

Discrete Logarithm Systems - Where are We??

Gerhard Frey
Institute for Experimental
Mathematics
University of Essen
e-mail: 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.

After an intensive research since 25 years
(Diffie-Hellman)
these criteria can be analysed quite sa-
tisfyingly in the case of **DL-systems**.

I shall not go into the analysis of pro-
tocols (we had a lot of talks during ear-
lier ECC-workshops and shall have so-
me during this one).
I shall speak on the mathematical part.

Assume that we have a function

$$\oplus : A \times A \rightarrow A$$

where A is a finite subset A of \mathbb{N} which is associative and which satisfies the following conditions:

1. The size of $a \in A$ is bounded by $c \cdot \log |A|$ where $c \in \mathbb{R}$ is small (e.g. $1 + \epsilon$)
2. The computation of \oplus is very fast.

Then we can define the function

$$\mathbb{N} \times A \rightarrow A$$

$$e(n, a) := n \circ a := a \oplus \cdots \oplus a \text{ (n times)}$$

$$\text{with } e(n_1, e(n_2, a)) = e(n_1 \cdot n_2, a),$$

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

.

Use these equations for key exchange and de-and encryption protocols and signatures.

Definition

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

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

is a **Discrete Logarithm System (DL-systems) of exponential security** $C \in \mathbb{R}_{>0}$ if for random elements $a, b \in A$ the computation of $\log_a(b)$ has (probabilistic) complexity $\geq e^{C \cdot \log(|A|)}$.

AIM

Construct DL-systems with large C .

1.1 Bilinear Structures

Assume that (B, \circ) is another DL system and that

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

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

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

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

- $Q(a_1, a_2) = Q(a_1, a')$ iff $a_2 = a'$
- $Q(., .)$ is non degenerate.

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

There are two immediate consequences:

- The DL-system (A, \circ) is at most as secure as the system (B, \circ) .
- Given a (random) element a and $a_1, a_2, a_3 \in \mathbb{N} \circ a$ one can decide in polynomial time (in $\log |B|$) whether (simultaneously)
 $a_1 = n_1 \circ a, a_2 = n_2 \circ a, a_3 = (n_1 \cdot n_2) \circ a$ holds.

We shall see examples for such a structure.

This are negative aspects of bilinear DL-systems but very interesting protocols due to Joux (tripartite key exchange) and Boneh use such structures in a positive way.

2 Realization of Discrete Logarithms:

2.1 Groups with numeration

The only known way to find a DL-system nowadays is by use of groups.

Let (G, \times) be a finite group.

Definition 2.1 *A numeration (A, f) of G is a bijective map*

$$f : G \rightarrow A$$

where A is a finite subset of \mathbb{N} containing 1.

*A **presentation** of an abstract finite group G is an embedding of G into a group with numeration.*

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

Define

$$\oplus : A \times A \rightarrow A$$

by

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

Then

$$e(n, a) = f(n \circ f^{-1}(a)).$$

Remark:

We require that \oplus is rapidly computable *without* the knowledge of f^{-1} and the security and the efficiency of the DL-System based on \oplus will depend crucially on f .

From now on we assume that we have a numeration f of G and identify G with its presentation given by f .

One sees immediately (Chinese remainder theorem and p-adic expansion) that we have to assume that the group order of G is a prime p or that $|G|$ is not computable.

We shall assume the first case in the following and so G has a prime order p .

We use the algebraic structure “group”.

This allows “generic” attacks:

Example: **Pollard’s ρ -Algorithm.**

Consequence: C is bounded by $\approx 1/2$.

Encouraging: Generically this is a bound from below, too.

A BAD numeration:

$$G := (\mathbb{Z}/p, +) .$$

Numeration:

$$f(r + p\mathbb{Z}) := [r]_p$$

where $[r]_p$ is the smallest positive representative of the class of r modulo p .

Security:

The *Euclidean algorithm* solves this in $O(\log(p))$ operations in \mathbb{Z} :

Hence if we can transform the numeration f in polynomial time to this numeration the DL-system is broken.

3 Construction of Numerations by Class Groups

ALL systems used today rely on
the following construction:

Let O be a finitely generated algebra
over an euclidian ring.

Invertible ideals (or better: rank-1 pro-
jective O -modules) form an abelian group:

Recall: Let K be the quotient ring of O .

A non empty subset $A \subset K$ is an O -ideal
if it is closed under addition and under
multiplication by elements of O .

The product of two ideals A, B is given
by

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

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

The set of invertible ideals form a commutative group $I(O)$. To make it manageable we introduce an equivalence relation:

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

The subgroup of ideals equivalent to O are the principal ideals P_O and the quotient

$$Pic(O) := I_O/P_O$$

is the ideal class group of O .

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 .**

Needed properties of O :

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 directly for elements of $Pic(O)$ (Algebraic Geometry).

Before looking for such O we have to be aware of an ”**Generic attack**” for DL-systems based on $Pic(O)$:

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**.

The expected complexity is **subexponential**, i.e estimated 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 Existing Systems

What is used today?

Only two examples:

- $\mathcal{B} = \mathbb{Z}$, 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 .

Orders O in number fields where introduced by Buchmann-Williams 1988. In general they are rather difficult to handle (e.g. determining the group order) and it soon turned out that the index-calculus attack is efficient. So we shall restrict ourselves to mention the most practical example:

K is an imaginary quadratic field .

What is special about imaginary quadratic fields?

Theory of Gauß:

$Pic(O_K)$ corresponds to classes of binary quadratic forms with discriminant D .

Multiplication of ideals corresponds to composition of quadratic forms.

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 $a = c$.

The great disadvantage:

The index-calculus-attack works very efficiently:

(Under GRH:) The complexity to compute the DL in $Pic(\mathcal{O}_K)$ is

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

QUESTION: CAN WE AVOID THIS WEAKNESS WITHOUT LOSING THE ADVANTAGES?

3.2 The geometric case

$\mathcal{B} = \mathbb{F}_p[X]$, and \mathcal{O} is the ring of holomorphic functions of a curve 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 $\text{Quot}(\mathcal{O})$.

C is the desingularisation of the projective closure of the curve corresponding to \mathcal{O} .

This relates $\text{Pic}(\mathcal{O})$ closely with the points of the Jacobian variety J_C of C and explains the role of abelian varieties in crypto systems used today.

Genus-Zero-Case:

In order to have a non-trivial Pic-group we have to take a non-integrally closed O corresponding to a singular curve C' . We can realize DL-systems based on tori, especially on the multiplicative group (“classical” DL).

Example:

$$O := \text{Pic}(\mathbb{F}_q[X, Y]/(Y^2 + XY - X^3))$$

The affine curve behind is

$$Y^2 + XY = X^3$$

with function field $\mathbb{F}_q(u)$ where

$$\begin{aligned} X &= u/(1-u)^2 \\ Y &= u^2/(1-u)^3. \end{aligned}$$

Exercise:

$$\text{Pic}(O) = \mathbb{F}_q^*.$$

Now assume that O is integrally closed. The corresponding curve C_O is an affine part of C .

The inclusion

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

corresponds to a morphism

$$C_O \rightarrow \mathbb{A}^1$$

which extends to a map

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

$$\infty := \mathbb{P}^1 \setminus \mathbb{A}^1.$$

We shall assume that there is an \mathbb{F}_q -rational point P_∞ in $\pi^{-1}(\infty)$.

The **Jacobian of C**:

A divisor of C is a formal sum (with integral coefficients) of points on $C(\overline{\mathbb{F}}_q)$.

A divisor is principal if there is a function on C whose zeroes and poles (counted with multiplicities) are equal to this formal sum. A divisor has degree 0 if the sum of its coefficients is 0.

Let $Cl^0(C)$ be the set of classes of divisors of C of degree 0 modulo principal divisors. This set carries a natural geometric structure defined over \mathbb{F}_q :

the Jacobian variety J_C which is an abelian variety over \mathbb{F}_q with $J_C(\mathbb{F}_{q^n})$ equal to the set of formal sums of $G_{\mathbb{F}_{q^n}}$ -orbits of points on C of degree 0 modulo principal divisors.

Relation between points and ideals:

Let P be a point on C_O and

$$M_P = \{f \in O, f(P) = 0\}.$$

M_P is a prime ideal in O and the map $P \mapsto M_P$ gives a one-to-one correspondence between Galois orbits of points (over $\bar{\mathbb{F}}_q$) of C_O and maximal ideals of O .

Hence there is a canonical map

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

which is surjective but not always injective. Its kernel is generated by sums of points in $\pi^{-1}(\infty)$.

If the kernel of ϕ is trivial or not interesting then we can use the ideal interpretation for computations and the abelian varieties for the structural background.

- Addition is done by ideal multiplication.
- The choice of ideals in classes uses the Riemann-Roch theorem on curves.

but key generation like computation of orders uses properties of abelian varieties.

Basic 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 for which $d = 2$.

We have the following parameters

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 $Quot(O)$.

Structural relation: Hasse-Weil

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

The **key length** is $n \cdot \log(p) \cdot g$.

QUESTION:

Which parameters lead to efficient and secure systems?

3.2.1 Hyperelliptic curves

We shall have a closer look at hyperelliptic curves. Assume that we have a \mathbb{F}_q -rational Weierstraß point P_∞ .

$$O = \mathbb{F}_q[X, Y]/f_C(X, Y)$$

where $f_C(X, Y)$ is a polynomial of degree 2 in Y and of degree $2g + 1$ in X .
 $J_C(\mathbb{F}_q) = \text{Pic}(O)$.

Very similar situation as in the case of class groups of imaginary quadratic fields.

Gauß - Artin - Cantor:

Connect $\text{Pic}(O)$ with reduced quadratic forms of discriminant $D(f)$ and the addition \oplus with the composition of such forms: **Cantor algorithm**.

Performance:

Best for elliptic curves, good for $g = 2, 3$ (sometimes with additional structures) and becoming worse with growing genus.

Negative aspect

Subexponential attack based on the index-calculus principle.

One essential difference to number fields: The subexponential function is a function of the order of the class group and so of q^g .

But in all known index-calculus algorithms one can **not** look at q and g as **independent** variables.

For instance: If $g = 1$ fixed then we do not get a subexponential attack for $q \rightarrow \infty$!

To understand this we have a short look at **the attack**¹:

Generically ideal classes of O can be represented by two polynomials with maximum degree g .

Choose as factor base the ideal classes which can be represented by polynomials of smaller degrees .

For $g = 1$ this is not possible.

This motivates why the attack becomes more and more efficient if we fix q and let g grow.

¹It works for all orders related to curves and is not restricted to hyperelliptic curves

More precisely (cf. Adleman, DeMarrais and Huang, Müller-Stein-Thiele, Engestein:)

For $g/\log(q) > t$ the DL in $Pic(O)$ can be computed with complexity bound

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

A slightly different approach of Gaudry (cf. ECC 2000) results in an **exponential attack which is very efficient for small genus**. Its complexity is for fixed genus

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

but it grows with $g!$.

“Result”: Orders related to curves with rational Weierstraß points of genus ≥ 4 or closely related abelian varieties should be avoided!

State of the art:

We have three types of rings O which avoid serious index-calculus attacks and for which $Pic(O)$ is manageable:

MAXIMAL ORDERS BELONGING TO CURVES OF GENUS 1,2,3 !

Their performance is excellent, the key lengths of secret and public keys and the length of signatures are optimal and they are resistant against the “generic” index-calculus attacks.

Are there other attacks?

We have used abelian varieties as structure, and so we have

4 Tate duality

This duality \langle , \rangle is defined over every field K and relates abelian varieties A 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

- \langle , \rangle 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, A is the Jacobian of a curve and has good reduction modulo the maximal ideal of K .

Remark:

Class field theory can be used to compute DL's in Brauer group of local and global fields and to explain all known attacks on the DL in finite fields including the number field and function field sieves (cf. Thesis Kim Nguyen, Essen 2001).

In general the conditions that K contains p -th roots of unity **and** $A(K)_p \neq \{0\}$ will not be satisfied at the same time.

For elliptic curves we can formulate this more precisely:

Corollary

Let E be an elliptic curve defined over \mathbb{F}_q and p a prime. Let π_p 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 π_p^f is congruent to $q^f + 1$ modulo p .

The corresponding discrete logarithm in $E(\mathbb{F}_{q^f})$ can be reduced to the discrete logarithm in μ_p in the field $\mathbb{F}_{q^{fm}}$ where m is the smallest integer such that the trace of π_p^{fm} becomes congruent to 2 modulo p .

Sometimes one can enforce these conditions (after a small extension).

Assume that there is an endomorphism η of A with

-

$$\langle P_0 + pA(k), \eta(P_0) \rangle = \zeta_p$$

- η can be computed in polynomial time.

Then the decision problem related to P, Q, R reduces in polynomial time to the equality test of $\langle R + pA(k), \eta(P_0) \rangle$ and $\langle P + pA(k), \eta(Q) \rangle$ in k .

So we have to be careful in the choice of our parameters in order not to be related with genus 0—curves even if we begin with curves of genus 1,2, and 3. What about the choice of n ?

4.1 **Scalar Restriction**

As outlined at ECC 1998 and worked out very nicely over fields of characteristic 2 of composite degree by Galbraith, Gaudry, Hess, Smart (1999) and in new papers (2001) by Jacobson-Menezes-Stein and again Galbraith-Hess-Smart² we can transfer DL's in many elliptic curves to DL's in Jacobians of curves for which the index-calculus method works .

²For 2^{104} (and perhaps more) elliptic curves over $\mathbb{F}_{2^{155}}$ the DL can be computed though it is resistant against the other attacks.

The general case is discussed in the thesis of C. Diem, Essen 2001) and in theory and in practice. It becomes clear that one cannot just copy the $\text{char}(k) = 2$ -case to the general case but that one has to expect similar attacks.

So again: Be careful with the choice of the parameter n .

For instance take $n \leq 3$ or n equal to a large prime which should not be a Mersenne prime.

5 Key Generation

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.

Usually the determination of P_0 is not so difficult if C is known.

To find (k, C) one uses mostly 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 mathematically most interesting. The key to it is to determine the characteristic polynomial of the Frobenius automorphism Π acting on vector spaces related to the geometry of C and J_C . In other words:

Compute the L-series of C/k resp. J_C/k . Examples for representation spaces are spaces of holomorphic differentials or more generally of differentials with prescribed poles and cohomology groups. Here in our context de Rham cohomology, étale cohomology and crystalline cohomology are especially interesting.

There are most important theorems (Deligne-Weil, Lefschetz) saying:

- Let Π operate on the étale or crystalline cohomology groups as above. Then its characteristic polynomial is independent of the choice of the cohomology and is a monic polynomial with coefficients in \mathbb{Z} . It is used to define the Zeta-series of C .
- The Lefschetz fixed point formula is used to compute $|Pic(O)|$ as special value of the Zeta-series of C .

5.0.1 Constant Field Extensions

Since the Frobenius automorphism of field extensions of degree n of \mathbb{F}_q is the n -th power of the Frobenius over \mathbb{F}_q its characteristic polynomials on objects related to $C \times \mathbb{F}_{q^n}$ is easily computed from the corresponding one of Π .

5.1 l -adic Methods

To realize these representations one uses the result that the étale cohomology is isomorphic to the Tate-modules of A w.r.t. primes l different from $\text{char}(\mathbb{F}_q)$.

Since Tate-modules $T_l A \text{ mod } l$ are just the the l -torsion points of A , and on this fact the strategy of Schoof's algorithm relies:

compute the Frobenius action modulo small primes l (and their powers if possible) and then use the Chinese remainder theorem to determine the L-series.

This algorithm is in general *in principle* polynomial (in $n \cdot \log p$) but in practise not working fast enough without further tricks (Atkins-Elkies for elliptic curves) so that nowadays we can use it only to count the points on randomly chosen elliptic curves in cryptographic relevant regions. The reason for the higher efficiency in the elliptic curve case is that we can “easily” decide whether elliptic curves have isogenies of a given degree (and they have many!).

Result:

It is no problem to determine cryptographically strong random elliptic curves over random ground fields rapidly. For curves of higher genus l-adic methods do not work fast enough till now.

5.2 \mathfrak{p} -adic Methods

As in the case of the Tate pairing lift the geometric objects like curves or Jacobians to \mathfrak{p} -adic fields K with residue field \mathbb{F}_q .

The crucial step is to lift the Frobenius automorphism Π .

Note: Π plays two roles over finite fields: It is an element of the Galois group of \mathbb{F}_q **and** it is an endomorphism of Jacobians resp. cohomology groups.

The lifting as element of the Galois group is easy.

The lifting as endomorphism is difficult and not always possible.

Typical complexity (when the method works):

Exponentially in the characteristic of the residue field but but the degree n contributes as a small power factor: so applications are for **small** characteristics p_0 of \mathbb{F}_q (and so for large n).

5.2.1 **Canonical liftings (Satoh, Gaudry-Harley-Mestre)**

Assume that A is an abelian variety over \mathbb{F}_q . If the ring of endomorphisms of A is “not too big” (e.g. commutative) there is a lifting of A to an abelian variety \tilde{A} over K with the same ring of endomorphisms.

Especially the Frobenius endomorphism and its dual, the Verschiebung V , can be lifted.

V has the same trace as Π , and it can be computed by evaluating isogenies of degree p_0 .

\tilde{A} and V is computed by \mathfrak{p} -adic approximation.

The method was applied first to ordinary elliptic curves by Satoh for $p_0 > 3$ and by Harley-Gaudry for all p_0 . By using “classical” properties of the arithmetical-geometrical mean Gaudry, Harley and Mestre can accelerate the method enormously and extend it to hyperelliptic curves.

5.2.2 Crystalline Cohomology: Work of Kedlaya

Following Monsky-Washnitzer we lift C \mathfrak{p} -adically **formally** to C^\dagger (we go from polynomial rings over \mathbb{F}_q to rapidly converging power series over the \mathfrak{p} -adics) and lift Π to C^\dagger . Its induced action on the Rham cohomology of C^\dagger gives the looked-for representation to which we can apply Lefschetz fixed points theorems.

This method works under certain conditions about geometric properties of C which are satisfied for hyperelliptic curves (and in many more situations, e.g. hypersurfaces or complete intersections).

An explicit description (in theory and as algorithm) for hyperelliptic curves can be found in

Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology by Kiran.S. Kedlaya, to appear soon, or in:

math.berkeley.edu/~kedlaya/math/index.html

5.3 Global lifting

Remaining open case: We want to count the element of $Pic(O)$ for underlying curves of genus larger than 1 in large characteristics.

The only working method today is a lifting to global fields in very special cases: C is such that its Jacobian has a lifting to a number field of small degree over \mathbb{Q} with a ring of endomorphism which contains either a lifting of Π or is at least not far away from it.

This means: C (resp. J_C) is the reduction mod \mathfrak{p} of a curve (an abelian variety) which has **real** or **complex** multiplication with an order in a number field of small class number.

Such a C is difficult to find over \mathbb{F}_q so following an idea of Atkin one begins with an appropriate endomorphism ring, construct a corresponding global curve and then uses for C the reduction of this curve. This idea can be applied to Jacobians of curves of genus 2,3 (Lecture of A. Weng).