Hard Homogeneous Spaces

Jean-Marc Couveignes

Fields Institute, Toronto, November 2006

I first have to say that I will not present anything new in this talk. I will just discuss a few questions that I raised a few years ago[1] about the possibility of generalizing the discrete logarithm (DL) problem to some more general problem that I then called a Hard Homogeneous Space (HHS). My main concern will be to show some instances of this more general problem that are not derived from any DL situation.

When I first thought about this question in 1997 I found essentially one large family of HHS that are not DL problems. Since then, I have been discussing this problem with a few colleagues (in particular David Kohel and Antoine Joux) but we found nothing new in the last nine years.

Recently, I have been advised by Antoine Joux that there may be some new interest for these matters and I decided to post my old 1997 preprint[2] to the ecrypt archive under number 2006/291.

This note was not updated after it was rejected at crypto 97 so there may be a few remarks in it that no longer make much sense.

In this talk I will first explain what a HHS is. Then I will give a non trivial example of HHS. I will finish with a few remarks and questions.

What is a HHS ?

The starting observation is that when looking at a discrete logarithm problem (that is, given some group G and two elements g and h in G, we are looking for a integer n such that $g^n = h$) we may to some extent forget that G is a group.

Indeed, instead of looking a g^n as the iterated product of g with itself we may see it as g acted on by the exponent n. This makes sense because n may be regarded as an element in the group $(\mathbb{Z}/\gamma\mathbb{Z})^*$ where γ is the order of g.

We thus set $A = (\mathbb{Z}/\gamma\mathbb{Z})^*$ and assume $G =< g >$ and $\#G = \gamma$. We know that A acts on G. Indeed A is the full automorphism group of G. But we prefer

[1] I gave a talk at the séminaire de complexité et cryptographie at the École Normale Supérieure (http://www.di.ens.fr/ wwwgrecc/Seminaire/1996-97.html).

[2] It was rejected at Crypto 97 and I have left it in its initial state, although I am not quite happy with it. If need be, I will publish an updated version later.

to introduce the set H of generators of G. It has cardinality γ and is acted on by A. For $a \in A$ and $h \in H$ we denote by $a \star h = h^a$ the result of this action.

The action of A on H is *transitive* : for every h_1 and h_2 in H there is an exponent a in A such that $h_2 = h_1^a = a \star h_1$. In fact this exponent is unique. This is expressed by saying that the action of A on H is *free*. One also says that H is a *homogeneous space* for A.

This is a very standard situation in the mathematical world. For any field k and integer $d \geq 1$, the vector space $A = k^d$ is a group for the addition law. Let's call H the corresponding affine space $\mathbb{A}^d(k)$.

Let P be a point in the affine space H and $\overrightarrow{u}$ a vector in A. We define $\overrightarrow{u} \star P$ to be the unique point Q in H such that $\overrightarrow{PQ} = \overrightarrow{u}$.

So homogeneous spaces are many. However there is a big difference between the discrete logarithm example and the affine space example : it concerns complexity issues. While it seems to be difficult to compute a discrete logarithm, the corresponding problem for affine spaces is very easily solved since the coordinates of the vector $\overrightarrow{PQ}$ are just $x_Q - x_P$ and $y_Q - y_P$.

In general, given two points P and Q in a homogeneous space H, the problem of finding the vector $\overrightarrow{u} \in G$ such that $\overrightarrow{u} \star P = Q$ is called the *vectorization* problem.

We are going to be interested in homogeneous spaces where the vectorization problem is difficult.

In fact, for possible cryptographic relevance, we must introduce a slightly easier problem :

Given three points P, Q, R in H, find a fourth point S that turns $PQSR$ into a parallelogram. This means that $\overrightarrow{PQ} + \overrightarrow{PR} = \overrightarrow{PS}$.

We call this problem the *parallelization* problem.

We will be interested in Homogeneous Spaces (A, H) for which the group law in A is easy to compute, the group action of A on H is easy to compute, there is an efficient way of constructing random elements in A, and the parallelization problem is difficult.

We call such homogeneous spaces *Hard Homogeneous Spaces* (HHS).

Many cryptosystems that are based on the DL problem can be rephrased in the context of HHS.

Our main concern for the rest of this talk will be to find out HHS that do not come from any DL problem (otherwise our definition would be void).

An HHS which is not a DL problem

There is a natural candidate HHS that comes from class field theory. Let q be a prime power and E an ordinary elliptic curve over $\mathbb{F}_q$. Let $\mathcal{O}$ be the endomorphism ring of E and let Φ be the Frobenius endomorphism. Let t be the trace of Φ.

The number of points in $E(\mathbb{F}_q)$ is $q + 1 - t$. The ring $\mathbb{Z}[\Phi]$ has discriminant

$t^2 - 4q$ and the ring $\mathcal{O}$ has discriminant $\Delta_{\mathcal{O}}$. The index θ of $\mathbb{Z}[\Phi]$ in $\mathcal{O}$ satisfies

$$\theta^2 \Delta_{\mathcal{O}} = t^2 - 4q.$$

Let A be the ideal class group of $\mathcal{O}$ and let H be the set of (isomorphism classes of) elliptic curves over $\mathbb{F}_q$ having endomorphism ring isomorphic to $\mathcal{O}$ and having the same number of points as E.

The cardinality of H is the order of A and there is a free action of A on H. A good reference for this is David Kohel's thesis[3].

I will now sketch the definition of this action of A. But I first want to stress that H is definitely not a group. Given two elliptic curves, there is no canonical way to construct a third one out of the two.

Now assume we are given a class c in the ideal class group A of $\mathcal{O}$. Let $\mathfrak{c}$ be an ideal in that class and assume the quotient group $\mathcal{O}/\mathfrak{c}$ is cyclic of order prime to $t^2 - 4q$ and the characteristic p.

Let $n = \#(\mathcal{O}/\mathfrak{c})$ be the norm of $\mathfrak{c}$ and let C be an element in $\mathfrak{c}$ such that $\mathfrak{c}$ is generated by n and C.

Let K be the intersection of the kernels of all endomorphisms in $\mathfrak{c}$. This is just the subgroup of $E[n]$ annihilated by C. It is a cyclic subgroup of order n.

Quotienting by K defines an isogeny $E \to E/K$. We set $F = E/K = c \star E$. This defines an action of $A = \mathcal{CL}(\mathcal{O})$ on H which is transitive and free.

From the definition it is clear that $c \star E$ can be computed in time polynomial in $\log q$ and the norm n of $\mathfrak{c}$.

This is an important point : not every class c in $\mathcal{CL}(\mathcal{O})$ can be represented by an ideal with small norm. But very likely, the group $\mathcal{CL}(\mathcal{O})$ is generated by classes of small prime ideals. And this suffices to construct random elements in $\mathcal{CL}(\mathcal{O})$ as combinations of those small generators.

If you like dynamical systems you may see H as a set of *states* and A as a set of *commands*. We are given a generating set $\mathcal{A} = \{a_1, a_2, \ldots, a_k\}$ for A. The action of these *elementary* commands on H can be computed easily. Since a random combination of the a_i's produces a random element in H we can apply a random command to any state.

It is important to notice that contrary to discrete logarithm problems, HHS do not allow fast exponentiation in general. This is just because fast exponentiation assumes H has a composition law. The existence of a generating set like $\mathcal{A}$ for A is a sufficient substitute to it however, because it allows to reach a random state quickly, which suffices to produce assymetry.

Questions and comments

Is the HHS presented above resistant to a quantum computer

[3] http://echidna.maths.usyd.edu.au/∼kohel/

How fast is it to compute isogenies ? It is polynomial time. It was hardly practical ten years ago. There now exist efficient implementations.

Shanks algorithm applies to any HS : to find the vector from P to Q one may apply small vectors to P iteratively until one reaches $\gg \sqrt{\#H}$ points and similarly to Q. Because of the birthday paradox, there is a reasonable probability that the two sets thus obtained have a non zero intersection. This gives the path from P to Q. This was observed by Galbraith in 1999.

Jao, Miller and Venkatesan (ASIACRYPT 2005) observed that under GRH one can actually prove that classes with small ideals in them do generate the full class group of a quadratic field.

In Jao and al. work, a more general problem is considered that mixes the HHS we described and the elliptic curve discrete logarithm. It can be shown (see my 97 preprint section 5.7) that DL in finite fields, DL on elliptic curves, our HHS and the one studied by Jao and al. are all instances of a general problem coming from class field theory.

Antoine Joux and J.-J. Quisquater asked me if one can extend the definitions of HHS to obtain something similar to pairings in this context. Indeed we may consider three homogeneous spaces H_1, H_2 and H_3 under the same group A together with a covariant map $\pi : H_1 \times H_2 \to H_3$. From a mathematical point of view such situations do exist : take A and H as above and $H_1 = H_2 = H$ and π the map that associates to the elliptic curves E_1 and E_2 their product $S = E_1 \times E_2$ which is an abelian variety. However, there is no known efficient algorithm to decide if to such varieties $E_1 \times E_2$ and $E_3 \times E_4$ are isomorphic. So H_3 in that case does not seem to be computational. So this example is bad. I know of no interesting example of such a triple of homogeneous spaces.