 are equal iff there is a function $f \in F(C)$ with $v_M(B_1) = v_M(B_2) + v_M((f))$ for all maximal ideals M of O.

For a point $P \in C_O(\overline{\mathbb{F}_q})$ define $M_P := \{f \in O : f(P) = 0\}$. This is a maximal ideal in O. It is easy to see that $M_P = M_{P'}$ iff P is conjugate to P' under the action of $G_{\mathbb{F}_q}$. So it makes sense to relate the Galois orbit $D_P := G_{F_q} \cdot P$ to M_P. The degree of D_P is equal to the degree of M_P defined as $\dim_{\mathbb{F}_q}(O/M_P)$.

Conversely a maximal ideal $M < O$ defines a homomorphism from O to a finite extension field $k_M := O/M$ of $\mathbb{F}_q$. Let σ be an embedding of k_M into $\overline{\mathbb{F}_q}$. Then the image under σ of the coordinate functions defining C_O corresponds to a point on $C_O(\overline{\mathbb{F}_q})$, and so M corresponds to a Galois orbit of points in $C_O(\overline{\mathbb{F}_q})$. Since O is integrally closed this correspondence is one-to-one.

In general, there is a one-to-one correspondence between proper ideals $A < O$ and effective $\mathbb{F}_q$-rational divisors D of C in which only points of C_O occur. If A corresponds to D then $\deg(D) = \log_q(|O/A|) =: \deg(A)$. Now we apply the Theorem of Riemann-Roch to ideal classes of O to get

Lemma 3.7. — *Let c be an element of* $\mathrm{Pic}(O)$. *Then c contains an ideal $A < O$ with* $\deg(A) \leqslant g$.

Proof. — Let $A' \in c$ be an O-ideal and assume that $\deg(A') > g$. Take the effective divisor $D_{A'}$ associated to A' and a function f such that $D' := (f)+D_{A'}-(\deg(A')-g)P_\infty$ is effective of degree g. Let D'' be the divisor obtained from D' by removing points in $\pi^{-1}(\infty)$ and let A be the ideal obtained from D''. Then $A \in c$ and $\deg(A) \leqslant g$. □

We are now ready to define a homomorphism from J_C to the ideal class group $\mathrm{Pic}(O)$.

Result 3.8. — *Define $\phi : J_C(\mathbb{F}_q) \to \mathrm{Pic}(O)$ by the following rule: in the divisor class c take a representative D' of the form $D' = D - gP_\infty$, D effective. Remove from D all points in $\pi^{-1}(\infty)$ and define A as ideal in O like above. Then $\phi(c)$ is the class of A in* $\mathrm{Pic}(O)$. *By Lemma 3.7 ϕ is surjective.*

For applications one is usually interested in the case that the kernel of ϕ is trivial. Then we can use the interpretation via ideal classes for computations and via the abelian varieties for the structural background.

The result sums up the steps we have performed so far: Starting from the non singular curve C we derived the ring of holomorphic differentials O of C_O. In an affine part of the Jacobian J_C, the group operation can be performed via ideal multiplication (using the map ϕ) whereas the reduction procedure is based on the effective version of the Riemann-Roch Theorem as described in the proof of Lemma 3.5 (this replaces Minkowski's theorem in the number field case). Both steps can be performed algorithmically or be (symbolically) translated to formulae. From the formulae it might be possible to derive the birational description of the group operation on J_C.

The computation of the order of $\mathrm{Pic}(O)$ and the construction of suitable curves is done by using properties of abelian varieties or Jacobians of curves, respectively.

Example. — Assume that there is a cover

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

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

Compared with the number theory case we have won a lot of freedom. The parameters are:

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

There are about $l_0^{3g\cdot n}$ curves of genus g over $\mathbb{F}_{l_0^n}$ and we can vary all three parameters independently.

***Theorem 3.9* (Structural relation: Hasse-Weil)**. — *The size of the Jacobian is related to the parameters as*

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

For cryptographic applications this implies a *key length* (*i.e.* number of bits needed to represent a key) of $O(ng\log(l_0))$ with small constants.

4. Hyperelliptic Curves

In this section we want to apply the previous results to hyperelliptic curves, elliptic curves ($g = 1$) are included. So far these are the most prominent non-singular curves used in practice and so for the convenience of the reader we shall go a bit into details.

***Definition 4.1* (Hyperelliptic Curve)**. — Assume that C is a projective irreducible non singular curve of genus $g \geqslant 1$ with a generically étale morphism π of degree 2 to $\mathbb{P}^1$. Then C is a *hyperelliptic curve*.

In terms of function fields this means, the function field $F(C)$ of C is a separable extension of degree 2 of the rational function field $\mathbb{F}_q(X)$. Let ω denote the non trivial automorphism of this extension. It induces an involution ω on C with quotient $\mathbb{P}^1$. The fixed points $P_1, \dots, P_{2g+2}$ of ω are called Weierstraß points. They are the points in which π is ramified.

Assume that we have a $\mathbb{F}_q$-rational Weierstraß point $P_\infty = P_{2g+2}$. We choose ∞ on $\mathbb{P}^1$ as $\pi(P_\infty)$. Then the ring of holomorphic functions O on $C \smallsetminus P_\infty$ 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 $f_C(X,Y) = Y^2 + h(X)Y - f(X)$ and h, f are polynomials in X with $\deg(h) \leqslant g$ and $\deg(f) = 2g+1$.

Theorem 4.2. — *With the notations and the assumptions mentioned above we have*

(1) *$J_C(\mathbb{F}_q)$ is isomorphic to $\mathrm{Pic}(O)$ under the isomorphism ϕ defined in Result 3.8.*

(2) *In every ideal class c of O there is exactly one ideal $A \subset O$ of degree $t \leqslant g$ with the property: The only prime ideals which could divide both A and $\omega(A)$ are those resulting from Weierstraß points.*

(3) *Let A be as above. Then $A = \mathbb{F}_q[X]u(X) + \mathbb{F}_q[X](v(X) - Y)$ with $u(X), v(X) \in \mathbb{F}_q[X]$, u monic of degree t, $\deg(v) < t$, and u divides $v^2 + h(X)v - f(X)$.*

(4) *$u(X)$ and $v(X)$ are uniquely determined by A and hence by c. So $[u, v]$ can be used as coordinates for c.*

Proof

(1) follows immediately from Result 3.8, and moreover we get that every $\mathbb{F}_q$-rational point on J_C can be represented by an ideal $A \subset O$ of degree g.

(2) Since for every ideal B we get that $B\cdot\omega(B)$ is a principal ideal we can reduce A repeatedly until the condition in (2) is satisfied without changing its class. After this process we call A reduced.

Now assume that $\deg(A) \leqslant g$, $\deg B \leqslant g$, with A, B reduced and that $A \sim B$. Then $A \cdot \omega(B)$ is a principal ideal in O and so it is equal to (b) with $b \in F(C)$ having only one pole of order $\leqslant 2g$ in P_∞. By Riemann-Roch all such functions lie in an $\mathbb{F}_q$-vector space of dimension $g+1$, and a basis of this space is given by $\{1, X, X^2, \ldots, X^g\}$. So $b \in \mathbb{F}_q[X]$ and $A\cdot\omega(B)$ is the conorm of an ideal in $\mathbb{F}_q[X]$. Since A and B are reduced this means that $A = B$ and (2) is proved.

(3) Let $A \in O$ be an ideal of degree t. Recall that $\{1, Y\}$ is a basis of O as $\mathbb{F}_q[X]$-module. We choose any basis $\{w_1 = f_1(X) + f_2(X)Y,\ w_2 = g_1(X) + g_2(X)Y\}$ of A as $\mathbb{F}_q[X]$-module. We find relative prime polynomials h_1, h_2 with $f_2h_1 - g_2h_2 = 0$ and choose $u_1, u_2 \in \mathbb{F}_q[X]$ with $u_1h_1 - u_2h_2 = 1$. Now take $w_1' := h_1w_1 + h_2w_2 =: u'(X), w_2' = u_2w_1 + u_1w_2$. Since the determinant of this transformation is 1 the pair $\{u(X), w_2' = v_1(X) + v_2(X)Y\}$ is again a basis of A. Since the rank of A is 2, $v_2(X)$ is not equal to 0. So $A \cap \mathbb{F}_q[X]$ is generated by u. Since A is reduced the degree of A is equal to the degree of u and we can and will take u monic. Now write $v_1 = a\cdot u + v$ with $\deg v < t$. By replacing w_2' by $w_2 - a\cdot w_1$ we get a basis $\{u(X), v(X) + v_2(X)Y\}$ of A. Since the degree of A is equal to $u(X)v_2(X)$ we get: $v_2(X)$ is constant, and so we can assume $v_2(X) = -1$. The element $(v+Y)(v-Y) = v^2 + h(X)Y - f(X) = (v^2 + h(X)v - f(X)) - h(X)(Y - v)$ lies in A and so the last claim of (3) follows.

(4) From the proof of (3) we have that $u(X)$ is determined by A as monic generator of $A \cap \mathbb{F}_q[X]$. Now assume that $v' - Y \in A$ with $\deg(v') < t$. Then $v' - v \in A \cap \mathbb{F}_q[X]$ and hence $v' - v = 0$. □

Remark 4.3. — 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 $D(f_C)$ and the addition $\oplus$ with the composition of such forms. Theorem 4.2 and its proof can easily be translated into this language.

The description of $J_C(\mathbb{F}_q)$ resp. $\mathrm{Pic}(O)$ by the "coordinates" $[u, v]$ is the basis for *Cantor's algorithm* [**11, 34**] which can be written down "formally" and then leads to *addition formulas* or can be implemented as *algorithm.* It works as follows:

Let A_i $(i = 1, 2)$ be given by the bases $\{w_1^i, w_2^i\} = \{u_i(X), v_i(X) - Y\}$ as above. Then $A_1 \cdot A_2$ has a basis $\{u_3'(X), v_3'(X) + w_3'(X)Y\}$ which is computed by Hermite reduction from the generating system $\{w_j^1 \cdot w_k^2;\ 1 \leqslant j, k \leqslant 2\}$. The next step is to find a reduced ideal of degree $\leqslant g$ in the class of $A_1 \cdot A_2$ and for this the Gauß algorithm can be used in a completely analogous way.

Example. — To give a flavor and, at the same time, an example, we present explicit formulas by Lange [**38**] for addition of ideal classes for a genus 2 curve.

Let the affine curve C_O be defined over $\mathbb{F}_q$, given by

$$C_O : y^2 + h(x)y - f(x), \quad \deg f = 5, \deg h \leqslant 2.$$

First look at the (real) picture:

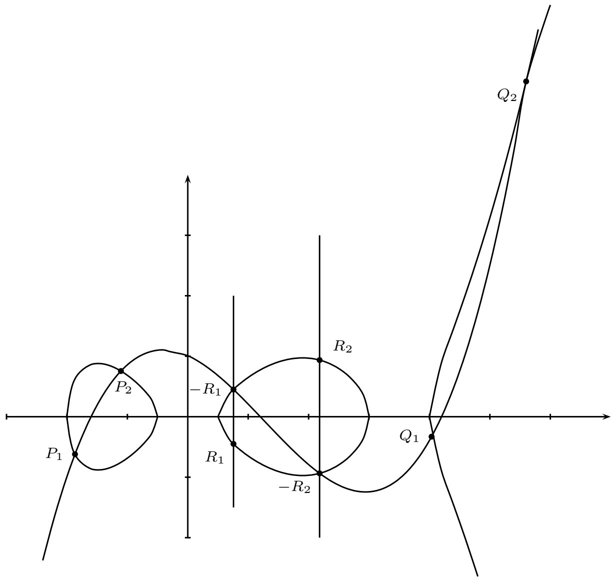


Figure 1. $(P_1 + P_2 - 2\infty) + (Q_1 + Q_2 - 2\infty) = R_1 + R_2 - 2\infty$

Each point on $J_C(\mathbb{F}_q)$ can be represented as $[u, v]$. The formulae use only the coefficients of u and v, the case given below is the most common one. The paper [**38**] contains a study of different coordinate systems for scalar multiplication on genus 2 curves.

On first view these formulae look much more involved than those for elliptic curves (1). However, due to Theorem 3.9 the field elements involved are of half size only. Therefore, the speed of scalar multiplication on elliptic and genus 2 curves is similar and the decision which system (or even more subtle, which kind of coordinates) to take will depend on the used computing device.

There are explicit formulae available for genus 3 hyperelliptic curves [**47**]. The same considerations hold.

Addition, $\deg u_1 = \deg u_2 = 2$		
Input	$[u_1, v_1], [u_2, v_2], u_i = x^2 + u_{i1}x + u_{i0}, v_i = v_{i1}x + v_{i0}$	
Output	$[u', v'] = [u_1, v_1] + [u_2, v_2]$	
Step	Expression	Operations
1	compute resultant r of u_1, u_2: $z_1 = u_{11} - u_{21}$, $z_2 = u_{20} - u_{10}$, $z_3 = u_{11}z_1 + z_2$; $r = z_2z_3 + z_1^2u_{10}$;	1S, 3M
2	compute almost inverse of u_2 modulo u_1 ($inv = r/u_2 \bmod u_1$): $inv_1 = z_1$, $inv_0 = z_3$;	
3	compute $s' = rs \equiv (v_1 - v_2)inv \bmod u_1$: $w_0 = v_{10} - v_{20}$, $w_1 = v_{11} - v_{21}$, $w_2 = inv_0w_0$, $w_3 = inv_1w_1$; $s'_1 = (inv_0 + inv_1)(w_0 + w_1) - w_2 - w_3(1 + u_{11})$, $s'_0 = w_2 - u_{10}w_3$; if $s'_1 = 0$ special case	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

An Outlook: Non hyperelliptic curves of genus 3. — One can also base DL-systems on Picard curves or more generally on plane curves of genus 3 given by an equation

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

with $\deg(f) = 4$. For these curves there is an efficient arithmetic available, too (*cf. e.g.* Flon-Oyono [**21**]) for which some further techniques [**6**] can be applied.

4.1. Index-Calculus. — As in the analogous situation in number theory there exists a subexponential "attack" based on the index-calculus principle. But there is *one essential difference*. Recall: in the number field case the subexponential function was a function in $|D|$ and therefore depending on the order of the class group. Due to Weil, the analog would be a dependency in q^g. But in the known index-calculus algorithms one cannot look at q and g as independent variables. *E.g.* if $g = 1$ is fixed then we do not get a subexponential attack for any $q \to \infty$! This is the reason for writing "attack" above.

Gaudry, Enge, and Stein [**18, 19, 20**] analyzed the complexity of the basic index-calculus algorithm.

Theorem 4.4. — *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*

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

For large genera this is a strong result. For practical use, *i.e.* moderately small genera, the results of Gaudry [**26**] and more recently of Thériault [**63**] are more serious. For hyperelliptic curves of relatively small genus (in practice: $g \leqslant 9$) there is an index-calculus attack of complexity

$$O(g^5 q^{2-\frac{2}{g+1}+\varepsilon})$$

with "reasonable small" constants and even for $g = 3$ and 4 the security is reduced.

The main additional ingredient to the generic index-calculus attack described above is to further reduce the size of the factor base. One uses only prime divisors of small degree (*e.g.* 1) as factor base and Thériault even proposes to only take a subset thereof.

Remark 4.5. — We can summarize the results:

– Orders related to curves of genus $\geqslant 4$ or closely related abelian varieties should be avoided!

– State of the art: We have only three types of rings O which avoid serious index-calculus attacks and for which $\mathrm{Pic}(O)$ in manageable. These are the *maximal orders belonging to curves of genus* $1, 2, 3$. Even for $g = 3$ one needs to take into account the group size to compare the complexities of the generic attacks and Thériault's large prime variant of the index calculus attack.

5. Galois Operation

Till now we used results from algebraic geometry applied to curves over finite fields but we only mildly made use of the additional structure induced by the Galois operation of $G_{\mathbb{F}_q}$, $q = l_0^n$ on geometric objects attached to curves. In this section we shall explain how this can be used in a constructive way but also investigate its application to attacks.

We shall investigate linear structures induced by the action of the Frobenius automorphism $\Pi_q \in G_{\mathbb{F}_q}$ on vector spaces attached to curves resp. semi linear structures induced by the Frobenius automorphism Π of the prime field of $\mathbb{F}_q$ as well as bilinear structures given by duality of algebraic groups.

5.1. Point Counting. — Examples for representation spaces of Π_q are spaces of holomorphic differentials or more generally of differentials with prescribed poles and cohomology groups.

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

There are most important theorems (Hasse, Deligne-Weil, Lefschetz) saying: Let Π_q operate on the first étale resp. crystalline cohomology groups attached to a projective non singular curve C of genus g. Then its characteristic polynomial is independent of the choice of the cohomology and is a monic polynomial of degree $2g$ with coefficients in $\mathbb{Z}$. Its zeroes are algebraic integers with absolute value $q^{1/2}$. It is called the L-series $L_C(s)$ of C resp. J_C.

By elementary linear algebra one sees:

$$|L_C(1)| = |J_C(q)|$$

and so the computation of the L-series of C solves the problem to determine the divisor class number of C.

A first method to do this computation is to use the concrete realization of the étale cohomology as Tate module of J_C for primes l different from p. By definition Tate-modules $T_l(J_C)$ are modulo l isomorphic to the l-torsion points, and on this fact the strategy of Schoof's algorithm [**52**] relies: compute the Frobenius action modulo small primes (and their powers if possible) and then use the Chinese remainder theorem to determine the L-series. This algorithm is *polynomial* (in $n \log l_0$). Nevertheless it is not working fast enough even for elliptic curves without further tricks (see [**53**] for an overview). In the moment we can use it only to count the points on randomly chosen elliptic curves in cryptographic relevant regions. By rather sophisticated implementations Gaudry and Schost can determine divisor class numbers of random curves of genus 2 [**28**] in ranges of cryptographic interest. According to their timings it takes $\sim$ one week on a single computer to do this, and so it is still far less efficient than point counting on elliptic curves.

A way out is the choice either of special curves or of special fields.

5.1.1. Reduction of global curves. — Though one is interested in curves over finite fields one starts with a curve over a number field K with the special property that its Jacobian has complex multiplication. Then explicit class field theory (theory of Shimura-Taniyama of CM fields) is available. This allows to compute the minimal polynomials of the curve invariants. Again by class field theory one can rapidly compute the trace of the Frobenius acting on the reduction of the curve modulo places of K. Hence, the order of the group of rational points on the Jacobian of C after reduction is known even before writing down the equations for the curve. Finally, when one has found a place of K leading to a good group order, one computes the equation of the curve modulo the prime from the invariants, *e.g.* by using a method of

Mestre [**44**]. Initially this method was proposed by Atkin and brought to applications together with Morain [**2, 3**] to find curves of smooth group order to factor integers. For cryptographic applications this was detailed by Spallek [**61**] for elliptic curves; for larger genera see Weng [**66**].

It is obvious that the degree of K must not be too large and so the method described will lead to curves over fields with small degree over their prime fields and hence to large characteristics.

Another complication is that for genus-3-curves we shall not get hyperelliptic curves if we choose the CM-field without special properties and so have even more special choices to make. An open question is whether the special properties of the constructed curves can be used for serious attacks. Till now no such attack is known.(5)

5.1.2. Fields with small characteristic

(1) We come back to random curves but over special fields $\mathbb{F}_q$ with $q = p^n$ and p *very small* (typically equal to 2). During the last years a very interesting series of papers appeared which all use certain parts of p-adic information obtained by rigid $\mathfrak{p}$-adic analysis and transform it into efficient algorithms. For instance instead of Tate modules one uses the *Dieudonné module* of J_C as realization of the crystalline cohomology or one goes to affine parts of the curves for which it is possible to compute the action of Π on de Rahm cohomology groups of completions of coordinate rings using "classical" work of Monsky-Washnitzer and of Dwork. This approach was proposed by Satoh [**50**] and generalized or refined by Satoh, Skjerna, Taguchi, Gaudry, Harley, Fouquet, Mestre, Kedlaya, Lauder, Wan, Gerkmann,... (see [**22, 45, 33, 39, 29**]).

(2) Now we specialize the curves we use, too. We assume that the curve is defined over a field $\mathbb{F}_{q_0}$ which is small enough to use methods like baby-step-giant step to determine the L-series. It is then easy to determine the group order over extension fields. To reach a suitable group size one makes a constant field extension. The main advantage of this construction is a speed-up of the scalar multiplication by using the Frobenius endomorphism (see [**5, 35, 46, 58, 60**] for elliptic and [**36**] for general curves).(6)

5.2. Scalar Restriction. — In 5.1.2 we have used the extra structure that the absolute Frobenius endomorphism Π is acting on objects attached to the curve. Can we use this for attacks?

One method to exploit it is the scalar restriction. It can be applied to transfer discrete logarithms in the rational points of abelian varieties over extension fields to

(5) Another special class of global curves are those with real multiplication. We get an interesting link to modular forms and Hecke operators but till now the complexity of the algorithms involved does not allow to come to cryptographically relevant regions.

(6) If q_0 is very small we have a direct generalization of a suggestion of Koblitz. The idea can be applied to small degrees ($n = 3, 5$) of extension and leads to secure instances if one avoids special choices of curves [**7, 15, 37**].

discrete logarithms in the rational points of abelian varieties of larger dimension but defined over a smaller field, and this problem could be easier. For instance one could end up with a Jacobians of a curve of "moderate" genus over the small field for which the index-calculus method works.

It seems to be clear that this approach does not work for random curves over random fields or for extensions of large prime degree (which is not a Mersenne prime). There are also some fields over which all curves are weak [**43**].

We now describe the main principles behind scalar restriction. There are basically two variants.

Variant 1. — Let L be a finite Galois extension of the field K. Assume that C is a curve defined over L, D a curve defined over K and

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

a non constant morphism defined over L.

Then we have a correspondence map

$$\phi : \mathrm{Pic}^0(C) \longrightarrow \mathrm{Pic}^0(D), \quad \phi := \mathrm{N}_{L/K} \circ \varphi^*.$$

If $\ker(\phi)$ is small then the (cryptographically relevant) part of $\mathrm{Pic}^0(C)$ is mapped injectively into $\mathrm{Pic}^0(D)$ and we have a transfer of the DLP in $\mathrm{Pic}^0(C)$ into a (possibly easier) DLP in $\mathrm{Pic}^0(D)$.

It seems that this variant works surprisingly well if C is a (hyper)elliptic curve of characteristic 2 not defined over K (*cf.* work of Galbraith, Smart, Hess, Gaudry, Diem Thériault,... under the key word *GHS attack* [**25, 27, 24, 14, 64**]).

In general this method relates the DLP to the highly interesting theory of fundamental groups of curves over non algebraically closed ground fields and so to inverse Galois theory.

A powerful tool to study this topic is the theory of Hurwitz spaces. A discussion can be found in [**15**].

Variant 2. — Again assume that C is defined over L. We apply scalar restriction from L to K to the (generalized) Jacobian variety of C and get a $[L : K]$-dimensional (group scheme) abelian variety A over K.

Now we look for curves D in K-simple factors B of A. As B is a factor of $Jac(D)$ we can hope to transfer the DLP from $Jac(C)$ to $Jac(D)$.

It is not clear whether this variant can be used in practice. But it leads to interesting mathematical questions:

Which curves have the scalar restriction of an abelian variety (*e.g.* an elliptic curve) as Jacobian?

Bouw, Diem, and Scholten, [**9**] have found families of curves related to the last question.

5.3. Pairings. — We shall use properties of abelian varieties with Galois action to build up a bilinear structure related to our DL-system in special cases. This structure allows to transfer the DLP to the Brauer group of local and global fields. Under appropriate conditions this transfer will end up with the "classical" discrete logarithm in finite fields not far away from the ground field. This can be used in attacks but also to construct identity based schemes.

5.3.1. Bilinear structures. — We shall begin with a general notion.

Definition 5.1. — Assume that a DL-system A is given (and hence A is a cyclic group of prime order with a numeration) and that there is a group A' in which we can compute "as fast" as in A. Assume moreover that B is another DL system and that a map

$$Q : A \times A' \longrightarrow B$$

satisfies the following requirements

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

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

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

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

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

There are two immediate consequences:

– The DL-system A is at most as secure as the system B.

– Assume that $A = A'$ and hence

$$Q(a_0, a_0) \neq 0.$$

Then for all triples $(a_1, a_2, a_3) \in \langle a_0 \rangle^3$ one can decide in polynomial time in $\log(p)$ whether

$$\log_{a_0}(a_3) = \log_{a_0}(a_1) \cdot \log_{a_0}(a_2)$$

holds. Hence the *decision Diffie-Hellman* (DDH) problem is easy.

These are negative aspects of bilinear DL-systems but very interesting protocols due to Joux [**31**] (tripartite key exchange) and Boneh-Franklin [**8**] use such structures in a constructive way.

5.3.2. Evaluations of functions. — We used rational points on principally polarized abelian varieties (namely Jacobians of curves) for the realization of DL-systems. These objects come with a duality theory which will be exploited now. To make this practical we first explain how to evaluate functions attached to points of order p at given points. We shall have to solve the following problem:

Let C be a curve of genus g defined over some ground field K, let E be a K-rational divisor of degree 0 on C and c a K-rational divisor class of degree 0 and of order n on C. Let $D_1 = A_1 - gP_0 \in c$ be a divisor where A_1 is an effective divisor of degree g. Any multiple $i \cdot c$ can be represented in a similar way by $D_i := A_i - gP_0$. We assume that the support of E is prime to the support of all divisors D_i. Especially the divisor nD_1 is the principal divisor of a function f on C which has no poles and zeroes in the points in the support of E. Hence $c(E) := f(E)$ is a well defined element in K^*.

We want to compute this element fast and follow an idea which —for elliptic curves— V. Miller has written in an unpublished letter and which in the general case is inspired by Mumford's theory of Theta groups of abelian varieties.

The basic step for the computation is: for given positive divisors A, A' of degree g find a positive divisor B of degree g and a function h on C such that $A+A'-B-gP_0 = (h)$. We can assume that this step can be done fast for otherwise we could not use J_C for DL-systems. As a measure for the complexity of our algorithm we shall take the needed amount of such steps.

Define the following group law on $\langle c\rangle \times K^*$:

$$(i \cdot c, a_1) \circ (j \cdot c, a_2) := ((i+j) \cdot c, a_1 a_2 \cdot h_{i,j}(E)),$$

with $A_i + A_j - A_{i+j} - gP_0 = (h_{i,j})$. The assumptions on E guarantee that each $h_{i,j}(E) \in K^*$. The degree of $h_{i,j}$ is at most g. It can be easily seen by induction that $l\cdot(c,1) = (lc, h_{l-1}(E))$ where h_{l-1} is a function on C satisfying $lA - A_{l-1} - (l-1)gP_0 = h_{l-1}$. Hence the n-fold application gives the result $(0, f(E))$, where f is a function on C with $(f) = nD_1$.

Now we can use the group structure on $\langle c\rangle \times K^*$ and apply the square- and multiply algorithm to evaluate f at E in $O(\log(n))$ basic steps.

5.3.3. The Tate pairing. — Let K be a field with absolute Galois group G_K and A be a principally polarized abelian variety over K. We assume that n is a prime p is different from $\mathrm{char}(K)$. [7]

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

$$0 \longrightarrow A(K_s)[p] \longrightarrow A(K_s) \xrightarrow{\cdot\, p} A(K_s) \longrightarrow 0.$$

Application of Galois cohomology gives the exact sequence

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

Next we use that $A(K_s)[p]$ is self dual (in fact the Weil pairing induces the duality) as G_K-module (since A is principally polarized) and so we can use the cup product

[7] The case $p = \mathrm{char}(K)$ is much easier. In this case one can break the DL-system in polynomial time (*cf.* [**49**]).

to get the *Tate-pairing*

$$\langle\, ,\, \rangle_K : A(K)/pA(K) \times H^1(G_K, A(K_s))[p] \longrightarrow H^2(G_K, \mu_p)$$

given by

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

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

The information we can obtain from the Tate-pairing depends on the information given by the Brauer group and on its degree of non-degeneracy. For instance if $K = \mathbb{F}_q$ is a finite field, the Brauer group is $\{0\}$. The situation changes if we take K as an $\mathfrak{l}$-adic field with residue field $\mathbb{F}_q$. Then we have the following theorem:

***Theorem 5.2* (Tate).** — *The pairing $\langle\, ,\, \rangle_K$ is non-degenerate.*

Hence, for principally polarized abelian varieties over $\mathfrak{l}$-adic fields we have transferred the DL-problem in $A(K)[p]$ to the corresponding problem in $\mathrm{Br}(K)[p]$ provided that we can evaluate the pairing in polynomial time. This implies especially the ability to describe $H^1(G_K, A(K_s))[p]$ and $\mathrm{Br}(K)[p]$ and to compute in it. Let us assume that K *contains a primitive p-th root of unity ζ_p, i.e. $p \mid (q-1)$.*

Standard calculations with cohomology groups yield:

***Corollary 5.3*.** — *Let L_p be a ramified extension of K of degree p.*

There is a non-degenerate pairing

$$\langle\, ,\, \rangle : A(K)/p \cdot A(K) \times \mathrm{Hom}(G(L_p/K), A(K)[p]) \longrightarrow \mathrm{Br}(K)[p]$$

induced by the Tate pairing.

5.3.4. Application to Jacobian varieties over finite fields. — Now we start with a finite field $\mathbb{F}_q$ and a prime p dividing $q-1$. Let C be a projective curve defined over $\mathbb{F}_q$ and let J_C be its Jacobian. We lift (C, J_C) to $(\widetilde{C}, J_{\widetilde{C}})$ over an $\mathfrak{l}$-adic field K with residue field $\mathbb{F}_q$ and apply Corollary 5.3 to $J_{\widetilde{C}}$.

Moreover we can apply Hensel's lemma in various forms and get

– $J_{\widetilde{C}}(K)/pJ_{\widetilde{C}}(K)$ is canonically isomorphic to $J_C(\mathbb{F}_q)/pJ_C(\mathbb{F}_q)$.

– $J_{\widetilde{C}}(K)[p]$ is canonically isomorphic to $J_C(\mathbb{F}_q)[p]$.

– Let τ be a generator of $G(L_p/K)$. Then $\varphi \in \mathrm{Hom}(G(L_p/K), J_{\widetilde{C}}(K)[p])$ is uniquely determined by $\varphi(\tau)$ and hence is (not canonically) isomorphic to $J_C(\mathbb{F}_q)[p]$.

– $\mathrm{Br}(K)[p]$ is (again not canonically since one has to fix L_p and τ) isomorphic to $\mathbb{F}_q^*/\mathbb{F}_q^{*p}$.

For this situation we describe the Tate pairing (up to sign) in a version due to Lichtenbaum.

Theorem 5.4 **(Lichtenbaum)**. — *Let τ be a generator of $G(L_p/K)$. Let P_1, P_2 be points of $J_{\widetilde{C}}(K)$ with P_2 a point of order p. Let φ be the homomorphism of $G(L_p/K)$ to $J_{\widetilde{C}}(K)[p]$ mapping τ to P_2. Represent P_i by coprime divisors D_i in the divisor class group of $\widetilde{C}$, and let f_2 be a function on $\widetilde{C}$ with divisor pD_2.*

Then

$$\langle P_1 + p \cdot J_{\widetilde{C}}(K), \varphi\rangle = f_2(D_1) \cdot N_{L_p/K}(L_p^*).$$

$K^*/N_{L_p/K}(L_p^*)$ is isomorphic to $\mathbb{F}_q^*/\mathbb{F}_q^{*p}$.

Corollary 5.5. — *There is a non-degenerate pairing*

$$\langle\, , \rangle_{\mathbb{F}_q} : J_C(\mathbb{F}_q)/pJ_C(\mathbb{F}_q) \times J_C(\mathbb{F}_q)[p] \longrightarrow \mathbb{F}_q^*/\mathbb{F}_q^{*p}$$

given by the following rule:

Let P_1, P_2 be points of $J_C(\mathbb{F}_q)$ with P_2 a point of order p. Represent P_i by coprime divisors D_i in the divisor class group of C, and let f_2 be a function on C with divisor pD_2.

Then

$$\langle P_1 + pJ_C(\mathbb{F}_q), P_2\rangle = f_2(D_1) \cdot \mathbb{F}_q^*/\mathbb{F}_q^{*p}.$$

Now we use the results in Section 5.3.2 and see that we can transfer the DLP in $J_C(\mathbb{F}_q)[p]$ to the discrete logarithm in $\mathbb{F}_q^*$ in polynomial time.

We end this section with a remark:

It may look strange that in order to prove a result on curves over finite fields we have to go to the theory of abelian varieties over l-adic fields. In fact having the pairing in Corollary 5.5 one can prove directly that it is not degenerate using only Kummer theory. But firstly we have seen already in the point counting algorithms that lifting varieties to local and global fields can give more information, secondly it was easier to find the pairing by going to the well studied local setting and most importantly the pairing in Corollary 5.5 is only a special and somewhat disguised part of a general picture showing for instance the importance of Brauer groups for DL systems.

5.3.5. Consequences. — We have seen how to reduce discrete logarithms in $J_C(\mathbb{F}_q)/pJ_C(\mathbb{F}_q)$ to discrete logarithms in $\mathrm{Br}(K)[p]$ for an $\mathfrak{l}$-adic field K with residue field $\mathbb{F}_q$ if $\zeta_p \in \mathbb{F}_q$. In general put

$$k := [\mathbb{F}_q(\zeta_p) : \mathbb{F}_q]$$

and let K be a $\mathfrak{l}$-adic field with residue field $\mathbb{F}_{q^k}$. Then discrete logarithms in $J_C(\mathbb{F}_q)/pJ_C(\mathbb{F}_q)$ can be transferred to discrete logarithms in $\mathrm{Br}(K)[p]$ with costs $O(\log(|\mathbb{F}_q(\zeta_p)|)) = O(k \log q)$.

This is no practical result if k is large. In general, the conditions that K – and hence also the residue field $\mathbb{F}_q$ – contains p-th roots of unity *and* that J_C has points of order p rational over $\mathbb{F}_q$ which are cryptographically interesting will not be satisfied at the same time.

For elliptic curves we can formulate this more precisely:

Proposition 5.6. — *Let E be an elliptic curve defined over $\mathbb{F}_q$ and p a prime. Let π be the Frobenius endomorphism of $E(\mathbb{F}_q)$. Then $\mathbb{Z}/p$ can be embedded into $E(\mathbb{F}_q)$ iff the trace of π is congruent to $q+1$ modulo p and the corresponding discrete logarithm in $E(\mathbb{F}_q)$ can be reduced to the discrete logarithm in $\langle\zeta_p\rangle$ in the field $\mathbb{F}_{q^k}$ where k is the smallest integer such that the trace of π^k becomes congruent to 2 modulo p.*

In general it is easy to *avoid* elliptic curves with small k and it is an interesting Diophantine problem to *construct* elliptic curves with small k if we want to avoid *supersingular elliptic curves*. The trace of the Frobenius acting on such curves is divisible by $\mathrm{char}(\mathbb{F}_q)$, and they are defined over the quadratic extension of the prime field. So one knows quite well their L-series.

For instance if E is supersingular and defined over the prime field $\mathbb{F}_l$ with characteristic l larger than 3 then the characteristic polynomial of the Frobenius is X^2+l. It follows immediately that if $E[p](\mathbb{F}_q) \neq \{0\}$ then after an extension of degree at most 2 the p-th roots of unity are rational and hence $k \leqslant 2$. For $l_0 = 2$ one gets: $k \leqslant 4$, and for $l_0 = 3$: $l \leqslant 6$ [**41**]. The bound $k = 6$ remains valid in general. For other curves one has

Theorem 5.7. — *Let A be a supersingular abelian variety of dimension g over $\mathbb{F}_q$ with a non-trivial point of order p. Then there exists an integer $k(g)$ such that the degree k is bounded by $k(g)$.*

For $g \leqslant 8$ Galbraith [**23**] explicitly determines $k(g)$. Cryptographically interesting are $g = 2, 3$. There one has $k(2) = 12$ and $k(3) = 30$. As result we get:

Supersingular curves (and some others) lead to DL-system which are only subexponentially secure.

5.3.6. The role of isogenies. — If we want to apply the bilinear structure to the Diffie-Hellman decision problem (destructively) and to tripartite key exchange and ID-based systems (constructively) we need more: we really need a pairing on one group of order p. In general the Tate pairing cannot be used directly. But sometimes one can use a trick:

Proposition 5.8. — *Assume that there are an endomorphism η of J_C and a point $P_0 \in J_C$ with $\eta(P_0)$ of order p satisfying*

- $\langle P_0 + pJ_C(\mathbb{F}_q), \eta(P_0)\rangle = \zeta_p$,
- *η can be computed in polynomial time.*

Then (DDH) can be solved in $A[p]$, and $A[p]$ can be used for an identity based system.

Let $E/\mathbb{F}_q$ be an elliptic curve. If the group of $\mathbb{F}_q$-rational points of order p is cyclic, k is small, and if there exists an endomorphism $\eta \notin \mathrm{End}_{\mathbb{F}_q}(E)$, which can be efficiently evaluated on $E[p]$ the conditions of the proposition are satisfied.

Example. — Let E be a supersingular elliptic curve and assume that $\mathbb{F}_q = \mathbb{F}_{l_0^n}$ has n odd and p does not divide $q-1$. If $\mathrm{End}(E)$ has small discriminant, the conditions are satisfied. To give a more concrete example: Let additionally $l_0 \equiv 3 \bmod 4$ and consider the curve

$$E : Y^2 = X^3 - X.$$

Since $\sqrt{-1} \notin \mathbb{F}_q$ such an η is given by

$$\eta : X \longmapsto -X, \quad Y \longmapsto \sqrt{-1}Y.$$

Remarks

– If the order of the rational points of E is not a smooth number we have examples of groups in which (DDH) is weak (of polynomial complexity) but the DLP is believed to be subexponentially hard. Explicit examples have been given by Joux and Nguyen [**32**].

– It is clear that both efficiency and security of the ID-system based on the example are critical.

– Higher dimensional examples are constructed Rubin and Silverberg [**56**] by using supersingular abelian varieties.

– Instead of using supersingular elliptic curves it would be much better to use ordinary elliptic curves with $k \approx 8$. Results in this directions are contained in [**17**].

References

[1] L. Adleman – The function field sieve, in *Algorithmic Number Theory Seminar ANTS-I*, Lect. Notes Comput. Sci., vol. 877, Springer, 1994, p. 108–121.

[2] A.O.L. Atkin. – The number of points on an elliptic curve modulo a prime, unpublished manuscript, 1991.

[3] A.O.L. Atkin & F. Morain – Elliptic curves and primality proving, *Math. Comp.* **61** (1993), p. 29–68.

[4] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen & F. Vercauteren – *The Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, 2005, to appear.

[5] R. M. Avanzi, M. Ciet & F. Sica – Faster Scalar Multiplication on Koblitz Curves combining Point Halving with the Frobenius Endomorphism, in *Public Key Cryptography – PKC 2004* (F. Bao, R. H. Deng & J. Zhou, eds.), Lecture Notes in Comput. Sci., vol. 2947, Springer-Verlag, 2004, p. 28–40.

[6] R.M. Avanzi, G. Frey, T. Lange & R. Oyono – On Expansions to the Base of -2, submitted, 2003.

[7] R.M. Avanzi & T. Lange – Cryptographic Applications of Trace Zero Varieties, preprint, 2003.

[8] D. Boneh & M. Franklin – Identity based encryption from the Weil pairing, in *Advances in cryptology – Crypto '2001*, Lect. Notes Comput. Sci., vol. 2139, Springer, 2001, p. 213–229.

[9] I. Bouw, C. Diem & J. Scholten – Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p$ with constant j-invariant, preprint, see `http://www.arehcc.org`, 2003.

[10] J. Buchmann & H.C. Williams – A key exchange system based on real quadratic fields, in *Advances in Cryptology – Crypto '89*, Lect. Notes Comput. Sci., vol. 435, Springer, 1990, p. 335–343.

[11] D.G. Cantor – Computing in the Jacobian of a hyperelliptic curve, *Math. Comp.* **48** (1987), p. 95–101.

[12] D. Coppersmith – Fast evaluation of discrete logarithms in fields of characteristic two, *IEEE Trans. Inform. Theory* **30** (1984), p. 587–594.

[13] J. Daemen & V. Rijmen – AES proposal : Rijndael, selected as the Advanced Encryption Standard (AES), 2001.

[14] C. Diem – A Study on Theoretical and Practical Aspects of Weil-Restriction of Varieties, Ph.D. Thesis, University Essen, 2001.

[15] C. Diem & J. Scholten – Cover Attacks – A report for the AREHCC project, see `http://www.arehcc.org`, 2003.

[16] W. Diffie & M.E. Hellman – New directions in cryptography, *IEEE Trans. Inform. Theory* **22** (1976), no. 6, p. 644–654.

[17] R. Dupont, A. Enge & F. Morain – Building curves with arbitrary small MOV degree over finite prime fields, *J. Cryptology* **18** (2005), no. 2, p. 79–89.

[18] A. Enge – Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time, *Combinatorics and Optimization Research Report University of Waterloo*, CORR 99-04. Preprint, 1999.

[19] A. Enge & P. Gaudry – A general framework for algorithms, *Acta Arith.* **102** (2002), p. 83–103.

[20] A. Enge & A. Stein – Smooth ideals in hyperelliptic function fields, *Math. Comp.* **71** (2002), p. 1219–1230.

[21] S. Flon & R. Oyono – Fast Arithmetic on Jacobians of Picard Curves, in *Public Key Cryptography – PKC 2004*, Lect. Notes Comput. Sci., vol. 2947, 2004, p. 55–68.

[22] M. Fouquet, P. Gaudry & R. Harley – On Satoh's algorithm and its implementation, *J. Ramanujan Math. Soc.* **15** (2000), p. 281–318.

[23] S.D. Galbraith – Supersingular Curves in Cryptography, in *Advances in Cryptology – Asiacrypt 2001*, Lect. Notes Comput. Sci., vol. 2248, Springer, 2001, p. 495–513.

[24] ———, Weil descent of Jacobians, in *WCC2001* (D. Augot & C. Carlet, eds.), Electronic Notes in Discrete Mathematics, vol. 6, Elsevier Science Publishers, 2001.

[25] S.D. Galbraith & N.P. Smart – A Cryptographic Application of Weil Descent, in *Cryptography and Coding*, Lect. Notes Comput. Sci., vol. 1746, Springer, 1999, p. 191–200.

[26] P. Gaudry – An algorithm for solving the discrete log problem on hyperelliptic curves, in *Advances in Cryptology – Eurocrypt'2000*, Lect. Notes Comput. Sci., Springer, 2000, p. 19–34.

[27] P. Gaudry, F. Hess & N.P. Smart – Constructive and destructive facets of Weil descent on elliptic curves, *J. Cryptology* **15** (2002), no. 1, p. 19–46.

[28] P. Gaudry & E. Schost – Construction of Secure Random Curves of Genus 2 over Prime Fields, in *Advances in cryptology – Eurocrypt'2004*, Lect. Notes Comput. Sci., vol. 3027, Springer, 2004, p. 239–256.

[29] R. Gerkmann – The p-adic Cohomology of Varieties over Finite Fields and Applications on the Computation of Zeta Functions, Ph.D. Thesis, University Duisburg-Essen, 2003.

[30] H.Stichtenoth – *Algebraic Function Fields and Codes*, Springer, 1993.

[31] A. Joux – A One Round Protocol for Tripartite Diffie-Hellman, in *Algorithmic Number Theory, ANTS-IV*, Lect. Notes Comput. Sci., vol. 1838, 2000, p. 385–394.

[32] A. Joux & K. Nguyen – Separating Decision Diffie-Hellman from Diffie-Hellman in Cryptographic Groups, *J. Cryptology* **16** (2003), p. 239–247, *cf.* Cryptology ePrint Archive, Report 2001/003.

[33] K. Kedlaya – Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology, *J. Ramanujan Math. Soc.* **16** (2001), p. 323–338.

[34] N. Koblitz – Hyperelliptic cryptosystems, *J. Cryptology* **1** (1989), p. 139–150.

[35] ______, CM-curves with good cryptographic properties, in *Advances in Cryptology – Crypto'91*, Lect. Notes Comput. Sci., vol. 576, Springer, 1992, p. 279–287.

[36] T. Lange – Efficient Arithmetic on Hyperelliptic Curves, Ph.D. Thesis, Universität Essen, 2001.

[37] ______, Trace zero subvariety fof genus 2 curves for cryptosystems, *J. Ramanujan Math. Soc.* **19** (2004), no. 1, p. 15–33, also available from Cryptology ePrint Archive `http://eprint.iacr.org/2003/094/`.

[38] ______, Formulae for Arithmetic on Genus 2 Hyperelliptic Curves, *Appl. Algebra Engrg. Comm. Comput.* **15** (2005), no. 5, p. 295–328, `http://www.ruhr-uni-bochum.de/itsc/tanja/preprints.html`.

[39] A. Lauder & D. Wan – Counting points on varieties over finite fields of small characteristic, to appear in MSRI Computational Number Theory Proceedings.

[40] A.K. Lenstra & E.R. Verheul – The XTR public key system, in *Proceedings Crypto 2000*, Lect. Notes Comput. Sci., vol. 1880, Springer-Verlag, Berlin, 2000, p. 1–19.

[41] A. Menezes, T. Okamoto & S. Vanstone – Reducing elliptic curve logarithms to a finite field, *IEEE Trans. Inform. Theory* **39** (1993), p. 1639–1646.

[42] A. Menezes, P. vanOorschot & S. Vanstone – *Handbook of Applied Cryptography*, CRC Press, 1996.

[43] A.J. Menezes, E. Teske & A. Weng – Weak fields for ECC, in *Topics in Cryptology – CT RSA 2004*, Lecture Notes in Comput. Sci., vol. 2964, Springer-Verlag, 2004, p. 366–386.

[44] J.-F. Mestre – Construction des courbes de genre 2 à partir de leurs modules, Progress in Math., vol. 94, Birkhäuser, 1991, p. 313–334.

[45] ______, Lettre adressée à Gaudry et Harley, `http://www.math.jussieu.fr/mestre/lettreGaudryHarley.ps`, December 2000.

[46] V. Müller – Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two, *J. Cryptology* **11** (1998), p. 219–234.

[47] J. Pelzl – *Fast Hyperelliptic Curve Cryptosystems for Embedded Processors*, Master's Thesis, Ruhr-University of Bochum, 2002.

[48] J.M. Pollard – Monte Carlo methods for index computation (mod p), *Math. Comp.* **32** (1978), p. 918–924.

[49] H.-G. Rück – On the discrete logarithm problem in the divisor class group of curves, *Math. Comp.* **68** (1999), p. 805–806.

[50] T. Satoh – The canonical lift of an ordinary elliptic curve over a finite field and its point counting, *J. Ramanujan Math. Soc.* **15** (2000), p. 247–270.

[51] O. SCHIROKAUER – Using number fields to compute logarithms in finite fields, *Math. Comp.* **69** (2000), p. 1267–1283.

[52] R. SCHOOF – Elliptic curves over finite fields and the computation of square roots mod p, *Math. Comp.* **44** (1985), p. 483–494.

[53] ______, Counting Points on elliptic curves over finite fields, *J. Théo. Nombres Bordeaux* **7** (1995), p. 219–254.

[54] D. SHANKS – Class number, a theory of factorization and genera, Proc. Symp. Pure Math., vol. 20, American Mathematical Society, 1971, p. 415–440.

[55] V. SHOUP – Lower bounds for discrete logarithms and related problems, in *Proceedings Eurocrypt'97*, Lecture Notes in Comput. Sci., vol. 1233, 1997.

[56] A. SILVERBERG & K. RUBIN – Supersingular abelian varieties in cryptology, in *Advances in Cryptology – Crypto 2002*, Lect. Notes Comput. Sci., vol. 2442, Springer, 2002, p. 336–353.

[57] ______, Algebraic tori in cryptography, in *High Primes and Misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Institute Communications, American Mathematical Society, 2004.

[58] N.P. SMART – Elliptic Curve Cryptosystems over Small Fields of Odd Characteristic, *J. Cryptology* **12** (1999), p. 141–151.

[59] P. SMITH & C. SKINNER – A public-key cryptosystem and a digital signature system based on the Lucas function analogue to discrete logarithms, in *Proceedings Asiacrypt'94*, Lecture Notes in Comput. Sci., vol. 917, 1995.

[60] J. SOLINAS – Efficient arithmetic on Koblitz curves, *Designs, Codes and Cryptography* **19** (2000), p. 195–249.

[61] A.M. SPALLEK – *Konstruktion einer elliptischen Kurve über einem endlichen Körper zu gegebener Punktegruppe*, Master's Thesis, Gesamthochschule Essen, 1992.

[62] M. STAM & A.K. LENSTRA – Efficient subgroup exponentiation in quadratic and sixth degree extensions, in *Cryptographic Hardware and Embedded Systems – CHES 2002*, Lecture Notes in Comput. Sci., vol. 2523, Springer-Verlag, 2003, p. 317–332.

[63] N. THÉRIAULT – Index calculus attack for hyperelliptic curves of small genus, in *Advances in cryptology – Asiacrypt 2003*, Lect. Notes Comput. Sci., vol. 2894, Springer, 2003, p. 75–92.

[64] ______, The discrete logarithm problem in the Jacobian of algebraic curves, Ph.D. Thesis, University of Toronto, 2003.

[65] A. WEIL – *Œuvres scientifiques. Collected papers. Vol. I (1926-1951)*, Springer, 1980.

[66] A. WENG – Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation, Ph.D. Thesis, Universität Essen, 2001.

G. FREY, Institute for Experimental Mathematics, University of Duisburg-Essen, Ellernstrasse 29, D-45326 Essen, Germany • *E-mail :* frey@exp-math.uni-essen.de

T. LANGE, Department of Mathematics, Technical University of Denmark, Matematiktorvet - Building 303, DK-2800 Kgs. Lyngby, Denmark • *E-mail :* t.lange@mat.dtu.dk