

# Perspectives of the Discrete Logarithm Systems

Gerhard Frey  
Institute for Experimental  
Mathematics  
University of Duisburg-Essen  
[frey@exp-math.uni-essen.de](mailto:frey@exp-math.uni-essen.de)

# 1 Abstract DL-Systems

We want

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

with simple protocols

clear and easy to follow implementation  
rules

based on secure crypto primitives

with a well understood mathematical  
background.

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

### 1.1 Key Exchange

Assume that the elements of  $B$  commute:

For all  $a$  and  $b_1, b_2 \in B$  we have

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

Then we can use

$$A, B$$

for a key exchange system in an obvious way - using (publicly known) base points in  $B$ -orbits of  $A$ .

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

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

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

## 1.2 Signature Scheme of El Gamal-Type

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

1.

$$h : \mathbb{N} \rightarrow B,$$

a hash function

2.

$$\mu : A \times A \rightarrow C$$

a map into a set  $C$  in which equality of elements can be checked fast

3.

$$\nu : B \times B \rightarrow D \subset \text{Hom}_{\text{set}}(A, C)$$

with

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

## **Signature:**

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

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

Let  $m$  be a message.

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

$P$  computes

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

in  $D$ .

$P$  publishes

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

## **Verification:**

$V$  computes

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

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

### 1.3 The most popular realization

$A \subset \mathbb{N}$  a cyclic group of prime order  $p$

$$B = \text{Aut}_{\mathbb{Z}}(A) \cong (\mathbb{Z}/p)^*$$

identified with  $\{1, \dots, p-1\}$

by  $b(a) := a^b$ .

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

$\nu =$  addition of endomorphisms

$h =$  a hash function from  $\mathbb{N}$  to  $\mathbb{N}$  followed by the residue map modulo  $p$ .

The security considerations

#### **for the crypto primitive**

boil down to the complexity of the computation of the

#### **Discrete Logarithm:**

For randomly chosen  $a_1, a_2 \in G$  compute  $n \in \mathbb{N}$  with

$$a_2 = a_1^n.$$

## 2 Realization as Class Groups

**ALL systems used today rely on the following construction:**

$O$  is a finitely generated algebra over an euclidian ring  $\mathcal{B}$ .

An ideal  $A$  of  $O$  is invertible if there is an ideal  $B$  with  $A \cdot B = O$ .

Two ideals  $A, B$  are in the same class if there is an element  $f \in K^*$  with  $A = f \cdot B$ .

$Pic(O)$ , the set of equivalence classes, is the ideal class group of  $O$ .<sup>1</sup>

---

<sup>1</sup>By using an enriched module structure, namely modules with metric (Arakelov theory) one can include infrastructures (Shanks, Buchmann) into our setting (cf. work of Schoof).

We have to assume that we can enumerate elements in  $Pic(O)$ . Then we get a numeration of  $\mathbb{Z}/p$  by embedding it into  $Pic(O)$  -  
**provided that  $Pic(O)$  has elements of order  $p$ .**

One has to be able to:

1. find a distinguished element in each class (resp. a finite (small) subset of such elements)(geometry of numbers, reduction theory).
2. find “coordinates” and addition formulas in  $Pic(O)$
3. compute  $| Pic(O) |$ .

# Speculations...

## 2.0.1 More Groups

There are many groups floating around in Arithmetic Geometry which are well studied because of their importance for theory.

Why not use them for practise?

For instance **cohomology groups** like

- Brauer groups of fields and varieties
- Selmer groups of abelian varieties
- Chow groups of varieties like surfaces
- K-groups

Of course both constructional and security aspects cannot be predicted. But we may have some surprises: There can be transfers from DL-systems we know already to other groups, and this can have consequences for security.

### **Open Problem:**

Study attacks and transfers

## 2.0.2 The Number Field Case

**Orders  $O$  in number fields** where introduced by Buchmann-Williams 1988. The easiest case:

$$K = \mathbb{Q}(\sqrt{-d}), d > 0.$$

### **Theory of Gauß:**

$Pic(O_K)$  corresponds to classes of binary quadratic forms with discriminant  $d$  with composition as addition law.

Choice of distinguished ideals:

In each class we find (by using Euclid's algorithm) a uniquely determined **reduced** quadratic form

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

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

### 2.0.3 The Geometric Case

$\mathcal{B} = \mathbb{F}_p[X]$ , and  $O$  is the ring of holomorphic functions of a curve  $C_a$  defined over a Galois field  $\mathbb{F}_q$ .

Intrinsically behind this situation is a regular projective absolutely irreducible curve  $C$  defined over  $\mathbb{F}_q$  whose field of meromorphic functions  $F(C)$  is given by  $Quot(O)$ .

$C$  is the desingularisation of the projective closure  $C_p$  of  $C_a$ .

This relates  $Pic(O)$  closely with the Generalized Jacobian variety of  $C_p$  and the Jacobian variety  $J_C$  of  $C$  and explains the role of group schemes like tori and abelian varieties in crypto systems.

## Singularities

We assume that  $O$  is not integrally closed.

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

### Examples:

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

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

**Example:**

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

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

## 2.0.4 **Work of Rubin-Silverberg**

To understand what is going on Silverberg and Rubin analyse rational parametrisations of (non-)split tori, are able to explain related systems like LUC and give a new system CEILIDH.

In addition they come to interesting questions (conjectures) about tori (Vroskresenskii).

They also show limits of the method.

These systems satisfy part of the aim to go away from group structures. It can be seen that they have relations with Chebychev polynomials (but the relation is not efficient).

## **Question:**

Can one use others of the one-to-one maps of projective lines over finite fields given by polynomials?

### 2.0.5 **Security?**

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

## **Question:**

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

## Curves without singularities

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

The inclusion

$$\mathbb{F}_q[X] \rightarrow \mathcal{O}$$

corresponds to a morphism

$$C_{\mathcal{O}} \rightarrow \mathbb{A}^1$$

which extends to a map

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

where  $\mathbb{P}^1 = \mathbb{A}^1 \cup \{\infty\}$ . The canonical map

$$\phi : J_C(\mathbb{F}_q) \rightarrow \text{Pic}(\mathcal{O})$$

is surjective but not always injective:

Its kernel is generated by formal combinations of degree 0 of points in  $\pi^{-1}(\infty)$ .

Most interesting case: The kernel of  $\phi$  is trivial.

Then we can use the ideal interpretation for computations and the abelian varieties for the structural background:

- Addition is done by ideal multiplication
- Reduction is done by Riemann-Roch theorem (replacing Minkowski's theorem in number field) on curves

but

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

## Example

Assume that there is a cover

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

in which one point ( $P_\infty$ ) is totally ramified and induces the place ( $X = \infty$ ) in the function field  $\mathbb{F}_q(X)$  of  $\mathbb{P}^1$ .

Let  $\mathcal{O}$  be the normal closure of  $\mathbb{F}_q[X]$  in the function field of  $C$ .

Then  $\phi$  is an isomorphism.

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

## **One glimpse at hyperelliptic curves:**

We are in a very similar situation as in the case of class groups of imaginary quadratic fields.

In fact: Artin has generalized Gauß 's theory of ideal classes of imaginary quadratic number fields to hyperelliptic function fields connecting ideal classes of  $O$  with reduced quadratic forms of discriminant  $D(f)$  and the addition  $\oplus$  with the composition of such forms. This is the basis for the **Cantor algorithm** which can be written down “formally” and then leads to addition **formulas** or can be implemented as **algorithm**.

## 2.0.6 **Explicit Formulas for hyperelliptic curves**

They are available for  $g = 2$  and  $g = 3$ . These formulas may have advantages in certain environments.

### **Task:**

Give explicit formulas for non hyperelliptic curves of genus 3.

This is partly done (non optimized till now), e.g. for Picard curves.

### 3 Generic Attacks for Picard Groups

We measure the complexity of attacks by

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

with  $0 \leq \alpha \leq 1$  and  $c > 0$ ,  $N$  closely related to  $|G|$ .

#### 3.1 Exponential Complexity:

$$\alpha = 1$$

We use **the algebraic structure “group”**.

This allows “generic” attacks:

**Pollard’s  $\rho$ -Algorithm**

**Shank’s Baby-step-Giant-step Algorithm**

They both have complexity  $\sim p^{1/2}$ , i.e.  $c = 1/2$ .

### 3.2 Subexponential Complexity:

$$0 < \alpha < 1$$

We use **Picard groups of orders over euclidean rings  $\mathcal{B}$** .

We have distinguished ideals: Prime ideals.

We have the arithmetic structure of  $\mathcal{B}$  which is used to define reduced elements (i.e. ideals) in classes which have a “size” of which behaves reasonable with respect to addition.

Hence we can apply **Index-Calculus-Attacks**.

They are **more effective than the exponential attacks** for all orders  $O$  which **do not belong to curves of genus 1, 2 or 3**.

## 4 Galois Operation

### 4.1 Find a Curve!

The tasks are:

Find a finite field  $k$ , a curve  $C$  defined over  $k$  and a prime number  $p$  dividing  $|Pic(O_C)|$ , a point  $P_0 \in Pic(O_C)$  such that we get a secure DL-system.

The determination of  $P_0$  is not difficult if  $C$  is known.

To find  $(k, C)$  one uses the following strategy:

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

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

### **Computation of the L-series of $C/k$ .**

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

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

## Methods:

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

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

## Counting on special curves

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

### 4.1.1 **Open Problems**

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

## 4.2 Scalar Restriction

One example to use the

**extra structure:**

**Frobenius endomorphism**

is the scalar restriction.

It is applied to curves which are not defined over prime fields.

It can be used to transfer DL's in many elliptic curves to DL's in Jacobians of curves for which the index-calculus method works.

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

## Principles:

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

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

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

a non constant morphism defined over  $L$ .

Then we have a correspondence map

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

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

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

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

It seems that this variant works surprisingly well if  $C$  is a (hyper-)elliptic curve not defined over  $K$  in characteristic 2.

cf. work of Galbraith, Smart, Hess, Gaudry, Diem, ...

Key word: **GHS attack**

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

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

Variant 2:

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

Now we look for curves  $D$  in  $K$ -simple factors  $B$  of  $A$ .

As  $B$  is a factor of  $Jac(D)$  we can hope to transfer the DL-problem from  $Jac(C)$  to  $Jac(D)$ .

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

But it leads to interesting mathematical questions:

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

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

## 5 Bilinear Structures

We assume that a DL System is given by a numeration of a group  $A$  and that  $B$  is another DL system of the same type. Assume that

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

is computable in **polynomial time** with

- $Q$  is  $\mathbb{Z}$ -bilinear
- $Q(., .)$  is non degenerate.

Then  $(A, Q)$  is a DL-system with bilinear structure  $Q^2$ .

There are two immediate consequences:

---

<sup>2</sup>It is obvious how to generalize bilinear to multilinear

- The DL-system  $A$  is at most as secure as the system  $B$ .
- The Diffie-Hellman Decision problem “ For given a (random) element  $a$  and  $a_1, a_2, a_3 \in \langle a \rangle$  decide whether (simultaneously)

$$a_1 = a^{n_1}, a_2 = a^{n_2}, a_3 = a^{n_1 \cdot n_2}$$

holds”

can become very easy.

These are negative aspects of bilinear DL-systems but very interesting protocols due to Joux (tripartite key exchange) and Boneh-Franklin (identity based schemes) use such structures in a positive way. For more information for this and for the following section visit the home page of Steven Galbraith.

## 5.1 Duality by Class Field Theory

The main results of class field theory (local, global and geometric) are duality theorems. So it is to be expected that this theory can be exploited for bilinear structures. The most prominent example nowadays is the

### **Tate-Lichtenbaum duality.**

It relates abelian varieties  $A/K$  with the Brauer group  $Br(K)$  of  $K$ .

Hence we get a **bilinear structure** on  $A(K)_p$  with values in  $Br(K)_p$  which can be used for DL-transfer and for decision problems-

provided that

- the pairing is not degenerate
- it can be computed rapidly
- we can compute in  $Br(K)_p$ .

These conditions are satisfied if  $K$  is a  $l$ -adic field or a field of power series over a finite field which contains the  $p$ -th roots of unity and  $A$  is the Jacobian of a curve.

For elliptic curves we can formulate this over finite fields (by reduction resp. Hensel's lemma) precisely in terms of the trace of the Frobenius automorphism.

**Proposition 1** *Let  $E$  be an elliptic curve defined over  $\mathbb{F}_q$  and  $p$  a prime. Let  $\pi$  be the Frobenius automorphism of  $\mathbb{F}_q$ .*

*Then  $\mathbb{Z}/p$  can be embedded into  $E(\mathbb{F}_{q^f})$  iff the trace of  $\pi^f$  is congruent to  $q^f + 1$  modulo  $p$  and the corresponding discrete logarithm in  $E(\mathbb{F}_{q^f})$  can be reduced to the discrete logarithm in  $\mu_p$  in the field  $\mathbb{F}_{q^{fm}}$  where  $m$  is the smallest integer such that the trace of  $\pi^{fm}$  becomes congruent to 2 modulo  $p$ .*

Sometimes one can enforce these conditions (after a small extension) by using endomorphisms of small norm, e.g. if  $E$  is supersingular.

## Open Questions

- Can we compute more dualities between interesting groups in polynomial time?
- How is the balance between efficiency and security?
- Are the pairings one-way-functions?
- Can we use more general cohomology groups (e.g. motives attached to specific abelian varieties) for multilinear structures?

## 6 Classical Discrete Logarithms: Computing in Brauer groups

### 6.0.1 Cyclic Algebras

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

$$(\sigma, a)$$

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

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

## 6.1 Local fields

### 6.1.1 Frobenius

Let  $K$  be complete with a discrete valuation  $v$ , a finite residue field  $k$  with  $q = l_0^d$  elements and with Galois group  $G_K$ . For instance:  $K = \mathbb{Q}_{l_0}$  and  $k = \mathbb{Z}/l_0$ .

Let  $\pi$  be the Frobenius automorphism of  $k$ .

Let  $L_u$  be the unique unramified extension of  $K$  of degree  $p$ . We can lift  $\pi$  in a canonical way to an element of the Galois group of  $L_u/K$ .

### 6.1.2 Invariants

The key results of local class field theory are:

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

$v(a) \in \mathbb{Z}/p\mathbb{Z}$  is the **invariant**  $inv(c)$  of  $c$ .

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

For cyclic algebras two cases occur:

1)  $c$  is given by a pair  $(\tau, a)$  and  $\tau$  is another generator of  $G(L_u)/K$ . We have to determine  $n$  with

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

2)  $c$  is given by  $(\sigma, a)$  with  $\sigma$  a generator of a ramified extension of degree  $p$ . We have to find an equivalent pair of the form  $(\pi, b)$ .

(This is the case coming out of the Tate pairing.)

For both cases we have to solve discrete logarithms in finite fields.

## 6.2 Global fields

### 6.2.1 The Hasse-Brauer-Noether sequence

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

We get the most important exact sequence

$$0 \rightarrow Br(K)[p] \xrightarrow{\oplus_{v' \in \Sigma_K} \rho_{v'}} \bigoplus_{v' \in \Sigma_K} Br(K_{v'})[p] \xrightarrow{\Sigma_{v' \in \Sigma_K} \text{inv}_{v'}} \mathbb{Z}/p \rightarrow 0.$$

where  $\Sigma_K$  is the set of equivalence classes of valuations of  $K$ .

### 6.3 Index-Calculus in Brauer groups

Assume that  $A_v$  is a cyclic algebra corresponding to  $c_v \in Br(K_v)_p$ .

Lift  $A_v$  to a cyclic algebra  $A$  defined over  $K$  and use the equation

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

to get relations.

For the lifting we need

**existence theorems**

for cyclic extensions of  $K$  with prescribed ramification delivered by

**global class field theory**

(in an explicit way e.g. by CM theory).

## 7 Example: $K = \mathbb{Q}$

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

**Theorem 1 (Kronecker–Weber)** *Every abelian extension  $K/\mathbb{Q}$  of  $\mathbb{Q}$  is contained in a easily determined cyclotomic extension  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ .*

*There exists an extension  $K/\mathbb{Q}$  of degree  $l$  ramified exactly at  $p$  iff  $l|p-1$  holds. If it exists it is uniquely determined.*

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

## 7.1 The Algorithm

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

$$\text{inv}_p(a) + \sum_{q \neq p} f_q n_q \equiv 0 \pmod{l}. \quad (1)$$

Here the factors  $f_q$  are defined as follows:

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

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

Let  $\sigma$  denote the fixed generator of  $G$ .

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

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

**Definition 7.1** *A natural number  $n \in \mathbb{N}$  is  $M$ -smooth iff the following holds:*

$$q \text{ prime, } q|n \Rightarrow q \leq M.$$

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

**Theorem 2** *Let  $\varepsilon$  be an arbitrary positive constant, then we have uniformly for  $x \geq 10$  and  $y \geq (\log x)^{1+\varepsilon}$ :*

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

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

### 7.1.1 One algorithm for $K = \mathbb{Q}$

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

Let  $d$  be the smallest number  $\geq \sqrt{p}$ .

For  $\delta \in L := [0, \dots, l]$  take

$$a_1(\delta) := d + \delta.$$

$$a_2(\delta) := c_0 + 2\delta \cdot d + \delta^2)$$

$$(\equiv a^2 \text{ modulo } p)$$

with  $c_0 = d^2 - p$ .

**Assume** that for  $\delta \in L$  both  $a_1(\delta)$  and  $a_2(\delta)$  are  $M$ -smooth. Then we get a relation for the  $f_q$  for  $q$  in the factor base.

To find such  $\delta \in L$  we can use sieves.

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

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