Hard Homogeneous Spaces

Jean-Marc Couveignes

August 24, 2006

Abstract

This note was written in 1997 after a talk I gave at the séminaire de complexité et cryptographie at the École Normale Supérieure After it was rejected at crypto97 I forgot it until a few colleagues of mine informed me that it could be of some interest to some researchers in the field of algorithmic and cryptography. Although I am not quite happy with the redaction of this note, I believe it is more fair not to improve nor correct it yet. So I leave it in its original state, including misprints. I just added this introductory paragraph. If need be, I will publish an updated version later.

We introduce the notion of hard homogeneous space (HHS) and briefly develop the corresponding theory. We show that cryptographic protocols based on the discrete logarithm problem have a counterpart for any hard homogeneous space. Indeed, the notion of hard homogeneous space is a more general and more natural context for these protocols. We exhibit conjectural hard homogeneous spaces independant from any discrete logarithm problem. They are based on complex multiplication theory. This shows the existence of schemes for authentication and key exchange that do not rely on the difficulty of computing dicrete logarithm in any finite group nor factoring integers. We show that the concept of HHS fits with class field theory to provide a unified theory for the already used discrete logarithm problems (on multiplicative groups of finite fields or rational points on elliptic curves) and the HHS we present here. We discuss a few algorithmic questions related to hard homogeneous spaces.

The paper is looking for a wider point of view on the discrete logarithm problem both mathematically and cryptographically.

Key Words: Discrete Logarithm, Authentication, Key Exchange, Elliptic Curves, Lattices
http://www.di.ens.fr/ wwwgrecc/Seminaire/1996-97.html

1 Introduction

In this paper we describe a special kind of assymetric function that we call hard homogeneous space (HHS). We show that this is a very natural object to study from the point of view of cryptography. Indeed, any such hard homogeneous space leads in a quite natural and elegant manner to cryptographic schemes for authentication and key-exchange.

A special case of HHS is provided by discrete logarithm over some commutative group such as $\mathbb{Z}/n\mathbb{Z}$ (for n an integer) or an elliptic curve over a finite field. But there exist many more HHS than these already known ones.

In the second part of the paper we give conjectural examples of new hard homogeneous spaces. They come from the theory of complex multiplication of elliptic curves. These examples lead to cryptographic schemes that rely on new algorithmic problems. We describe a general mathematical context for both these new HHS and the already known discrete logarithm problems in finite fields and elliptic curves.

We did not study any other example of hard homogeneous spaces than the one we present here but we do believe it is an interesting problem to look for some different and more practical ones since the concept of HHS is more general and more natural than the one of hard discrete logarithm. In particular it may be interesting to look for HHS based on more combinatorial problems than the ones we discuss there.

In the next section we define hard homogeneous spaces (HHS) and give several examples. In the third one we show how to make key-exchange schemes through HHS. In section four we construct authentication schemes with a HHS and make a connection with graph isomorphism problems as in [4]. In section five we show how complex multiplication theory leads to many HHS, some of them beeing just discrete logarithm problems are some others beeing different. Finally we list a few problems and questions about HHS.

This work benefited from comments by Jacques Stern and the audience of his weekly seminar on Complexity and Cryptography. We thank David Pointcheval for interesting discussions and comments on section 4.

2 Definition of Hard Homogeneous Spaces

Let G be a finite commutative group. A homogeneous space H for G is a finite set H of the same cardinality $S = \#H = \#G$ which is acted on simply transitively by G. This means that there is a single orbite and for any $g \in G$ not the identity, the permutation of H induced by g has no fixed points. In other words there is a unique g in G that maps a given h_1 to a given h_2. The left action is denoted by a dot. We thus have

$$(\exists h \in H, g.h = h) \Longrightarrow g = 1.$$

Any group admits a homogeneous space. Namely itself together with the action by left multiplication. But this is not a very interesting example.

A more intrinsic example would be for H an affine space and for G the underlying vector space.

Given a homogeneous space, there are several algorithmic problems one would like to consider.

We assume that elements in G and H are represented by strings in a non necessarily unique way.

We first have to compute the composition law, inversion of an element and testing for equality.

Problem 1 (Group Operations) *Given strings g_1 and g_2 decide if they represent elements in G and if these elements are equal or not. Given $g_1, g_2 \in G$ compute g_1^{-1}, $g_1 g_2$ and decide if $g_1 = g_2$.*

We also need to choose random elements in G.

Problem 2 (Random Element) *Find a random element in G with uniform probability.*

Remark: If we know some element in H, then applying a random element of G to it we obtain a random element of H.

We may like to decide membership and equality for elements in H.

Problem 3 (Membership) *Given a string h_0 decide if h_0 represents an element in H*

Problem 4 (Equality) *Given $h_1, h_2 \in H$ decide if $h_1 = h_2$.*

We also want to compute the action of G on H.

Problem 5 (Action) *Given $g \in G$ and $h \in H$ compute $g.h$.*

All these problems are sort of basic requirements for an Homogeneous Space to be algorithmic.

We now come to more subtle ones. Remember that because of the lack of fixed points, there is a unique g mapping h_1 on h_2. This is the unique vector mapping h_1 to h_2. We denote it by $\delta(h_2, h_1)$. We thus have

$$\delta(h_2, h_1).h_1 = h_2.$$

We may like to compute this $\delta(h_2, h_1)$.

Problem 6 (Vectorization) *Given $h_1, h_2 \in H$ find $g \in G$ such that $g.h_1 = h_2$.*

A related problem would be to complete a parallelogram namely

Problem 7 (Parallelization) *Given $h_1, h_2, h_3 \in H$ compute the unique h_4 such that $\delta(h2, h1) = \delta(h4, h3)$.*

Remark: This h_4 is just $\delta(h_2, h_1).h_3$.

We will be interested in Homogeneous Spaces for which problems 1 to 5 are easy while problems 6 and 7 are difficult. We call these Hard Homogeneous Spaces.

We observe that under the above conditions problem 7 is easier than problem 6.

We notice also that problem 6 can be solved in time S by exhaustive search and even in time and space $S^{1/2}$ if we use baby-step-giant-step algorithm. This is possible if elements in H admit a sufficiently unique representation together with some order on it and if we know enough about the group G. For example if G is cyclic of known order and generator.

Example: We show how discrete logarithm is a special case of homogeneous space.

Let C be a cyclic group of order n and generator c and let G be its automorphism group. An element g of G maps c to $g(c) = c^a$ where a is an integer prime to n. The map

$$g \mapsto a \bmod n$$

defines an isomorphism between G and $(\mathbb{Z}/n\mathbb{Z})^*$.

We take E to be the set of generators of C. Then $\#E = \phi(n)$ and G acts simply transitively on E.

Remark: we may consider an eighth problem namely

Problem 8 (ParallelTesting) *Given four elements h_1, h_2, h_3, h_4 in H decide whether $\delta(h_2, h_1) = \delta(h_4, h_3)$.*

If the later problem is difficult we say our homogeneous space is very hard (VHHS).

Discrete logarithm apparently leads to VHHS.

3 Key exchange

We describe a key exchange scheme based on a HHS. It is the evident generalization of the Diffie-Hellman scheme to HHS.

If Alice and Bob are to exchange a key, they proceed in several steps

1. Alice chooses a random element h_0 in H and a random element g_1 in G. She computes $h_1 = g_1.h_0$ and sends (h_0, h_1) to Bob.

2. Bob chooses a random element g_2 in G and computes $h_2 = g_2.h_0$. He sends h_2 to Alice. The secret key is $K = g_2.h_1$.

3. Alice computes the secret key $K = g_2.h_1 = g_1.h_2$.

In order to break the system one has to solve the Parallelization problem for the considered HHS.

We stress the importance of the commutativity of G in the above protocol.

4 Authentication

Protocols in this section are adaptation to the HHS context of ideas in [3] and [4].

We describe an authentication protocol that is not zero-knowledge. An extensive study of interactive proofs can be found in the work of Pointcheval [11].

The public knowledge will include the description of the HHS plus some element h_0 in H. The set of participants is called I. Each participant $i \in I$ picks a random element g_i in G and computes $g_i.h_0 = h_i$. The secret of i is g_i and i publishes h_i. The participant i is then defined as the one who knows $g_i = \delta(h_i, h_0)$.

We assume Alice is user number 2 and Bob is user number 1. Now if Alice is to identify Bob the scheme goes as follows.

1. Alice finds h_1 in the phonebook at the entry "Bob". She picks a random element g_t in G and computes $h_t = g_t.h_0$. She sends h_t to Bob.

2. Bob knows g_1 such that $h_1 = g_1 h_0$. He computes $h_p = g_1.h_t$ and sends it to Alice.

3. Alice checks that $h_p = g_t.h_1$.

The information obtained by some observer is a random parallelogram with size $[h_0, h_1]$ that is a random h_t and a h_p such that $\delta(h_p, h_t) = \delta(h_1, h_0)$. But this is no knowledge since anyone can build such a parallelogram by choosing a random g_t.

In order to break the system one has to solve the parallelization problem.

Now if we want to get a zero-knowledge protocol we adapt ideas about graph isomorphism to our situation. We will also discuss the similarity and differences between graph (non) isomorphism problems and HHS.

The public and private knowledge are the same as before. Alice is user number 2 and Bob is user number one. Bob proves himself.

1. Bob picks a random $g_r \in G$ and computes $g_r.h_1 = h_r$. He sends h_r to Alice.

2. Alice flips a coin and sends the result $\epsilon \in \{0, 1\}$ to Bob.

3. If $\epsilon = 0$ then Bob sends $g_p = g_r$ to Alice. Otherwise he sends $g_p = g_r g_1$.

4. Alice checks that $g_p.h_1$ is h_r (if $\epsilon = 0$) or $g_p.h_0 = h_r$ (if $\epsilon = 1$).

An unfair prover will escape with probability one half.

Iterating the process we get a proof that Bob knows g_1. Therefore breaking the system amounts to solving the vectorization problem.

If we now come back to the Goldreich, Micali, Wigderson paper we realize that in the case of graph isomorphism the group involved is not commutative and the verifier is not supposed to have an oracle for graph isomorphism.

Indeed the above protocol will work for a HHS with non commutative group and even if membership is not easy to decide. Both these later hypothesis are necessary though to key exchange. So is randomly choosing a transformation in all cases.

Perhaps the main difference between graph theory and our HHS is that in the context of graphs it is difficult to decide isomorphism (and even more difficult to find some isomorphism) while in our case the existence of a transformation between h_1 and h_2 can be tested easily (problem 3).

Nevertheless, if we have a *very* hard homogeneous space (VHHS) we can reproduce a very similar situation to the one in [4] by considering *pairs* of elements in H and say that two such pairs (h_1, h_2) and (k_1, k_2) are isomorphic if there is a $g \in G$ such that $g.(h_1, h_2) = (g.h_1, g.h_2) = (k_1, k_2)$. Then testing isomorphism of two pairs is hard but there is a zero knowledge protocol to convince a verifier that two pairs are actually isomorphic without saying anything about the g.

*****

5 A HHS that does not rely on any discrete logarithm problem

In this section we discribe candidate HHS that are different from any discrete logarithm problem. The first paragraph recalls basic facts about elliptic curves. The three following paragraphs are devoted to the description of the HHS we propose. In paragraph 5 we study a nice elementary problem of additive number theory connected to HHS. The sixth paragraph is concerned with efficiency considerations. The last paragraph enlarges the point of view of this paper to complex multiplication theory.

5.1 Ordinary elliptic curves over a finite field

We recall here a few basic facts concerning elliptic curves over finite fields. We will restrict to the most trivial cases of the theory. See [14, 8, 12] for a complete account on these questions.

We consider a finite field $\mathbb{F}_q$ of cardinality $q = p^d$ and an elliptic curve E_0 over $\mathbb{F}_q$. We assume that E_0 is ordinary or equivalently not supersingular. This means that the endomorphism ring of E_0 is an order $\mathcal{O}$ in some quadratic field. We call t the trace of the Frobenius map. It is related to the cardinality of the curve by

$$\#E = q + 1 - t.$$

We call $\Delta = t^2 - 4q$ the discrimimant of the curve E_0. We assume that Δ is squarefree. This implies that $\mathcal{O} = \mathrm{End}(E_0) = \mathbb{Z}[\Phi]$ and $\mathcal{O}$ is the maximal order $\mathcal{O}_{\mathbb{K}}$ in $\mathbb{K} = \mathbb{Q}(\sqrt{\Delta}) = \mathrm{End}(E_0) \otimes_{\mathbb{Z}} \mathbb{Q}$.

For any ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{K}}$ one defines an elliptic curve $\mathfrak{a}.E_0$ and an isogeny

$$I_{\mathfrak{a}} : E_0 \to \mathfrak{a}.E_0$$

of degree $\mathcal{N}(\mathfrak{a})$ the norm of $\mathfrak{a}$. All these can be computed in polynomial time in $\mathcal{N}(\mathfrak{a})$.

If $\mathfrak{a}$ and $\mathfrak{b}$ are ideals in $\mathcal{O}_{\mathbb{K}}$ then the two elliptic curves $\mathfrak{a}.E_0$ and $\mathfrak{b}.E_0$ are equal if and only if $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent i.e. there exists $\alpha \in \mathbb{K}^*$ such that $\mathfrak{b} = (\alpha)\mathfrak{a}$. We denote by $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$ the class group of $\mathcal{O}_{\mathbb{K}}$ and by $[\mathfrak{a}]$ the class of the ideal $\mathfrak{a}$.

There is a simply transitive action of $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$ on the set $\mathcal{I}(E_0)$ of isogeneous curves to E_0.

One can test easily if a curve E is in $\mathcal{I}(E_0)$. It is enough to check that $\#E = \#E_0$ which is easy if we are given a factorisation of $\#E_0$.

The group $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$ is a commutative group. Its size S is given assymptotically by

$$\log(S) \sim \log(\Delta)/2.$$

If ℓ is a prime integer such that Δ is a non zero square modulo ℓ then the polynomial

$$f(X) = X^2 - tX + q$$

has two roots λ and μ and the prime ℓ decomposes in $\mathcal{O}_{\mathbb{K}}$ as

$$\ell = \mathfrak{l}\mathfrak{m} \text{ with } \mathfrak{l} = (\ell, \Phi - \lambda) \text{ and } \mathfrak{m} = (\ell, \Phi - \mu).$$

We shall consider small primes ℓ_i such that Δ is a non zero square modulo ℓ_i and the corresponding ideals $\mathfrak{l}_i$ and $\mathfrak{m}_i$. We notice that

$$[\mathfrak{l}_i][\mathfrak{m}_i] = [\ell_i] = 1$$

in the class group.

On average, one prime over two satisfies the property we require. Such primes are called Elkies primes. It may be that few small primes are Elkies. In this case we pick another curve E_0.

We will consider all Elkies primes $(\ell_i)_{1\leq i\leq I}$ smaller than a constant times $\log S$. Heuristically the corresponding $\mathfrak{l}_i$ will generate $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$ ([2] page 249). We are interested in the module of relations among them. Indeed we want to know the kernel $\mathcal{R}$ of the map

$$G : \quad \mathbb{Z}^I \longrightarrow \mathcal{CL}(\mathcal{O}_{\mathbb{K}})$$

$$(x_1, ..., x_I) \longmapsto \prod_i [\mathfrak{l}_i]^{x_i}$$

These data can be computed once for all in subexponential time using Hafner-McCurley-Buchmann algorithm [5, 1]. This gives us in particular the structure and cardinality $S = h_{\mathbb{K}}$ of $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$.

Suppose to be simpler that $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$ is cyclic (this will always be the case if $S = h_{\mathbb{K}}$ is squarefree) and $[\mathfrak{l}_1]$ is a generator. In particular we know residues γ_i mod S such that $[\mathfrak{l}_i] = [\mathfrak{l}_1]^{\gamma_i}$. Then any element $[\mathfrak{l}_1]^k$ with $k \in \mathbb{Z}/S\mathbb{Z}$ can be writen as a product

$$[\mathfrak{l}_1]^k = \prod_i [\mathfrak{l}_i]^{a_i}$$

with small a_i's. The a_i are small solutions to the congruence

$$\sum_i a_i \gamma_i \equiv k \pmod{S}$$

and they correspond to short vectors in the lattice $\mathcal{R}$.

We can see now how to proceed. One can pick a random element in $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$ choosing a random exponent k then express it as a product of small primes with small exponents and apply it to some elliptic curve in $\mathcal{I}(E_0)$.

On the other hand, given two elliptic curves, it is a difficult matter to find an isogeny between them.

From a mathematical point of view there are two possible ways to prove the existence of such an isogeny.

The first one is to lift the elliptic curves as elliptic curves over $\bar{\mathbb{Q}}$ with complex multiplication. Then these curves will be defined over some degree $h_{\mathbb{K}}$ extension of $\mathbb{Q}$ which is impossible to deal with using a computer.

The other approach is Tate's proof for the existence of isogenies between abelian varieties. But it uses a pigeon hole principle on $\mathcal{I}(E_0)$ which clearly gives rise to an exponential algorithm.

In the following paragraphs we will describe in more detail the computational aspects of the homogeneous spaces introduced in the previous section. We first explain how such an homogeneous space can be given. We then explain how problems 1 to 5 can be dealt with. Then we explain how to construct the initial data for our HHS.

5.2 Presentation

We here explain how our HHS will be given. It will consist of certain data available to all users and that any one can check in polynomial time.

First of all, one is given a finite field $\mathbb{F}_q$ with $q = p^d$ of size 10^{80} typically. We also have an ordinary elliptic curve E_0 given in Weierstrass form with invariant $j \in \mathbb{F}_q$. We also know $c = \#E_0$ the cardinality of E_0 i.e. the number of $\mathbb{F}_q$-rational points on E_0. We also are provided with the prime decomposition of c together with a proof of it. Further c is squarefree. We set $t = q + 1 - c$ and we have a list of small primes $(\ell_i)_{1 \leq i \leq I}$ and residues λ_i modulo ℓ_i that are simple roots of $f(X) = X^2 - tX + q$ modulo ℓ_i. We define the ideals $\mathfrak{l}_i = (\ell_i, \Phi - \lambda_i)$ and $\mathfrak{m}_i = (\ell_i, \Phi - \mu_i)$ where $\mu_i = t - \lambda_i$.

We know the class number $h_{\mathbb{K}}$ and its factorisation. Further $h_{\mathbb{K}}$ is squarefree and $[\mathfrak{l}_1]$ is a generator of $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$. We set $S = h_{\mathbb{K}}$ and we are given residues γ_i modulo S such that $[\mathfrak{l}_i] = [\mathfrak{l}_1]^{\gamma_i}$.

We call J the integral part of $\log_2(S)$. We are given small integers $(e_{i,j})_{1 \leq i \leq I; 0 \leq j \leq J}$ such that

$$[\mathfrak{l}_1]^{2^j} = \prod_{1 \leq i \leq I} [\mathfrak{l}_i]^{e_{i,j}}.$$

We call K the maximum of $|e_{i,j}|$.

We will also assume that we know a table of modular equations $\mathcal{E}_{\ell_i}(x, y)$ for $1 \leq i \leq I$. We only need to store these equations modulo p the characteristic.

5.3 Complexity of our homogeneous spaces

In this paragraph we evaluate the complexity of problems 1 to 5 for the homogeneous spaces we consider.

Group Computation: Elements in G will be denoted by an integer $0 \leq k < S$. The integer k denotes the element g^k where $g = [\mathfrak{l}_1]$ is the generator. Group computations then reduce to arithmetic modulo S.

Random Element: We just pick a random integer in $[0, S[$.

Membership: Elements in H are given as elliptic curves in Weierstrass form. Such a representation is not unique. An elliptic curve E is in H if and only if its cardinality is equal to $\#E_0$. Since the latter is given (an even its prime decomposition) we can easily check that a point P on E has order dividing $\#E_0$. If this is not the case then we know E is not isogenous to E_0. If the order of P is exactly $\#E_0$ then the cardinality of E is a multiple $\lambda\#E_0$ of $\#E_0$. But $\#E_0 > q - 2\sqrt{q}$ thus $\lambda\#E_0 > \lambda(q - 2\sqrt{q})$. On the other hand $\#E < q + 2\sqrt{q}$ thus $\lambda < (q + 2\sqrt{q})/(q - 2\sqrt{q})$. This implies $\lambda = 1$ as soon as $q > 36$. Thus if we find a point of order $\#E_0$ on E then $E \in H$. Finally, if P is of order a divisor of $\#E_0$ we pick another P.

This procedure must end quickly since a random element in E is very likely to be a generator. Indeed E is a commutative group, product of at most two cycles. And since the endomorphism ring is maximal we even know that E is cyclic [9]. The proportion of generators in a cyclic group of order n is $\prod_{p|n}(1 - 1/p)$. We thus can easily evaluate this proportion μ for E_0. We will have to perform $1/\mu$ tries on average.

Equality Two Weierstrass elliptic curves are isomorphic over $\mathbb{F}_q$ if an only if they have the same j invariant and are not twisted to each other. We first compute the j invariants. If they are equal, testing for isomorphism reduces to a quadratic residue computation in $\mathbb{F}_q$ [13].

Action: We first explain how to compute the action of a small prime ideal $[\mathfrak{l}_i]$ on an elliptic curve $E \in H$. We have to factor modular equations of level ℓ_i as explained in [10]. This gives us two candidate elliptic curves. One is $[\mathfrak{l}_i].E$ and the other one is $[\mathfrak{m}_i].E$. We sort of by looking at the action of Φ on the corresponding subgroups of the ℓ_i-torsion on E. All this is detailed in [10]. The complexity is $O(\ell_i^3)$ operations in $\mathbb{F}_q$ and $O(\ell_i^{2+\epsilon})$ if we use fast multiplication.

Now if we want to apply an arbitrary element g^k of G to some elliptic curve $E \in H$ we first express g^k as a product of $[\mathfrak{l}_i]$ with small exponents. For example we can write k in base 2 and use the $(e_{i,j})_{i,j}$.

If we find $g^k = \prod_i [\mathfrak{l}_i]^{a_i}$ we have to apply each $\mathfrak{l}_i$ successively a_i times to E. If a_i is negative we apply $\mathfrak{m}_i$ instead of $\mathfrak{l}_i$.

Since the $|a_i|$ are smaller than JK we have at most IJK isogenies to consider. Their degree is bounded by $I^{1+\epsilon}$ so the total complexity is bounded by $I^{4+\epsilon}JK$.

All these computations will be polynomial time in $I = O(\log(S))$ provide K is. In practice we shall be able to find $e_{i,j}$ that are essentially constant so the computation of $\prod_i [\mathfrak{l}_i]^{a_i}.E$ will take time $\log^{5+\epsilon}(S)$ multiplications in the field $\mathbb{F}_q$ if one uses no fast multiplication technique.

5.4 Construction

We now explain how the data for an HHS can be prepared. We first choose a finite field $\mathbb{F}_q$. Since the cardinality of the class group is going to be like $\sqrt{q}$ we may take q of size 10^{80} to avoid any baby-step-giant-step attack. For reasons that will appear later we also prefer a field with small characteristic (2 is perfect).

We then pick an elliptic curve E_0 over $\mathbb{F}_q$ and we compute its cardinality using Schoof's algorithm and the many known improvements. This computation takes around 30 minutes on a DEC alpha 250 using the most recent ideas and implementations. We then set $t = q + 1 - \#E_0$ and try to factor the discriminant Δ. If Δ is not a large prime times a product of distinct small ones then we pick another random curve E_0. After a few tries we get an elliptic curve E_0 such that the Δ is squarefree. We then pick an integer $I = O(\log(S))$ and look for the I first primes $(\ell_i)_{1\le i\le I}$ that split . If we have any difficulty finding such primes i.e. if the small primes are not Elkies then we pick another curve E_0. Another approach would be to check that the elliptic curve has many small Elkies primes before computing its cardinality. By exhaustive search it is reasonable to look for an elliptic curve on $GF(2^{80})$ with all twenty smallest primes Elkies primes.

We then compute the class number and class group of $\mathbb{Z}[\sqrt{\Delta}]$. This is done using Hafner-McCurley-Buchman's algorithm [5, 1]. The complexity of this algorithm is subexponential. Implementations in progress [7] achieve this computation within a few days on a station for Δ of size 10^{70} although many improvements and tricks are still to be implemented. Thus computing the class group for a Δ of size 10^{80} will be soon a standard calculation. The algorithm will also give us the module of relations between the $[\mathfrak{l}_i]$ i.e. the kernel $\mathcal{R}$ of the map

$$G: \qquad \mathbb{Z}^I \longrightarrow \mathcal{CL}(\mathcal{O}_{\mathbb{K}})$$

$$(x_1, ..., x_I) \longmapsto \prod_i [\mathfrak{l}_i]^{x_i}$$

We observe that the discriminant of $\mathcal{R}$ is the cardinality of $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$. Since the dimension is I we expect to find a basis of size $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})^{1/I}$. In order to simplify the presentation we assume that $\mathcal{CL}(\mathcal{O}_{\mathbb{K}})$ is cyclic although this is by no way essential.

We compute the $(e_{i,j})_{i,j}$ applying LLL to $\mathcal{R}$. For S of size 10^{40} with $I = 40$ one finds small $e_{i,j}$'s (between -17 and 17 experimentally with an average absolute value smaller than 3) in a few minutes. We note that LLL is not garanteed to success there although it works surprisingly well in practice. We discuss these questions in the next paragraph.

As for modular equations $\mathcal{E}_{\ell_i}(x, y)$ for $1 \le i \le I$, these are everywhere. We only need to store these equations modulo p the characteristic. This is why we prefer $p = 2$. Since the degree of $\mathcal{E}_\ell$ is $\ell+1$ in each variable we need $(\ell+1)(\ell+2)/2$ bits to store it modulo 2.

5.5 Cyclic groups with prescribed generators

We study here the problem we encountered above of representing an arbitrary element w in a cyclic group $\mathbb{Z}/S\mathbb{Z}$ as a linear combination of certain given elements

$(g_i)_{1\leq i\leq I}$. To be simpler we shall deal with the slightly more restrictive question of expressing w as a subset sum of the g_i's. We use standard tools see [6]. We assume we are given a cyclic group $G = \mathbb{Z}/S\mathbb{Z}$ and a random sequence of elements $(g_i)_{1\leq i\leq I}$ in G. For $1 \leq n \leq I$ we call X_n the set of sums $\sum_{k\in J} g_k$ where J is any subset of $\{1, 2, ..., n\}$. We call α_n the ratio $\#X_n/S$ i.e. the density of X_n. We want to show that for n big enough this density is very likely to be 1.

We shall compare α_n and α_{n+1}. We know that X_n is a subset of G with cardinality $\alpha_n S$ and take $y = g_{n+1}$ to be a random element in G. Then $X_{n+1} = X_n \cup X_n + y$. We claim that for any fixed X_n the average cardinality of $X_n \cup X_n + y$ is $(\alpha_n + \alpha_n(1 - \alpha_n))S$. Indeed for any two subsets A and B of G the average cardinality of $A \cap B + y$ when y runs over all values of G is $\#A\#B/N$ (exercise). We then take $A = \bar{X}_n$ the complement of X_n and $B = X_n$ and we get the desired result.

We thus reduce to the study of the iterated sequence

$$u_{n+1} = f(u_n) \text{ with } f(X) = 2X - X^2.$$

We see from the graph of f that $(u_n)_n$ will have a geometric behaviour (i.e. $u_{n+1} \sim 2u_n$) as long as it is small enough. When it gets close to 1 the behaviour is quadratic i.e. $(1-u_{n+1}) \sim (1-u_n)^2$. From this one deduces that for n greater than a constant times $\log_2(S)$ the set X_n is equal to G with overwhelming probability.

So we see that representations of w as a linear combination of the $(g_i)_{1\leq i\leq I}$ with small coefficients do exist. We can look for them using LLL algorithm. Of course there is an exponential (in the dimension) factor in the bound for the norm of LLL reduced basis so that we are no sure to catch an actual small vector. In practice however we can find really small coefficients as already mentioned.

If we have represented well choosen w's as a linear combination of the $(g_i)_{1\leq i\leq I}$ with small coefficients we can then obtain decent expressions for all values of w. In the previous section we recommanded to use $w = 1, 2, 2^2, 2^3, ...$ but any decreasing sequence of integers such that $x_0 = S$ and $x_{n+1} \geq x_n/2$ will work.

5.6 Efficiency

As interesting as they may be from the point of view of complexity theory the above HHS are still far from competing with classical ones. The construction of the HHS should require a few days of CPU on a workstation which is reasonable. The size of the public data also is reasonable (a few kilo bites). The difficulty will be in computing the action of some element of the class group on some curve. Experimental data show that the time required to authentify safely on a standard work station following the above scheme is of a few hours. There is certainly much to be thought about improving the scheme presented above. To start with, we may not use the $e_{i,j}$ and look for the a_i directly using LLL. This is not garanteed to work but it will provide much smaller a_i on average. Another possibility would be to use abelian varieties of higher dimension over a smaller field since they have in a sense more isogenies of small degree but it is not yet clear how to make this idea work in practice.

5.7 Class field theory

In this paragraph we show that the discrete logarithm problem over a finite field, the discrete logarithm problem over an elliptic curve and the HHS we introduced are actually the three most elementary HHS one can obtain from class field theory. We just recall the context.

Assume we have a number field $\mathbb{K}$ and an abelian extension $\mathbb{L}$ of $\mathbb{K}$. We call $\mathcal{O}_{\mathbb{K}}$ and $\mathcal{O}_{\mathbb{L}}$ the ring of integers. Let $\mathfrak{q}$ be a prime in $\mathcal{O}_{\mathbb{L}}$ of residual degree 1. Set $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_{\mathbb{K}}$ and p the characteristic of the residue field $\mathbb{F}_p$. We assume there is no ramification at $\mathfrak{p}$. Let $\zeta = (\zeta_1, ..., \zeta_u)$ be a set of integral generators of $\mathbb{L}$ over $\mathbb{K}$. We call $\bar{\zeta} \in {\mathbb{F}_p}^u$ the reduction of ζ modulo $\mathfrak{q}$. For σ an element of the Galois group G of $\mathbb{L}/\mathbb{K}$ we denote by $\zeta^\sigma = (\zeta_i^\sigma)_{1 \le i \le u}$ the conjugate of ζ by σ. Since there is no ramification at $\mathfrak{p}$ the conjugates of ζ have pairwise distinct reductions modulo $\mathfrak{q}$. We call H the set of all these vectors in ${\mathbb{F}_p}^u$ that are reductions of conjugates of ζ. This H is clearly acted on simply transitively by G. This action is the action induced on the $\bar{\zeta}$'s by the Galois action on the ζ. And class field theory tells us that in some cases there is a way to compute this action *inside* $\mathbb{F}_p$ in polynomial time by some geometric construction.

We review the three most classical cases of this situation and find our discrete logarithms and new HHS.

1. If $\mathbb{K} = \mathbb{Q}$ and $\mathbb{L} = \mathbb{Q}(\zeta_n)$ where n is a primitive n-th root of unity and $\mathfrak{p} = p\mathbb{Z}$ with $n|p-1$. The group G is canonically isomorphic to $(\mathbb{Z}/n\mathbb{Z})^*$ and the action of $\sigma \in (\mathbb{Z}/n\mathbb{Z})^*$ on $\bar{\zeta}_n$ is just by exponentiation. We find the discrete logarithm problem in a subgroup of $(\mathbb{Z}/p\mathbb{Z})^*$.

2. Suppose $\mathbb{K} = \mathbb{Q}(j_n)$ is the definition field of an elliptic curve (E, T) with complex multiplication and n-torsion structure $j_n \in X_0(n)$. This means E is an elliptic curve over $\mathbb{K}$ and T a one dimensional n-torsion space on E. Let $\mathfrak{p}$ be a prime in $\mathbb{K}$ with residue field $\mathbb{F}_p$ with p prime to n. Let $\mathbb{L} = \mathbb{K}(P)$ be the field of definition of an n-torsion point $P \in T$ and assume that $\mathfrak{p}$ splits in $\mathbb{L}$ and we call $\mathfrak{q}$ a prime above it. The action of the Galois group G on the points in T identifies G with a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. All the points in T reduce modulo $\mathfrak{q}$ to points defined over $\mathbb{F}_p$. We end up with the problem of discrete logarithm in $E \bmod p$.

3. Suppose $\mathbb{K}$ is $\mathbb{Q}$ and $\mathbb{L}$ is $\mathbb{Q}(j)$ with j the invariant of an elliptic curve E with complex multiplication. Take a prime $\mathfrak{p} = p\mathbb{Z}$ that splits in $\mathbb{L}$. Here G is identified with the class group of the endomorphism ring of E. When reducing modulo $\mathfrak{q}$ we obtain the HHS presented above.

We observe that we may mix the last two examples considering the Galois action on curves with torsion structure over $\mathbb{Q}$ let's say.

The main difference between cases 1 and 2 and case 3 is that in cases 1 and 2 elements of H are also generators of an algebraic group. This allows fast exponentiation. In case three on the contrary we have nothing like an algebraic group (rather correspondances on a moduli space).

As we can see, any class field theory leads to an homogeneous space. It may be that well choosen CM abelian varieties of higher dimension are of some use.

6 Conclusion

We have introduced the notion of Hard Homogeneous Space and we have shown its relevance to cryptography. We also have shown that it provides a range of new algorithmic problems to do cryptography with. The discrete logarithm problems on finite fields or elliptic curves are special cases of HHS. Although the new HHS that we discribed are not practical enough to be used efficiently as they are now, one can hope for improvements. The bottleneck is solving modular equations efficiently. Alternatively one may look for completely different HHS based on other mathematical ideas. In any case it is interesting to look at discrete logarithm problem from the point of view of HHS. Not all the algorithmic ideas for discrete logarithm generalize to HHS. As we have seen there is no fast exponentiation on a HHS. We instead have the notion of prescribed *easy* generators and the related problems connected with integer lattices problems.

From the point of view of complexity theory HHS provide a bridge between the discrete logarithm problem and the graph (non) isomorphism one.

References

[1] J. Buchmann. On the computation of units and class numbers by a generalization of lagrange algorithm. *Journal of Number Theory*, 26:8–30, 1987.

[2] Henri Cohen. *A course in computational algebraic number theory*. Number 138 in Graduate texts in Mathematics. Springer, 1993.

[3] A. Fiat and A. Shamir. How to prove yourself: practical solutions to identification and signature problems. *Advances in Cryptology - CRYPTO'86*, 263:186–194, 1986.

[4] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity and a methodology of cryptographic protocol design. *Proceedings of the 27th Symposium on the Foundation of Computer Science FOCS*, pages 174–187, 1986.

[5] J. Hafner and K. McCurley. A rigorous subexponential algorithm for computation of class groups. *Journal of the American mathematical society*, 2:837–850, 1989.

[6] H. Halberstam and K.F. Roth. *Sequences*. Oxford, 1966.

[7] Michael Jacobson. personnal communication.

[8] D. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Thesis of the University of California, 1996.

[9] H. W. Lenstra. Complex multiplication structure of elliptic curves. *Journal of Number Theory*, 56(2):227–241, 1996.

[10] R. Lercier and F. Morain. Counting the number of points on elliptic curves over finite fields: strategies and performances. In L.C. Guillou and J.-J. Quisquater, editors, *Advances in cryptology, EUROCRYPT 95*, volume 921 of *Lecture notes in computer science*, pages 79–94. Springer, 1995.

[11] David Pointcheval. *Les preuves de connaissance et leurs preuves de sécurité*. École Normale Supérieure, 1996.

[12] Goro Shimura. *Automorphic Functions and Number Theory*. Number 54 in Lecture Notes in Mathematics. Springer, 1968.

[13] J. H. Silverman. *The arithmetic of elliptic curves*. Number 106 in Lecture Notes in Mathematics. Springer, 1986.

[14] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*. Number 151 in Lecture Notes in Mathematics. Springer, 1994.