From Bilinear to Multilinear Pairing-based Cryptography

Ming-Deh Huang
University of Southern California
and
Wayne Raskind
Arizona State University

Diffie-Hellman protocol: given a finite abelian group, A, written additively, and an element $x \in A$, then it is often difficult to compute abx from knowledge of ax and bx without knowing the integers a and b. This is the basis of many public-key cryptographic systems used today. For various applications, it is useful to have multi-person generalizations of this protocol. Assume that A is cyclic of prime order, ℓ, that x is a generator, and that we have an efficiently computable bilinear pairing:

$$(,) : A \times A \to \mathbb{Z}/\ell\mathbb{Z}.$$

Then three people, say Andrea, Bill and Carlos, can exchange information by each choosing a random integer a, b and c, respectively, broadcasting, respectively, ax, bx and cx, and computing, respectively,

$$a(bx, cx), b(ax, cx), c(ax, bx),$$

all of which are equal to $abc(x, x)$. Several people have used the Weil and Tate pairings on elliptic curves as examples of such bilinear pairings.

In this talk, we are aiming at an n-linear generalization, which would, among other things, give us an $(n+1)$-person Diffie-Hellman protocol. It also has applications to identity based encryption and broadcast encryption.

Let E be an elliptic curve over a finite field $\mathbb{F}$ with chosen algebraic closure $\overline{\mathbb{F}}$. We fix a prime number ℓ different from the characteristic of $\mathbb{F}$ and denote by $E[\ell]$ the set of points P of E defined over $\overline{\mathbb{F}}$ such that $\ell P = 0$. Then we have the Weil pairing:

$$E[\ell] \times E[\ell] \to \mu_\ell,$$

which is bilinear, alternating and nondegenerate.

Recall how this may be defined explicitly. Given $P_i \in E[\ell]$ (i=1,2), represent them by divisors D_i and functions f_i whose divisors have disjoint supports such that $\ell D_i = \mathrm{div}(f_i)$, Weil reciprocity says that we have:

$$f_1^{\mathrm{div}(f_2)} = f_2^{\mathrm{div}(f_1)},$$

and hence

$$\frac{f_1^{D_2}}{f_2^{D_1}}$$

is an ℓ-th root of unity.

Let $\overline{\mathbb{F}}$ be an algebraic closure of $\mathbb{F}$ and put $G = Gal(\overline{\mathbb{F}}/\mathbb{F})$. Assume that $\mathbb{F}$ contains the ℓ-th roots of unity μ_ℓ.

Then we also have the Tate pairing:

$$E[\ell]^G \times E[\ell]_G \to \mu_\ell,$$

where, for a G-module M, M_G denotes the *coinvariants* of M, which is the largest quotient module upon which G acts trivially.

These groups are isomorphic to each other via the map:

$$E[\ell]^G \cong E(\mathbb{F})[\ell] \to E(\mathbb{F}) \to E(\mathbb{F})/\ell E(\mathbb{F}) \cong E[\ell]_G.$$

The last isomorphism comes from taking G-cohomology of the exact sequence:

$$0 \to E[\ell] \to E(\overline{\mathbb{F}}) \xrightarrow{\ell} E(\overline{\mathbb{F}}) \to 0.$$

and using Lang's theorem, which says that $H^1(G, E(\overline{\mathbb{F}})) = 0$. Suppose $E(\mathbb{F})[\ell]$ is cyclic of order ℓ. Then $E[\ell]^G$ and $E[\ell]_G$ are both one-dimensional. Using these identifications, the Tate pairing can be viewed as a symmetric pairing on $E(\mathbb{F})[\ell]$ and is very efficient to compute. Let φ be the geometric Frobenius and let $N = \varphi - 1$. Note that $E[\ell]^G = \ker N$ and $E[\ell]_G = \mathrm{coker} N$. Then $N^2 = 0$ and N induces an isomorphism:

$$E[\ell]_G \cong \mathrm{coker}\, N \cong \ker N \cong E[\ell]^G,$$

which is the inverse of the isomorphism mentioned above. It is sometimes called a *distortion map*. This interpretation will help us in a multidimensional generalization of this pairing. Note the analogy with the monodromy theory of semi-stable elliptic curves over a p-adic field with multiplicative reduction. In that theory, N is the monodromy operator.

Let A be a principally polarized abelian variety of dimension g over a finite field $\mathbb{F}$. We fix a prime number ℓ and denote by $V = A[\ell]$ the set of points P of A defined over $\overline{\mathbb{F}}$ such that $\ell P = 0$. The principal polarization allows us to identify $Pic^0(A)[\ell]$ with $A[\ell]$. Actually, we could simply work with an abelian variety that is if the form $Pic^0(X)$ for some smooth projective variety X over $\mathbb{F}$. There is a well-known $2g$-multilinear, alternating, nondegenerate form:

$$A[\ell] \times \cdots \times A[\ell] \to \mu_\ell^{\otimes g}$$

that may be defined using the étale cohomology of abelian varieties. More precisely, we have:

$$\bigwedge^{2g} H^1(A_{\overline{\mathbb{F}}}, \mu_\ell) \cong H^{2g}(A_{\overline{\mathbb{F}}}, \mu_\ell^{\otimes 2g}) \cong \mu_\ell^{\otimes g}.$$

Here $\mu_\ell^{\otimes g}$ is μ_ℓ twisted g-times. That is G acts on the tensor product diagonally.

This is a well-known generalization of the Weil pairing on elliptic curves. We now make the assumption that $N = \varphi - 1$ acts on $A[\ell]$ in a maximally nilpotent way. That is, $N^{2g} = 0$, but $N^{2g-1} \neq 0$. Then we can produce the same situation as we did for elliptic curves.

Set $d = 2g - 1$ so that $N^{d+1} = 0$.

There is a unique filtration $V.$

$$V = V_d \supset V_{d-2} \supset ... \supset V_{-d}$$

such that $N(V_i) \subseteq V_{i-2}$ and, letting $Gr_iV = V_i/V_{i-2}$, then N^i induces an isomorphism:

$$Gr_iV \to Gr_{-i}V.$$

In fact,

$$Gr_iV \cong (Gr_{-i}V)^*$$

where * denotes the dual vector space. This analysis generalizes the well-known duality:

$$Gr_{-d}V = V^G \cong (V_G)^* = Gr_dV.$$

(1) For all $i \in I$, $Gr_i V$ is of $\mathbb{F}_\ell$-dimension one and G acts trivially on this space.

(2) A non-trivial $2g$-linear alternating pairing on V taking values in μ_ℓ induces a non-trivial multilinear pairing:

$$Gr_d V \times Gr_{d-2} V \times ... \times Gr_{-d} V \to \mu_\ell^{\otimes g}.$$

(3) Moreover if $<,>$: $V \times V \to \mu_\ell$ is a non-degenerate bilinear pairing, then the bilinear pairing induces a perfect pairing between Gr_i and Gr_{-i}, and the $(2g)$-linear pairing $Gr_d V \times ... \times Gr_{-d} V \to \mu_\ell^{\otimes g}$ sending $v_i \in V_i$ to $\zeta^{\prod b_i}$, where $\zeta^{b_i} =< v_i, v_{-i} >$, is identical, up to a constant factor, to the multilinear pairing in (2).

We have put $\mu_\ell^{\otimes g}$ to emphasize the twist, g. In fact, by a famous theorem of Quillen, we have a canonical isomorphism:

$$K_{2g-1}(\overline{\mathbb{F}})[\ell] \cong \mu_\ell^{\otimes g}.$$

A better way to do this would be to define a multilinear map:

$$A[\ell] \times \cdots \times A[\ell] \to K_{2g-1}(\overline{\mathbb{F}})$$

in an explicit way as for the Weil pairing above on elliptic curves. We are working on this now, but it does not appear to be easy, even for $g = 2$.

Does there exist an abelian variety with the desired properties? Let $\alpha_1, \cdots \alpha_{2g}$ be the eigenvalues of φ,arranged in such a way that $\alpha_{2j} = \overline{\alpha_{2j-1}}$ for $j = 1, \cdots, g$ and all of these ℓ-adic units are congruent to 1 mod ℓ. By a theorem of Honda and Tate, there is an isogeny class of abelian varieties with such numbers as eigenvalues of φ. We need to find one with $A(\mathbb{F})[\ell]$ of order ℓ. From a probabilistic point of view, this appears unlikely, even for $g = 1$, and yet we know that it is possible in that case. It would be nice if we could find a Jacobian of a curve, but we doubt that this is possible.

This problem can be approached by using Bloch's higher Chow groups. We briefly recall their definition. Consider the n-simplex Δ^n, which we view as being embedded into an $(n+1)$-dimensional affine space with coordinates $x_0, \cdots, x_n$ via the equation:

$$\sum_{i=0}^{n} x_i = 1.$$

There are faces Δ^r of this simplex given by setting some coordinates equal to 0. Given an algebraic variety X, Bloch takes the group $\mathcal{Z}^m(X, n)$ of cycles of codimension m on the product $X \times \Delta^n$ that meet each $X \times \Delta^r$ properly (that is, the intersection is of the expected codimension).

One gets a complex by taking boundary maps given by the alternating sum of the intersections of a cycle with the $X \times \Delta^{n-1}$, for each of the embeddings of Δ^{n-1} into Δ^n. He then defines $CH^m(X, n)$ as the homology of this complex. With appropriate indexing, these groups are isomorphic to Voevodsky's motivic cohomology groups:

$$CH^m(X, n) \cong H^{2m-n}(X, \mathbb{Z}(m)).$$

For $n = 0$, we get the usual Chow groups of codimension m-cycles modulo rational equivalence.

Each of these definitions has its advantages and disadvantages. Voevodsky's groups have excellent functorial properties, since they are defined as derived functors, but they are not so easy to compute directly. Bloch's groups have the nice presentations described above, but there are technical difficulties with proving moving lemmas to establish the key exact sequences.

Also, if K is a field, then $CH^2(K,3) \cong H^1(K,\mathbb{Z}(2)) \cong K_3(K)^{ind}$, where ind denotes indecomposable K_3, which is the quotient of the Quillen K-theory group by the Milnor K-theory group. If K is a finite field or an algebraic closure thereof, the Milnor K_3 is trivial.

Thus K_3 of a finite field $\mathbb{F}$ may be described in this way as the homology of the complex:

$$\mathcal{Z}^2(\mathbb{F} \times \Delta^4) \to \mathcal{Z}^2(\mathbb{F} \times \Delta^3) \to \mathcal{Z}^2(\mathbb{F} \times \Delta^2).$$

One can also do motivic cohomology with $\mathbb{Z}/\ell\mathbb{Z}$-coefficients by taking the cycle groups in Bloch's higher Chow groups with $\mathbb{Z}/\ell\mathbb{Z}$-coefficients. We then have that $H^1(X, \mathbb{Z}/\ell\mathbb{Z}(1)) \cong Pic(X)[\ell]$ for X smooth and proper over a separably closed field of characteristic prime to ℓ.

If X is smooth and proper of dimension g, we have a trace map:

$$H^{2g}(X, \mathbb{Z}/\ell\mathbb{Z}(2g)) \to H^0(\overline{\mathbb{F}}, \mathbb{Z}/\ell\mathbb{Z}(g)).$$

We then consider the cup-product pairing followed by the trace:

$$\bigwedge_{i=1}^{2g} H^1(X, \mathbb{Z}/\ell\mathbb{Z}(1)) \to H^{2g}(X, \mathbb{Z}/\ell\mathbb{Z}(2g)) \to H^0(\overline{\mathbb{F}}, \mathbb{Z}/\ell\mathbb{Z}$$

Cup-product in motivic cohomology can be described in "functorial" terms and the group on the right is canonically isomorphic to $\mu_\ell^{\otimes g}$, but the description in terms of Bloch's higher Chow groups should allow us to describe the pairing more explicitly.

For $g = 1$, we can recover the explicit description of the Weil pairing, but even this is not so obvious. However, this appears to be the best known framework for generalization of the explicit description of the Weil pairing.