

The Future of the Discrete Logarithm

Gerhard Frey
Institute for Experimental
Mathematics
University of Essen
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 on orbits:

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 .

Note:

The private keys are elements in B , the common secret is an element in A , the parameters are B and a chosen base point in an B -orbit 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 $\phi(a)$.

Open Question:

Analysis of security in terms of protocols and properties of B, μ, ν .

Obvious: There must be a very good randomization and the complexity to find for random $a \in A, c \in C$ a $\phi \in D \subset Hom_{set}(A, C)$ with $\phi(a) = c$ has to be big.

1.3 (Only) known realization

A a cyclic group of prime order p
embedded into \mathbb{N}

by a numeration.

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

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

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

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

$\nu =$ addition of automorphisms

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

The security considerations 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

$$a_2 = a_1^n.$$

Open Questions:

Are there other usable structures avoiding the known generic attacks?

Can one use group sets or permutation representations?

It is easily seen how to generalize the frame to (principal) homogeneous spaces. Does this give new aspects?

Are there no group-like structure at all?

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 .¹

¹By using a more general module structure, namely metrisised modules (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 $| Pic(O) |$.

2.1 Used Systems

- $\mathcal{B} = \mathbb{Z}$, and \mathcal{O} is an order or a localization of an order in a number field
- $\mathcal{B} = \mathbb{F}_p[X]$, and \mathcal{O} is the ring of holomorphic functions of a curve defined over a finite extension field of \mathbb{F}_p .

2.1.1 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 $a = c$.

2.1.2 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 .

Open Question:

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.

Can this structure be used (as in the case of elliptic curves) 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 ϕ is trivial.

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

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

but

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

Example

Assume that there is a cover

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

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

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

Then ϕ is an isomorphism.

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

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**.

The parameters for geometric systems are:

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

There are about $p^{3g \cdot n}$ curves of genus g over \mathbb{F}_{p^n} .

By Weil's theorem we get a fairly good estimate for $|Pic(O)|$ and so for the choice of these parameters.

But what about security?

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 ρ -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 (maybe 4)**.

Remark:

The worst case is $\alpha = 0$, and then the DL-system is obviously broken. We do not have a generic attack to Picard groups which leads to this case. But there are **special cases** of this type: Systems based on G_a have this property.

Are there others?

3.3 Remaining Problems

3.3.1 Perfection

Systems built on curves of genus 1,2,3 are promising.

So one should try to establish most efficient addition formulas for (not only) hyperelliptic curves of genus 2 and 3.

(cf. work of Harley, Lange, Chao, Pelzl,...)

3.3.2 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

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 Π acting on vector spaces related to the geometry of C and J_C :

Computation of the L-series of C/k .

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

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

Methods:

- l -adic Methods:
Use étale cohomology for small prime numbers l and then the Chinese remainder theorem (Schoof's algorithm)
- \mathfrak{p} -adic Methods:
Use rigid \mathfrak{p} -adic analysis and corresponding cohomology theories (Sato, Gaudry-Harley-Mestre, Kedlaya, Lauder-Wan)

Result: One can count very efficiently points on elliptic curves over all finite fields, points on hyper(super-)elliptic curves over fields of small characteristic, and (near future?) on random curves of genus 2 (Gaudry).

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 2 and 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).

But in other cases it is hard to give criteria, and there are more and more examples (“GHS-attack”, many other examples (e.g. by Diem-Scholten)).

Open Problems:

- Are there possibilities of trap doors?
- What about tori?

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:

²It is obvious how to generalize bilinear to multilinear

- The DL-system A is at most as secure as the system B .
- Given a (random) element a and $a_1, a_2, a_3 \in \langle a \rangle$ one can decide in polynomial time (in $\log |B|$) whether (simultaneously)

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

holds.

This 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.

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 precisely in terms of the trace of the Frobenius automorphism.

Sometimes one can enforce these conditions (after a small extension) by using endomorphisms of small norm.

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?