

# Pairings

Lorentz Center Sept. 26-October 2, 2003

Gerhard Frey  
Institute for Experimental Mathematics  
University of Duisburg-Essen  
Ellernstrasse 29, D-45326 Essen, Germany  
`frey@exp-math.uni-essen.de`

September 30, 2003

# 1 Bilinear structures

## 1.1 DL-System

Let  $p$  be a prime and consider an injective map  $(\mathbb{Z}/p, +) \xrightarrow{f} \mathbb{N}$ .

Let  $A = \text{Im}(\mathbb{Z}/p)$  be the image of  $f$ .

$A$  becomes a group with the composition  $\oplus$  by the rule:

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

For an element  $P \in A$  and  $k \in \mathbb{N}$  we define

$$k \circ P = \underbrace{P \oplus P \oplus \dots \oplus P}_{k \text{ times}}.$$

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

Now fix a generator  $a_0 \in A$ .

For  $a \in A$  define

$$\log_{a_0}(a) := k \in \mathbb{N} \text{ with } k \circ a_0 = a.$$

Of course  $k$  is only defined modulo  $p$  and its class is called the discrete logarithm of  $a$  with respect to the base  $a_0$ . In the following we call  $(A, \circ)$  a DL-system.

We want to use it as crypto primitive for public key systems and so we assume that we can compute in  $A$  efficiently (measure:  $\log(p)$ ) and that the computation of the discrete logarithm for random elements  $a$  is difficult, i.e. the computational Diffie-Hellman problem

For random  $a \in A$  compute

$$\log_{a_0}(a) \text{ (CDH)}$$

is hard.

For many applications an even stronger condition is needed:

For random triples  $(a_1, a_2, a_3)$  decide whether

$$\log_{a_0}(a_3) = \log_{a_0}(a_1) \log_{a_0}(a_2). \\ \text{(DDH)}$$

## 1.2 Definition

Let  $(A, \circ)$  be a *DL*-system.

**Definition 1.1** *Assume that there is a group  $A'$  in which we can compute “as fast” as in  $A$ . Assume moreover that  $(B, \circ)$  is another *DL* system and that a map*

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

*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
 
$$Q(n_1 \circ a_1, n_2 \circ a'_2) = n_1 \cdot n_2 \circ Q(a_1, a'_2)$$
- $Q(., .)$  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.

## Most important examples:

1.) Let  $V$  be a vector space over  $\mathbb{F}_p$  with bilinear map  $\phi$  which maps  $V \times V$  to a  $\mathbb{F}_p$  vector space  $W$ .

Take  $a_0 \in V$ ,  $A = \langle a_0 \rangle$  and

$$\langle a_0 \rangle^\perp := \{v \in V \text{ with } \phi(a_0, v) = 0_W\}.$$

Take  $a'_0 \in V \setminus \langle a_0 \rangle^\perp$ ,  $A' := \langle a'_0 \rangle$ ,

$B := \phi(\langle a_0 \rangle, \langle a'_0 \rangle)$  und  $Q =$

$$\phi|_{A \times A'}.$$

2.) A little more general:

Let  $\varphi : V \rightarrow V'$  be a (computable(!))

linear map and

$$\phi' : V \times V' \rightarrow W$$

bilinear. Define

$$\phi := \phi' \circ (id_V \times \varphi)$$

and then proceed as in example 1.

### 1.3 Transfer of DL

The DL-system  $(A, \circ)$  is at most as secure as the system  $(B, \circ)$ .

For take random  $a' \in A'$   
and denote  $b_0 := Q(a_0, a')$ .

Then the map

$$\begin{aligned} \langle a_0 \rangle &\rightarrow \langle b_0 \rangle \\ a := n \circ a_0 &\mapsto Q(a, a') \end{aligned}$$

is a monomorphism of numerated groups,  
and the claim follows.

## 1.4 DDH

Assume that

$$A = A'$$

and hence

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

Then for all triples  $(a_1, a_2, a_3) \in \langle a_0 \rangle$  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. For we can use the identities

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

$$Q(a_3, a_0) = \log_{a_0}(a_3) Q(a_0, a_0).$$

## 1.5 Tripartite Key Exchange

The following is a nice idea of A. Joux (ANTS 4).

Parties  $P_1, P_2, P_3$  want to create a common secret.

We assume that we have  $A$  with bilinear structure  $Q$  on  $A \times A$ .

Each partner  $P_i$  chooses a secret number  $s_i$  and publishes

$$a_i := s_i \circ a_0.$$

Hence every partner can compute

$$s_1 \circ Q(a_2, a_3) = s_2 \circ Q(a_1, a_3) = s_3 \circ Q(a_1, a_2),$$

the common secret.

## (Semantical) Security needs

1. hardness of the (computational) DL problem in  $A$
2. hardness of the following problem called Bilinear Diffie-Hellman-Problem (BDH):  
For  $(a, a_1 = n_1 \circ a, a_2 = n_2 \circ a, a_3 = n_3 \circ a)$  compute  $n_1 n_2 n_3 \circ Q(a, a)$ .

## 1.6 Identity based Protocol

This is an old dream (of Shamir):  
One wants to send an encrypted message to a certain person without building up a public key environment but by the **use of one's identity** and some trusted institution  $TA$  which **computes a secret key** and the related public one (and the public key does not give information about the identity!)

We shall assume that we have a DL-system  $A = \langle a_0 \rangle$  with  $A' = A$ .

We shall explain an idea of **Franklin and Boneh**: how to use it to come nearer to the dream.

We have a sender  $P$  who wants to transmit a message  $m$  to the receiver  $Q$ . We shall assume that  $m \in (\mathbb{Z}/2)^n$ .

He uses the service of  $TA$ .

**Setup:**

There are two publicly known hash functions

$$G : \mathbb{N} \rightarrow A$$

and

$$H : B \rightarrow (\mathbb{Z}/2)^n.$$

$TA$  chooses  $s$ , the master key, and publishes  $a_{pub} := s \circ a_0$ .

## Generation of keys:

$P$  sends (after authentication) an element  $ID \in (\mathbb{Z}/2)^n$  representing his identity to  $TA$ .

$P$  (or  $TA$ , or the sender) computes

$$a_{ID} := G(ID) \in A$$

and then as

“public key” of  $P$

$$b_{ID} := Q(a_{ID}, a_{pub}).$$

$TA$  generates the “private key”

$$s_{ID} := s \circ a_{ID}$$

of  $P$ .

## Encryption:

The message is  $m \in (\mathbb{Z}/2)^n$ .

Choose  $r$  randomly and compute

$r \circ a_0$  and  $r \cdot b_{ID}$

and send the ciphertext

$C := (r \cdot a_0, m \oplus H(r \cdot b_{ID}))$ .

## Decryption:

Let  $(U, V)$  be a cyphertext.

$P$  computes

$T := H(Q(s_{ID}, U))$ .

Then  $m = V \oplus T$ .

Proof:

Since  $V = m \oplus H(r \cdot b_{ID})$  we have to show that  $Q(s_{ID}, U) = r \cdot b_{ID}$ .

But

$$\begin{aligned} Q(s_{ID}, U) &= Q(s \circ a_{ID}, r \cdot a_0) \\ &= r s Q(a_{ID}, a_0) = r \cdot Q(a_{ID}, s \circ a_0) = r \cdot b_{ID}. \end{aligned}$$

**(Semantical) Security**

needs again the hardness of (BDH).

## Work to do:

Assume that  $TA$  has done the original setup and has published

$A, B, Q, G, H, a_0, a_{pub}$ .

To serve  $P$  it has to perform one scalar multiplication in  $A$  (with fixed argument  $a_0$ ).

The **sender** has to compute  $b_{ID}$  by one application of  $Q$  with one argument ( $= a_{pub}$ ) independent of  $P$ , one scalar multiplication in  $A$  of a fixed element ( $a_0$ ) and one scalar multiplication in  $B$  with argument depending on  $ID$ .

$P$  has to get his private key from  $TA$  and to compute  $Q$  (with one argument independent of the message and the sender).

In all cases precomputation is possible to accelerate the computation.

Advantage:

For the **sender**: He can send a message to a receiver who does not have a public key system before. (But he has to be sure that there is a TA which will communicate with  $P$ .)

For the **receiver**  $P$ : He has not to have a public or private key but only a ID before a message comes. So for instance  $TA$  could become active **after** a message arrives.

Big disadvantage:

$TA$  knows everything since it has the master key  $s$ .

One case is interesting:

$P$  is his own  $TA$  and creates different public keys with one master key and different identities, e.g. on laptops.

## 2 Realization

Very popular realizations of DL-systems are embeddings of  $\mathbb{Z}/p$  into the rational points of commutative group schemes over finite fields  $\mathbb{F}_q$ .

One example is the multiplicative group  $G_m$ . There is an index-calculus attack to the (CDH) in  $\mathbb{F}_q^*$  which is subexponential.

The other examples are Jacobians of curves of genus 1,2,3 and closely related abelian varieties.

As discussed yesterday there is a duality theory of abelian varieties and Jacobians are self dual.

The duality is closely related to the **Weil pairing** on torsion points or their projective limit, Tate-modules.

In fact, the Weil pairing is one possibility to construct a bilinear structure on DL systems inside of abelian varieties.

We shall concentrate ourselves on a derived pairing .

The definition is more involved but it has nicer properties especially for higher dimensional varieties.

It is the **Tate pairing**. It was explained yesterday for elliptic curves.

It is defined for abelian varieties  $A$  (which we assume to be principally polarized) over every field  $K$  and uses Galois cohomology applied to the Kummer sequence

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

We get the exact sequence

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

Next we use that  $A(K_s)[p]$  is self dual as  $G_K$ -module (here the Weil pairing plays its role) and so we can use the cup product to get the *Tate-pairing*

$$\begin{aligned} \langle, \rangle_K: A(K)/pA(K) \times H^1(G_K, A(K_s))[p] \\ \rightarrow H^2(G_K, \mu_p) \end{aligned}$$

given by

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

Let  $K$  be a **local field** (e.g. a p-adic field) and let  $A$  have good reduction modulo the valuation ideal of  $K$ . We change notation:  $A \mapsto \tilde{A}$  and the reduction is denoted by  $A$  defined over the residue field  $\mathbb{F}_q$ . Recall the theorem of Tate that  $\langle, \rangle$  is not degenerate.

For further use we have to analyze the groups occurring.

## Classes modulo $\mathfrak{p}$

We shall assume that  $p$  does not divide  $q$  and that  $A(\mathbb{F}_q)$  has no points of order  $p^2$ . Using Hensel's lemma we get

$$\tilde{A}(K)/p\tilde{A}(K) \approx A/(\mathbb{F}_q)/pA(\mathbb{F}_q)$$

and this group is isomorphic to  $A(\mathbb{F}_q)[p]$ .

$\mathbf{H}^1$  :

To compute  $H^1(G_K, A(K_s))[p]$  we use that unramified extensions of  $K$  do not split elements in this group and that therefore a well known inflation-restriction sequence reduces the computation of this group to the computation of **Frobenius-invariant** elements in

$$\text{Hom}(G(K_{\text{tame}}/K^{\text{unr}}), A[p]).$$

After fixing a generator  $\tau$  of  $G(K_{tame}/K^{unr})$  we can identify

$$\phi \in \text{Hom}(G(K_{tame}/K^{unr}), A[p])$$

with

$$\phi(\tau) =: P_\tau \in A[p]$$

and hence with  $A[p]$  but be aware that the Frobenius acts in general both on  $G(K_{tame}/K^{unr})$  and on  $A[p]$ . Here the cyclotomic character becomes important: Over  $K(\zeta_p)$  we can realize a ramified cyclic extension of degree  $p$  by taking a  $p - th$  root of a uniformizing element of  $K$ .

## Example:

Assume that  $A[p](\mathbb{F}_q)$  cyclic of order  $p$  and generated by  $P$ .

1. Assume that  $p|(q-1)$ .

Then  $H^1(G_K, A)[p] = A[p](\mathbb{F}_q)$ , and  $\langle P, P_\tau = P \rangle \neq 0$ .

2. Assume that  $p$  does not divide  $q-1$ .

Then  $\phi$  with  $\phi(\tau) = P$  is not in  $H^1(G_K, A)[p]$ . Especially " $\langle P, P \rangle$ " is not defined.

If  $A[p](\mathbb{F}_q)$  is not cyclic and  $p|q-1$  then for all points  $P, Q \in A[p](\mathbb{F}_q)$  we can form  $\langle P, Q \rangle$  but it is not clear whether there is a  $P$  with  $\langle P, P \rangle \neq 1$ .

## The Brauer group

$H^2(G_K, \mu_p)$  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*  $Br(K)$  of  $K$ . Its elements can be represented by cyclic algebras which become isomorphic to matrix algebras after an extension of degree  $p$ .

There is an isomorphism

$$inv : Br(K)[p] \rightarrow \mathbb{Z}/p\mathbb{Z}.$$

where  $inv$  relates to cyclic algebras their invariants.

Hence the DL in  $Br(K)[p]$  would be trivial if we could compute invariants.

Let  $\pi$  be the Frobenius automorphism of  $k$  and 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  $L_u/K$ .

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  $p$ .

This looks promising. But for cyclic algebras two cases will occur:

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

In both cases we get a close relation to the discrete logarithm in  $\mathbb{F}_q$ .

**Assume now that  $p|q-1$ .** Let  $L$  be as above be a cyclic ramified extension of degree  $p$ . Then the Tate pairing ends in  $H^2(G(L/K), L^*)$ , and elementary computations with cohomology groups yield that this group is isomorphic (canonically after the choice of  $\tau$ ) to  $\mathbb{F}_q^*/\mathbb{F}_q^{*p}$ .

So we finally get in this special case from the Tate pairing the non degenerate pairing

$$\langle, \rangle: A[p](\mathbb{F}_q) \times A[p](\mathbb{F}_q) \rightarrow \mathbb{F}_q^*/\mathbb{F}_q^{*p}.$$

## 2.1 Computation

Now assume that  $A$  is the Jacobian  $J_C$  of a curve  $C$ . We can compute  $\langle, \rangle$  in the case that  $p|q - 1$  analogous as explained for elliptic curves:

Let  $P_1, P_2$  be points of  $\tilde{A}(k)$  with  $P_2$  a point of order  $p$ . Represent  $P_i - P_0$  by coprime divisors  $D_i$  in the divisor class group of  $C$ , and let  $f_2$  be a function on  $C$  with divisor  $p \cdot D_2$ .

Then

$$\langle P_1 + p \cdot J_C(k), P_2 \rangle = f_2(D_1) \cdot k^* / k^{*p},$$

and the evaluation of  $f_2(D_1)$  is done in  $O(\log(p))$  steps.

Background: Mumford's Theta groups which describes extensions of (finite subgroups of) abelian varieties by linear groups.

Basic step:

for positive divisors  $A_1, A_2$  of degree  $g$   
find a positive divisor  $A_3$  and a function  $h$  on  $C$  with

$$A_1 + A_2 - A_3 - gP_0 = (h).$$

Recall:

We have a birational morphism,  $\phi_g$ , between the  $g$ -fold symmetric product of  $C$  and  $J_C$ .

Let  $S$  be a subset of  $J_C(k)$ . A divisor  $E$  of  $C$  is called prime to  $S$  if it is prime to all divisors in  $\phi_g^{-1}(s)$ ,  $s \in S$ .

Let  $S$  is a finite subgroup of  $J_C$  and  $E$  prime to  $S$ . Define the following group law on  $S \times k^*$ :

$$(s_1, a_1) \circ (s_2, a_2) := (\phi_g(A_3), a_1 a_2 \cdot h(E)),$$

where  $A_3, h$  are computed as above with  $A_i = \phi_g^{-1}(s_i)$ . The assumptions on  $E$  guarantee that  $h(E) \in k^*$ . The degree of  $h$  is at most  $g$ , and so the evaluation is polynomial in  $g \cdot \log |k|$ .

Apply this to:  $S = \langle \bar{D} \rangle$  with  $D$  an element of order  $p$  in  $J_C(k)$  and  $D \in \bar{D}$  be a divisor of the form  $D = A - gP_0$ ,  $E$  be a divisor of degree 0 on  $C$  prime to  $S$ .

By induction: The  $p$ -fold application of  $\circ$  gives the result  $(0, f(E))$ , where  $f$  is a function on  $C$  with  $(f) = pD$ .

Now use the group structure on  $\langle \bar{D} \rangle \times k^*$  and apply the square- and multiply algorithm to evaluate  $f$  at  $E$  in  $O(\log(p))$  group operations.

### 3 Applications

**Consequence:** We can reduce the discrete logarithm in  $A(K)/pA(K)$  to the discrete logarithm in  $Br(K)_p$  with costs  $O(\log(|\mathbb{F}_q(\zeta_p)|))$ , and we can solve (DDH) if we can decide equality in  $\mathbb{F}_q(\zeta_p)$ .

So this is no practical result if

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

is large.

In general, the conditions that  $K$ , and hence the residue field  $\mathbb{F}_q$ , contains  $p$ -th roots of unity *and* that  $A$  has points of order  $p$  rational over  $\mathbb{F}_q$  which are cryptographically interesting will not be satisfied at the same time.

For elliptic curves we can formulate this more precisely:

**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  $\langle \zeta_p \rangle$  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  $p$ .*

To **avoid** elliptic curves with small  $k$  is easy.

To **construct** elliptic curves with small  $k$  is an interesting diophantine problem. There is one family of elliptic curves for which these statements are wrong:

**Supersingular Elliptic curves**

The trace of the Frobenius acting on such curves is divisible by  $\text{char}(\mathbb{F}_q)$ , 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  $E[p](F_q) \neq 0$  then after an extension of degree at most 2 the  $p$ -th roots of unity are rational and hence  $k \leq 2$ .

For  $l_0 = 2$  one gets:  $k \leq 4$ , and for  $l_0 = 3 : l \leq 6$ .

The bound  $k = 6$  remains valid in general, too.

In general one has the

**Theorem 1** *Let  $A$  be a supersingular abelian variety of dimension  $g$  over  $\mathbb{F}_q$ , then there exists an integer  $k(g)$  such that, for all natural numbers  $r$ , the degree  $k$  is bounded by  $k(g)$ .*

One finds the number  $k(g)$  in papers of S. Galbraith. Cryptographically interesting are  $g = 2, 3$  with  $k(2) = 12$  and  $k(3) = 30$ .

As result we get:

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

Example:

Take a supersingular curve over a prime field. In order to get acceptable security the number  $p$  has to have about 500 bits.

By very special choices ( $\text{Char}(\mathbb{F}_q) = 3$ ) one can do better and work with about 200 bits as usual.

Going to Jacobians of curves of higher genus seems to have as result lower efficiency; and combination with scalar restriction (work of Rubin-Silverberg) again leads to rather restricted examples.

### 3.1 The role of isogenies

If we want to apply the bilinear structure to (DDH)(destructively) and to tripartite key exchange and  $ID$ -based systems (constructively) we need more: We really need a pairing on one group  $A$ .

As explained above the Tate pairing cannot be used directly.

But sometimes one can use the second type of the examples from above:

**Proposition 2** *Assume that there is an endomorphism  $\eta$  of  $A$  with*

- $\langle P_0 + pA(k), \eta(P_0) \rangle = \zeta_p,$
- $\eta$  can be computed in polynomial time.

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

**Example:**

Let  $E$  be a supersingular elliptic curve and assume that  $\mathbb{F}_q$  has odd degree over  $\mathbb{Z}/p$ . Assume moreover that there is an endomorphism of  $E$  which is not contained in  $\mathbb{Z} \cdot id_E$  and whose restriction to the points of order  $p$  can be computed in polynomial time (e. g.  $E : Y^2 = X^3 - X$  and  $\eta : X \mapsto -X, Y \mapsto \sqrt{-1}Y$ ). Then the conditions of the proposition are satisfied.

It is clear that both efficiency and security of the  $ID$ -system are critical. It would be much better to use ordinary elliptic curves with small  $k \approx 8$ . (cf. work of Dupont-Enge-Morain).

### 3.2 "The Gap"

The last application we mention is the construction of DL-systems in which (DDH) is weak (of polynomial complexity) but (CDH) is believed to be subexponentially hard.

The groups are points of order  $p$  in supersingular elliptic curves  $E$  over fields  $\mathbb{F}_q$  of odd degree over the prime field. The curves  $E$  have to be chosen in such a way that the order of  $E/(\mathbb{F}_q)$  is not a smooth number.

Explicit examples have been given by A. Joux and K. Nguyen.