

# Cover Attacks

## A report for the AREHCC project

Claus Diem and Jasper Scholten

September 29, 2003

### 1 Introduction

In this report, we give an overview of a certain class of attacks on elliptic and hyperelliptic curve cryptography. The attacks we will discuss are only applicable if one considers discrete logarithms in class groups of elliptic or hyperelliptic curves over finite *non-prime* fields.

Let us state the general idea of the class of attacks we will consider:

Let  $H/K$  be a elliptic or hyperelliptic curve (or even a more general curve) defined over a finite non-prime field  $K$ . Assume that the DLP in the divisor class group  $\text{Cl}^0(H/K) = \text{Jac}(H)(K)$  of  $H/K$  (of degree 0) is used as a cryptographic primitive. (Note that if  $E$  is an elliptic curve, one has a canonical isomorphism  $E(K) \simeq \text{Cl}^0(E/K)$ , thus we consider in particular the DLP in elliptic curves.)

The assumption that the DLP is used as a cryptographic primitive means in particular that  $\text{Cl}^0(H/K)$  contains a large subgroup of prime order. We will use this fact in the following.

If the genus of  $H$  would be  $\geq 4$  (and maybe  $\geq 3$ ), index calculus attacks on  $\text{Cl}^0(H/K)$  would be more efficient than “generic attacks” like Pollard  $\rho$ . If however the genus of  $H$  is 1 or 2, generic attacks are more efficient than index calculus attacks; c.f. [4], [7], [17].

The idea is now to transfer the DLP in  $\text{Cl}^0(H/K)$  in a DLP in the class group of a curve of higher genus over a smaller field.

Let us assume that  $K$  is an extension of another finite field  $k$ . (The field  $k$  need not be a prime field.) Let us fix explicitly that  $\text{char}(k) = p$ ,  $k = \mathbb{F}_q$  and  $K = \mathbb{F}_{q^n}$ , i.e.  $[K : k] = n$ . Assume that we have an explicitly given curve  $C/k$  defined over  $k$  and an explicitly given cover  $c : C \rightarrow H$  defined over  $K$ . (A non-constant morphism between two curves is called a *cover*.)

Then we have the *conorm* or *pull-back map*  $c^* : \text{Cl}^0(H/K) \rightarrow \text{Cl}^0(C/K)$ , and we also have the *norm map*  $N : \text{Cl}^0(C/K) \rightarrow \text{Cl}^0(C/k)$ . By composing

these two maps, we obtain a map

$$N \circ c^* : \text{Cl}^0(H/K) \longrightarrow \text{Cl}^0(C/k). \quad (1)$$

Let us assume that the subgroup of large prime order of  $\text{Cl}^0(H/K)$  is preserved under this map, i.e. it does not lie in the kernel. Then one might try to map the DLP from  $\text{Cl}^0(H/K)$  to  $\text{Cl}^0(C/k)$  and solve it in the latter group via index calculus. We will call such an attack on the DLP in a curve  $H/K$  a *cover attack*.

If the group order of  $\text{Cl}^0(H/K)$  is nearly prime (i.e. prime up to a small factor 2,3,4,5 say), the genus of  $C$  is at least equal to the  $g(H)n$ , where  $g(H)$  is the genus of  $H$ .

Here is an intuitive argument for this:

By assumption the kernel of the map  $N \circ c^*$  is very small – let us assume that it is trivial. Then  $\log_q(\#\text{Cl}^0(C/k)) \geq \log_q(\#\text{Cl}^0(H/K))$ . Now by the bounds of Hasse-Weil,  $\log_q(\#\text{Cl}^0(C/k))$  is roughly  $g(C)$ , and  $\log_q(\#\text{Cl}^0(H/K))$  is roughly  $ng(H)$ . We thus get

$$g(C) \geq g(H)n. \quad (2)$$

Sometimes in the cryptological applications, one considers the following applications:

Let the curve  $H$  be defined over  $k$ , but consider it over  $K$ . Then  $\text{Cl}^0(H/K)$  contains  $\text{Cl}^0(H/k)$ . On the other hand,  $\text{Cl}^0(H/K)$  contains another group, called *trace-zero group* (see Section 4) which most of the time in the applications has trivial intersection with  $\text{Cl}^0(H/k)$  inside  $\text{Cl}^0(H/K)$ . If one now assumes that the order of the trace-zero group is nearly prime, one can use the DLP in this group as a cryptographic primitive.

Now in order to be able to transfer this DLP into the DLP in  $\text{Cl}^0(C/k)$ , one has to assume that the large prime factor of the trace-zero group is preserved under the above map. Under this condition, one obtains with the same arguments as above

$$g(C) \geq g(H)(n - 1). \quad (3)$$

From a practical point of view, this inequality only makes a difference to equality (2) if  $n$  is small, say 3 or 5.

Note that attacks on the DLP in  $\text{Cl}^0(C/k)$  become less efficient if – given the size of the ground field – the genus of  $C$  grows. For this reason it is of greatest importance for the practicability of the attack that  $g(C)$  is “as small as possible”.

Let us repeat what we need to make the attack work. We need an explicitly given curve  $C/k$  and a morphism  $c$  from  $C$  to  $H$  defined over  $K$  such that

- the kernel of  $N \circ c^*$  does not contain the large subgroup of prime order of  $\text{Cl}^0(H/K)$
- the genus of  $C$  is “not too large”.

Furthermore, it would be best if the curve  $C$  would be hyperelliptic or given by another “easy” equation, for example if it would be superelliptic. Automorphisms of  $C$  would lead to a further speed up.

The formulation that the genus of  $C$  should “not be too large” is of course very vague. What is “too large” depends of course on the state of the art in index calculus attacks. For large  $n$ , by the results of Enge and Gaudry ([4]), one might say that  $g(C)$  is “small enough” if  $g(C)$  is  $\leq (g(H)n)^2$ .

For very small numbers (like  $n = 5, 7$  and  $g(H) = 1$ ), it would be best if  $g(C)$  is equal to  $g(H)n$  (or  $g(H)(n - 1)$  in the “trace-zero” case) or only slightly bigger.

In Sections 3 to 5, we will give three (potential) methods to construct a curve  $C/k$  and a homomorphism as in (1). The first method is the GHS-attack and several generalizations of it, the second one is an attack developed by the authors to specifically attack DLPs in trace-zero groups, the third one is another potential new attack developed by the authors.

## 2 Cover attacks and the Weil restriction

The *Weil restriction* is an important mathematical tool to study cover attacks.

As above, let  $K/k$  be an extension of finite fields of degree  $n$ .

Let  $V$  be a (affine or projective) variety defined over  $K$  (for example a curve). Then there exists an  $n$ -dimensional (affine resp. projective) variety  $W/k$  and a morphism  $u : W \rightarrow V$  defined over  $K$  which has the following *universal property*:

For every variety  $X$  defined over  $k$  and every morphism  $c : X \rightarrow V$  defined over  $k$ , there exists a unique morphism  $a : X \rightarrow W$  defined over  $K$  with  $c = u \circ a$ .

Note that this means in particular that we have a bijection between  $\text{Mor}_K(X, V)$  and  $\text{Mor}_k(X, W)$ , where  $\text{Mor}_K(X, V)$  denotes the set of morphisms from  $X$  to  $V$  defined over  $K$  and  $\text{Mor}_k(X, W)$  denotes the set of morphisms from  $X$  to  $W$  defined over  $k$ .

The above variety  $W/k$  is “essentially unique”, it is called the *Weil restriction of  $V$  with respect to  $K/k$* .

In particular, the universal property of the Weil restriction can be applied to the case that the variety  $X$  consists of just one point (a point is also a variety). So let  $X$  be a point. Then the morphisms from  $X$  to  $V$  defined

over  $K$  are just the points of  $V$  whose coordinates all lie in  $K$ . Such points are called  $K$ -rational, and the set of  $K$ -rational points is denoted by  $V(K)$ . Explicitly, if one is given a morphism from the point  $X$  to  $V$ , one assigns to it the image of  $X$  in  $V$  which is a  $K$ -rational point. On the other hand, to a  $K$ -rational point  $P$  on  $V$  one assigns the morphism  $X \rightarrow V$  which maps the point  $X$  to  $P$ .

These considerations can also be made for morphisms from  $X$  to  $W$  defined over  $k$  and  $k$ -rational points of  $W$ . We thus have canonical bijections  $V(K) \simeq \text{Mor}_K(X, V)$  and  $W(k) \simeq \text{Mor}_k(X, W)$ . Together with the above bijection  $\text{Mor}_K(X, V) \simeq \text{Mor}_k(X, W)$ , we obtain the bijection

$$V(K) \simeq W(k). \tag{4}$$

Sometimes one can define an algebraic group law on a variety: An algebraic group law on  $V$  is by definition a morphism  $m : V \times V \rightarrow V$  such that for all field extensions  $\lambda/k$ ,  $V(\lambda)$  with the composition  $P + Q := m(P, Q)$  is a group. A variety defined over  $K$  with an algebraic group law which is also defined over  $K$  is called *group variety* defined over  $K$ . Projective group varieties are called *abelian varieties*. One can show that the group law of an abelian variety is always commutative. A very important special case of abelian varieties are the *elliptic curves* which are by definition nothing but 1-dimensional abelian varieties.

If  $V$  is a group variety, then there also exists a canonical algebraic group law on the Weil restriction  $W$  defined over  $k$ . With this group law,  $W$  becomes a group variety defined over  $k$ . Now both sets  $V(K)$  and  $W(k)$  are groups, and in fact (4) is a group isomorphism. In particular, if  $E$  is an elliptic curve defined over  $K$  and  $W/K$  is the Weil restriction of  $E$  with respect to  $K/k$ , we obtain an isomorphism

$$E(K) \simeq W(k). \tag{5}$$

The importance of the Weil restriction in the context of cover attacks is derived from the universal property:

If  $H/K$  is a hyperelliptic curve and  $C/k$  is another curve and we have a morphism  $c : C \rightarrow H$  defined over  $K$ , then we have a unique morphism  $a : C \rightarrow W$  defined over  $k$ . The converse is also true.

If one has such an  $a : C \rightarrow W$ , one can study its image on  $W$ , and in this sense, the search for curves on  $W/k$  amounts to the same as the search curves  $C/k$  and morphisms  $C \rightarrow H$  defined over  $K$ . Thus the search for curves on  $W/k$  is an approach to the problem of making the general idea of cover attacks explicit.

### 3 The GHS-attack and its variants

We will use the theory of function fields (in one variable) instead of the theory of curves.

Let us recall the connection between these two theories. For further information on function fields, see [16].

Let  $K$  be a finite field. Then for every curve  $C/K$ , one can define an addition and a multiplication on the set of rational functions  $C \rightarrow \mathbb{P}^1/K$  defined over  $K$ . With these operations, this set becomes a field, called the *function field* of  $C/K$  and denoted  $K(C)$ . This field is a finitely generated extension of  $K$  of transcendence degree 1, i.e. it is an (abstract) function field over  $K$ . Moreover,  $K$  is the exact constant field of  $K(C)$ , which means that  $K$  is algebraically closed in  $K(C)$ .

Now, if  $\alpha : C \rightarrow D$  is a cover of two curves defined over  $K$ , we have a corresponding homomorphism  $\alpha^\# : K(D) \rightarrow K(C)$  which is defined by  $\beta \mapsto \beta \circ \alpha$ .

Conversely, to every function field with exact constant field  $K$ , one can assign in an essentially unique way a curve defined over  $K$ . If  $a : L \hookrightarrow M$  is a homomorphism of such function fields,  $C$  is the curve corresponding to  $M$  and  $D$  is the curve corresponding to  $L$ , there exists a unique curve cover  $\alpha : C \rightarrow D$  with  $\alpha^\# = a$ .

Let  $C/K$  be a curve with function field  $L/K$ , let  $\bar{K}$  be the algebraic closure of  $K$ . To every  $\bar{K}$ -rational point of  $C$ , one can associate a so-called *place* of  $L/K$ . If  $K$  is itself algebraically closed, this assignment is a bijection, in the general case, places correspond to Galois-orbits of  $\bar{K}$ -rational points on  $C$ .

Now just as for curves one can define a divisor class group for function fields, and for a curve  $C$  defined over  $K$ , the groups  $\text{Cl}^0(C)$  and  $\text{Cl}^0(K(C))$  are equal.

The GHS-attack is originally an attack on elliptic curves defined over non-prime finite fields of characteristic 2; see [8]. Here we give a generalization of the attack to arbitrary (hyper-)elliptic curves over non-prime finite fields; see [3].

Let  $K/k$  be an extension of finite fields of characteristic  $n > 1$ . Let  $H/K$  be a (hyper-)elliptic curve.

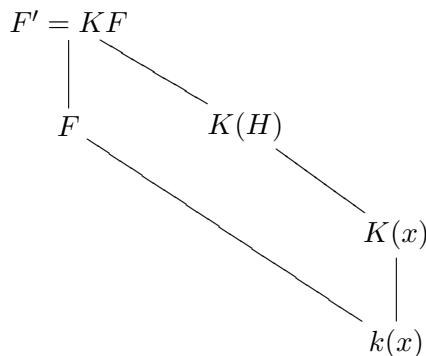
Let  $K(x)$  be the rational function field,  $K(H)$  the function field of  $H/K$ , and fix an extension  $K(H)/K(x)$  of degree 2. For  $\sigma \in \text{Gal}(K/k)$ , let  $K(H)^\sigma$  be the corresponding ‘‘Galois twisted’’ function field. This is defined as follows:

The automorphism  $\sigma$  of  $K/k$  can in a unique way be extended to an

automorphism of  $K(x)/k(x)$ , let us denote this automorphism again by  $\sigma$ . If  $K(H) \simeq K(X)[T]/(f)$  where  $f \in K(X)[T]$ , then  $K(H)^\sigma \simeq K(X)[T]/(f^\sigma)$ . Here,  $f^\sigma$  is obtained by applying  $\sigma$  to the coefficients of  $f$  (which lie in  $K(x)$ ).

Just as  $K(H) \simeq K(x)[T]/(f)$  is an extension of degree 2 of  $k(x)$ , so is  $K(H)^\sigma \simeq K(x)[T]/(f^\sigma)$ .

Let  $F'$  be a compositum of  $K(H), K(H)^\sigma, \dots, K(H)^{\sigma^{n-1}}$  over  $K(x)$ . It is easy to see that either  $K$  is the exact constant field of  $F'$  or the unique quadratic extension of  $K$  is the exact constant field of  $F'$ . For the applications, we can always assume that we are in the first case. Now under certain conditions, for example if  $n = 2$  or  $n$  is odd, there exists a subfield  $F$  of  $F'$  which has  $k$  as its exact constant field such that  $F' = KF$ .



We have a homomorphism

$$N_{F'/F} \circ \text{Con}_{F'/K(H)} : \text{Cl}^0(K(H)) \longrightarrow \text{Cl}^0(F), \quad (6)$$

where  $\text{Con}_{F'/K(H)}$  is the conorm homomorphism and  $N_{F'/F}$  is the norm homomorphism. If one sets  $C/k$  to be the curve corresponding to the function field  $F/k$ , this homomorphism becomes a special case of homomorphism (1).

Recall that the first condition for the feasibility of a cover attacks is that the kernel of homomorphism (1), i.e. (6) in the special case we consider, is small.

One can show that under obviously necessary conditions in order that this is the case, the homomorphism contains only elements of order a power of 2. If for example  $n$  is a prime number and  $F' \not\supseteq K(H)$ , this is the case; see [3, Theorem 1].

From a theoretical point of view, the study of the GHS-attack is quite different for even and odd characteristic. Besides the original paper ([8]), the even characteristic case is discussed in [13], [5], [11], [12], [6] and [9]. The odd characteristic case is discussed in [3] and [18].

Will will now address the following question: Given a field extension  $K/k$  of degree  $n$  and a natural number  $g$ , what is the minimal genus one

can obtain for a curve  $C/k$  one obtains by applying the GHS-attack to a (hyper-)elliptic curve of genus  $g$  over  $K$ ?

Additionally, we are interested if the extension  $F'/K(x)$  has a subfield of index 2 which is rational. If this is so, the curve  $C/K$  corresponding to  $F'/K$  will be hyperelliptic, if not, we cannot rule out that it is hyperelliptic but one might expect that “in general” it is not.

By construction of  $F'$ , there exists a number  $m \in \mathbb{N}$  such that  $[F' : K(x)] = 2^m$ . In a certain sense one can say that this “magic number” controls the genus of  $F'$  (or  $F$ ). Let us note that our assumption that  $K$  is the exact constant field of  $F'$  is equivalent to  $[F' : K(H)] = [F'\overline{K} : \overline{K}(x)]$ .

We now discuss the attack separately for even and odd characteristic. In even characteristic, one can use Artin-Schreier Theory to study the field  $F'$ , and in odd characteristic one can use Kummer Theory.

### 3.1 Even characteristic

The extension  $K(H)/K(x)$  is an Artin-Schreier extension. From this and general facts on the genera of composita of function fields, we have the following relation between the genus of  $F$  and  $m$ :

$$g(F) \leq 2^m g(H) \tag{7}$$

In certain cases, one can prove that  $g(F) = g(H)2^{m-1}$  or  $g(F) = g(H)2^{m-1} - 1$  and  $F$  is hyperelliptic; see [19]. In general, we are convinced that the genus cannot become “much smaller” than  $g(F)2^{m-1}$ . (For example, if  $H$  is an elliptic curve, it can be proved that  $g(F) \geq 2^{m-1} - 1$ .)

Let  $y^2 + y = f(x)$  be a defining equation with  $f \in K(x)$ . By Artin-Schreier theory, the extension  $F'/K(x)$  corresponds to a vector subspace  $U$  of the  $\mathbb{F}_2$ -vector space  $K(x)/\mathcal{P}(K(x))$ , where  $\mathcal{P}$  is the Artin-Schreier operator. The “magic number”  $m$  is equal to  $\dim_{\mathbb{F}_2}(U)$ . Now  $\text{Gal}(K/k)$  operates on this space in a canonical way, and by construction,  $U$  is generated by  $\bar{f}$  as a  $\mathbb{F}_2[\text{Gal}(K/k)]$ -module, where  $\bar{f}$  is the residue class of  $f$  in  $K(x)/\mathcal{P}(K(x))$ .

The fact that  $U$  is a  $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}] \simeq \mathbb{F}_2\mathbb{F}_2[\text{Gal}(K/k)]$ -module imposes strong conditions on the values  $m$  can obtain.

For some prime number  $p$ , let  $\varphi_p(n)$  be the order of  $p$  in  $(\mathbb{Z}/n\mathbb{Z})^*$ , so that  $[\mathbb{F}_p(\zeta_n) : \mathbb{F}_p] = \varphi_p(n)$ .

Let us now make the assumption that  $n$  is prime. (This does not necessarily mean that the absolute extension degree  $[K : \mathbb{F}_p]$  is prime.) Then  $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}] \simeq \mathbb{F}_2 \oplus \mathbb{F}_2(\zeta_n)^{(n-1)/\varphi_2(n)}$ . The fact that  $U$  is a non-trivial  $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$ -module implies that

$$m = \kappa\varphi_2(n) \text{ or } m = \kappa\varphi_2(n) + 1 \tag{8}$$

with some natural number  $\kappa = 1, \dots, \frac{n-1}{\varphi_2(n)}$ . As the genus of  $F$  is roughly  $g(H)2^{m-1}$ , this means that one can expect the genus of  $F$  to be in the magnitude of

$$g(H)2^{\kappa\varphi_2(n)}.$$

It is not difficult to show that for a given extension  $K/k$  there exist ordinary (hyper)-elliptic curves of a given genus such that  $\kappa = 1$ . (An elliptic curve is ordinary if and only if it is non super-singular.) Now, the attack is most feasible if  $2^{\varphi_2(n)}$  is not much larger than  $n$ . This is the case for *Mersenne primes*. These are primes  $n$  of the form  $2^a - 1$ . For these primes,  $\varphi_2(n) = a$  and thus  $2^{\varphi_2(n)} = n + 1$ . The Mersenne primes in the cryptographically important range are

$$3, 7, 31, 127.$$

For the primes 7, 31, 127, some curves in cryptographically important range (i.e. 160 bit) can efficiently be attacked. For more information, we refer to [11].

The next best class of primes (best from the point of view of this attack) are the *Fermat primes*. In the cryptographically important range they are

$$3, 5, 17, 257.$$

Explicitly, if  $n = 5$  and  $g(H) = 1$ , the minimal genus one can obtain is 7, if  $n = 17$ , the minimal genus is 127, and for  $n = 257$ , it is 32768. For the latter two cases,  $g(F)$  is already quite high in relation to  $n$ . In these cases, it might be that the index-calculus attack by Enge-Gaudry is faster than the generic attacks on the original curves, but it will probably not be a major improvement.

Finally, let us mention that if  $E$  is an ordinary elliptic curve, one can always choose an extension  $K(E)/K(x)$  such that  $F$  is hyperelliptic. In [8], explicit equations for  $F$  are given.

For more information on the GHS attack applied to composite field extensions, we refer to [12].

### 3.2 Odd characteristic

As above, the “magic” number  $m$  is of greatest importance when one tries to determine the genus of  $F$ .

Let  $r$  be the number of branched places of  $\overline{K}F/\overline{K}(x)$ . Then

$$g(F) = 2^{m-2}(r - 4) + 1; \tag{9}$$

see [3, Equation (7)]. For prime  $n$  and elliptic curves  $H$  it is shown in [3]:



- If  $n = 2, 3, 5, 7$  there exists an elliptic curve  $E$  over  $K$  such that  $g(F) = n$ . If  $n = 2$  or  $3$ ,  $E$  can additionally be chosen such that  $F$  is hyperelliptic.
- If  $n \geq 11$  and  $\#K \geq 2^{160}$ , then  $\#\text{Cl}^0(F) \approx \#k^{g(F)} \geq 2^{5000}$ .

It follows that the GHS attack in odd characteristic is not a threat to the DLP in elliptic curves if the absolute extension degree  $[K : \mathbb{F}_p]$  is prime and not 3, 5 or 7. As index calculus attacks for genus 3 curves are not much more efficient than generic attacks, for  $n = 3$ , the attack only gives at most a minor improvement on the generic attacks. However by the results of N. Thériault on index calculus with “large primes” ([17]), the attack will probably give a small improvement (in the order of 1/20 of the key size).

The results for  $n = 2$  and  $n = 3$  can be generalized to some (hyper-)elliptic curves  $H$ . For  $n = 2$ , there exist (hyper-)elliptic curves  $H$  of any genus over  $K$  such that  $g(F) = 2g(H)$ . For  $n = 3$ , there exist (hyper-)elliptic curves  $H$  of any genus over  $K$  such that  $g(F) = 4g(H) - 1$  and  $F$  is hyperelliptic. Moreover, there is an algorithm to determine – given a hyperelliptic equation of  $H$  – an equation of  $F$ ; see [18] for details.

For  $n = 3$ , one can with the methods of [3] also obtain hyperelliptic curves  $H/K$  of a given genus such that  $g(F) = 3g(H)$ . For this, let  $g \in \mathbb{N}$ ,  $[K : k] = 3$ ,  $a_1, \dots, a_{g+1} \in K \setminus k$  such that  $a_1, a_1^q, \dots, a_{g+1}, a_{g+1}^q$  are pairwise distinct. (Here  $q = \#k$ .) Then the curve given by an equation of the form

$$y^2 = (x - a_1)(x - a_1^q)(x - a_2)(x - a_2^q) \cdots (x - a_{g+1})(x - a_{g+1}^q) \quad (10)$$

is a hyperelliptic curve of genus  $g$  such that  $g(F) = 3g(H)$ . However, the extension  $F'/K(x)$  does not possess a subfield of index 2 which is rational. Note however that the extension  $F/k(x)$  has degree 4 which is rather small.

In the following table, we give for certain small  $n$  the smallest genera one can with the GHS attack obtain for the resulting function field  $F$ .

		$n$						
		2	3	4	5	7	11	
$g(H)$	1	2	3	5	5	7	$\geq 1793$	(11)
	2	4	6	9*	25	49	$\geq 1793$	
	3	6	9	21	25	21	$\geq 1793$	

(\*) Note: We do not know that for  $n = 4$  and  $g(H) = 2$ , the function field  $F$  exists. The problem is that we do not know whether one can prolong the Frobenius from  $K(x)/k(x)$  to  $F'$ . The other cases do not cause problems as always  $n$  is odd or  $m = n$  (see also next table).

Let us describe how one can obtain curves  $H/K$  corresponding to the entries in the table.

The Galois group  $\text{Gal}(\overline{K}/k)$  operates on the branched places of  $\overline{K}F'/\overline{K}(x)$  cyclicly. (If all branched places of  $F'/K(x)$  have degree 1, then  $\text{Gal}(K/k)$  operates on the branched places of  $F'/K(x)$ .) We fix the following notation: If  $(p_1, \dots, p_d)$  is a cycle under this operation (where  $d|n$  if the branched places of  $F'/K(x)$  have degree 1), then we define a vector in  $\mathbb{F}_2^d$  whose entries are 1 at entry  $i$  if and only if  $F'/K(x)$  is also branched at  $p_i$ . Then to each  $K(H)/K(x)$  we assign the tuple of these vectors in  $\mathbb{F}_2^d$  representing all cycles (the tuples should be ordered by length).

Let us for example consider the above curve given by (10). In this case, the corresponding tuple is

$$(110)(110) \cdots (110).$$

From this tuple, the number of branched places  $r$  and the “magic number”  $m$  can be calculated. In the following table, we give tuples with the corresponding  $r$  and  $m$  which lead to the above table (11). (The last column of the table follows with (9).)

$g(H)$	$n$	tuple	$r$	$m$	$g(F)$
1	2	(1)(1)(1)(10)	5	2	2
	3	(110)(110)	6	2	3
	4	(1)(1110)	5	4	5
	5	(11110)	5	4	5
	7	(1110100)	7	3	7
2	2	(1)(1)(1)(1)(1)(10)	7	2	4
	3	(110)(110)(110)	9	2	6
	4	(1110)(1110)	8	3	9
	5	(1)(111110)	7	5	25
	7	(1111110)	7	6	49
3	2	(1)(1)(1)(1)(1)(1)(1)(10)	9	2	6
	3	(110)(110)(110)(110)	12	2	9
	4	(1)(1)(1)(1)(1)(1)(1110)	9	4	21
	5	(11110)(11110)	10	4	25
	7	(1110100)(1110100)	14	3	21

### 3.3 Extensions of the GHS attack and conclusion

Additionally to the generalizations of the original GHS attack described here, there are some further extensions of the attack.

The first one is not to restrict oneself to extensions  $K(H)/K(x)$  of degree 2. Indeed, whenever  $H$  has an automorphism which induces a (cyclic) Galois cover  $H \rightarrow \mathbb{P}^1$ , one can use this automorphism to fix a Galois extension  $K(H)/K(x)$ . Then one can define  $F'$  and  $F$  as above. This approach is described in [9], [19] and [18].

Further, if  $E$  is an elliptic curve, one can try to first apply an isogeny and then use the GHS attack with respect to the isogenous curve. For characteristic 2, this approach is discussed in [6]. Because of this possibility, one should – if one uses elliptic curves – avoid all fields over which there exists *some* elliptic curve which can by the GHS attack be attacked in such a way that the number of bit operations required for the index calculus is less than the prescribed security level.

All in all, we give – with respect to the GHS-attack – the following advice for the use of (hyper-)elliptic curves over non-prime finite fields.

- Composite field extensions should be avoided unless one has checked that over the field in question there does not exist a single “weak curve”.
- For characteristic 2, the usage of curves over fields whose absolute extension degree (i.e. the extension degree over their prime field) is divisible by 4, 5, 6, 7, 31, 127 is dangerous. If one uses hyperelliptic curves, the same applies if the absolute extension degree is divisible by these numbers or 2 or 3.
- For odd characteristic, the usage of curves over fields whose absolute extension degree is divisible by 4, 5 or 7 is dangerous. If one uses hyperelliptic curves of genus 2, the same applies if the absolute extension degree is divisible by 2, 3, and if one uses hyperelliptic curves of genus 3, the same applies if the absolute extension degree is divisible by 2, 3, 5 or 7. On the other hand, the GHS attack does not pose a threat to the DLP in elliptic curves over fields of odd characteristic whose absolute extension degree is prime and  $\geq 11$ .

## 4 Cover attacks on trace-zero groups

In this section we discuss another construction, developed by the authors, of curves that admit a cover attack.

Let  $H$  be a genus  $g$  hyperelliptic curve defined over  $k$ . Let  $K/k$  be an extension of degree  $n$ , and let  $M(k)$  be the kernel of the norm map  $\text{Cl}^0(H/K) \rightarrow \text{Cl}(H/k)$ ; this is called the *trace-zero* group of  $\text{Cl}^0(H/K)$  (with respect to  $K/k$ ). In certain cases (e.g. if  $n = 3$  and  $g(H) = 1$  or 2, the arithmetic on  $M(k)$  can be implemented more efficiently than the arithmetic in the whole group  $\text{Cl}^0(H/K)$ . On the other hand, if  $\#k$  is small and  $n$  is large (the case of “Koblitz curves”), the difference between the bit-size of  $\#M(k)$  and the bit-size of  $\#\text{Cl}^0(H/K)$  is negligible. In all cases, one can use the Frobenius automorphism to speed up the addition of two points and the multiplication of a point by a scalar. Therefore, these groups

are particularly useful for cryptographic applications. On the other hand, at least for small  $n$ , certain groups of this type are subject to a cover attack.

Let  $\phi : C \rightarrow H$  be a cover defined over  $k$ , and suppose that  $C$  has an automorphism  $\tau$  of order  $n$ , such that  $\phi \circ \tau \neq \phi$ . Let  $C^\tau$  denote the twist of  $C$  over the extension  $K/k$  with respect to  $\tau$ . (Note that  $C/K \simeq C^\tau/K$ .) In [2, Theorem 9] it is made plausible that under some mild condition, one can expect that the kernel of the map

$$M(k) \hookrightarrow \text{Cl}^0(H/K) \xrightarrow{c^*} \text{Cl}^0(C/K) \xrightarrow{N} \text{Cl}^0(C^\tau/k)$$

does not contain the large subgroup of prime order. (The proof involves that there is a canonical non-trivial map from  $\text{Jac}(C^\tau/k)$  to the so-called *trace-zero subvariety* of the Weil restriction of  $\text{Jac}(H/K)$  with respect to  $K/k$ .) If the genus of  $C$  is not much bigger than  $(n-1)g(H)$  then index calculus on  $\text{Cl}^0(C^\tau)$  is more efficient than square-root attacks on  $M(k)$  for solving the discrete logarithm problem.

Here we present a method for finding curves  $C$  in certain situations that make this attack possible. The idea is to find a rational function  $f$  on  $H$  of degree  $n$  whose induced cover  $f : H \rightarrow \mathbb{P}^1$  has suitable ramification. Then one considers the Galois closure  $\phi : C \rightarrow H$  of the cover  $f$ . (By the Galois closure of a cover of curves, we mean a curve associated to the Galois closure of the corresponding function fields.) The Galois group of  $f \circ \phi$  is a subgroup of  $\text{Aut}(C)$ , and its order is a multiple of  $n$ . So for example, if  $n$  is prime, then  $C$  has an automorphism  $\tau$  of order  $n$  which satisfies  $\tau \circ \phi \neq \phi$ , as required.

In order to describe how to find suitable covers  $f : H \rightarrow \mathbb{P}^1$ , we first consider the case that both  $H$  and  $f$  are defined over  $\bar{k}$ , the algebraic closure of  $k$ . Further, we assume that we only have tame ramification. Then the question of what ramification may occur, and what the genus of  $C$  is can be answered by certain group theoretic considerations. Let  $\sigma_1, \dots, \sigma_r$  be  $r$  elements of  $S_n$  that generate a transitive subgroup, such that  $\sigma_1 \dots \sigma_r = 1$ . Let  $\sigma_i$  have cycle lengths  $e_{i,j}$ . Then, by Galois theory, there exists a (connected) cover  $f : H \rightarrow \mathbb{P}^1$  of degree  $n$  with  $r$  ramification points  $P_i$  in  $\mathbb{P}^1$ , and with ramification indices  $e_{i,j}$  above  $P_i$ . The Galois closure  $f \circ \phi : C \rightarrow \mathbb{P}^1$  has Galois group  $\langle \sigma_i | i = 1, \dots, r \rangle$  and ramification indices  $\# \langle e_{i,j} | j \rangle$ . Both the genus of  $H$  and  $C$  are determined by the Hurwitz formula.

This allows one to study whether geometrically, certain good covers  $f : H \rightarrow \mathbb{P}^1$  exist. The next task is then to study the precise fields over which such covers can be defined, and to construct them explicitly.

We now give some examples of (hyper-)elliptic curves which are subject to the attack described here. The most important examples are arguably 4.1. and 4.2. They show that the DLP in the trace-zero group  $M(k)$  of a genus 2 curve with respect to an extension degree 3  $K/k$  (with  $\text{char}(k) \neq 2, 3$ ) can

always be transferred into a DLP of a genus 6 curve  $C/k$ . Moreover, for a very large percentage of such curves, the DLP in  $M(k)$  can even be transferred into a DLP in a hyperelliptic genus 5 curve defined over the ground field  $k$ .

Together with the results of [17] this second result means that a very large percentage of discrete logarithm problems in these trace-zero groups  $M(k)$  of cryptographically relevant size are breakable.

It is interesting to note that there is a certain converse to this statement, namely:

If  $K/k$  is an extension of finite fields of degree 3 and  $H/k$  is a genus 2 curve such that 3 does not divide  $\text{Cl}^0(H/L)$ , where  $L/K$  is the unique extension of degree 2, then via a cover attack, the DLP in the trace-zero group  $M(k)$  can – with a very high probability – only be transferred to DLPs of curves of genus at least 6.

This statement follows from some theory on the trace-zero variety, in particular [10, Theorem 3.3].

#### 4.1 The case $n = 3$ , $g(H) = 2$ , $g(C) = 6$ .

Let  $n = 3$ . Let  $\sigma_1 = (1\ 2\ 3)$ ,  $\sigma_2 = (3\ 2)$ ,  $\sigma_3 = \dots = \sigma_7 = (1\ 2)$ . With these data we have  $g(H) = 2$  and  $g(C) = 6$ . For every curve  $H$  of genus 2 there exists a map with the desired property: one can take a point  $P \in H(k)$ , and take  $f$  in the Riemann-Roch space  $\mathcal{L}(3P) \setminus \mathcal{L}(2P)$ .

#### 4.2 The case $n = 3$ , $g(H) = 2$ , $g(C) = 5$ .

Let  $\sigma_1 = \sigma_4 = (1\ 2\ 3)$ ,  $\sigma_2 = \sigma_5 = (3\ 2)$  and  $\sigma_3 = \sigma_6 = (2\ 1)$ . This yields  $n = 3$ ,  $g(H) = 2$  and  $g(C) = 5$ . Let  $\iota : H \rightarrow H$  denote the hyperelliptic involution. If  $\text{Cl}^0(H/k)$  has a 3-torsion point of the form  $P_1 + P_2 - O - \iota(O)$  with  $P_1$  and  $P_2$  in  $H(k)$ , then  $P_1 - \iota(P_2)$  has order 3 in  $\text{Cl}^0(H)$ , hence there is a function  $f$  with divisor  $3P_1 - 3\iota(P_2)$ . Generically, this  $f$  has the required ramification.

If  $\text{Cl}^0(H/k)$  does not have a 3 torsion point of the above form, but the class group of a quadratic twist of  $H/k$  does, then the above construction can be applied as well. This yields that about one third of the genus 2 curves  $H$  admit a genus 5 cover in this way.

One can construct an explicit family of curves  $H$  for which the covering genus 5 curve  $C$  is hyperelliptic. For this, first construct a degree 3 cover  $\mathbb{P}^1 \rightarrow \mathbb{P}^1$  associated to the ramification data given by  $\sigma_1$ ,  $\sigma_2$  and  $\sigma_3$ . The Galois closure is also a  $\mathbb{P}^1$ . A quadratic base-change ramified outside the ramification points already there yields the Galois cover  $C \rightarrow H \rightarrow \mathbb{P}^1$  with every curve hyperelliptic.

### 4.3 The case $n = 3$ , $g(H) = 2$ , $g(C) = 4$ .

Let  $\sigma_1 = \sigma_2 = \sigma_3 = (1\ 2\ 3)$  and  $\sigma_4 = \sigma_5 = (1\ 2)$ . This yields  $n = 3$ ,  $g(H) = 2$  and  $g(C) = 4$ . One can construct an explicit family of such curves using Kummer theory.

### 4.4 The case $n = 5$ , $g(H) = 1$ , $g(C) = 4$ .

Let  $\sigma_1 = (1\ 2\ 3\ 4\ 5)$ ,  $\sigma_2 = (1\ 2\ 3\ 5\ 4)$  and  $\sigma_3 = (1\ 3)(2\ 4)$ . This yields  $n = 5$ ,  $g(H) = 1$ ,  $g(C) = 4$ . There is only 1 curve in this case, which is defined by the equation  $y^2 = x^3 + 3165x - 31070$ .

### 4.5 The case $n = 7$ , $g(H) = 1$ , $g(C) = 8$ .

Let  $\sigma_1 = (1\ 6)(2\ 5)(3\ 4)$ ,  $\sigma_2 = (1\ 7)(2\ 6)(3\ 5)$ ,  $\sigma_3 = (1\ 2\ 4)(3\ 6\ 5)$  and  $\sigma_4 = (2\ 5\ 3)(4\ 6\ 7)$ . This yields  $n = 7$ ,  $g(H) = 1$ ,  $g(C) = 8$ . One can show that if  $\text{char}(k) \notin \{2, 3\}$  then, geometrically, every elliptic curve  $H$  has a map  $f : H \rightarrow \mathbb{P}^1$  corresponding to this data. So such  $f$  also exists over many finite fields. So far, we only know the existence of  $f$ , but we have no examples with such  $f$  given explicitly.

## 5 The $L$ -Polynomial Approach

In the previous section, we showed that the DLP in class groups  $\text{Cl}^0(H/K)$  of certain curves defined over a field  $k \subsetneq K$  can be attacked via cover attacks. Earlier, we saw that the GHS attack and generalizations provide several explicit constructions of curves  $H/K$  not necessarily defined over  $k$  subject to cover attacks. But the number of curves obtained via these methods is limited, and it is conceivable that there exist other curves that are vulnerable to cover attacks.

In this section we discuss a method developed by the authors to construct, for a given non-trivial field extension  $K/k$ , many hyperelliptic curves  $C$  over  $k$  that admit maps to elliptic curves  $E/K$  (where most of the time,  $E/K$  cannot be defined over  $k$ ); see [1]. The main idea of this construction is that one constructs curves with suitable  $L$ -polynomial. The existence of maps to  $E$  then follows from some theory. Disadvantage of this approach is that although the maps to  $E$  are known to exist, it is not easy to give them explicitly. Work to make these maps explicit is still in progress.

The main theorem is the following

**Theorem 1** *Let  $\ell$  be a prime, and  $q$  a prime power such that  $q^2$  generates*

the squares in  $(\mathbb{Z}/\ell\mathbb{Z})^*$ . Let  $a \in \mathbb{F}_q^*$  and let

$$D_\ell(x, a) := \left( \frac{x + \sqrt{x^2 - 4a}}{2} \right)^\ell + \left( \frac{x - \sqrt{x^2 - 4a}}{2} \right)^\ell$$

be the  $\ell$ -th Dickson polynomial. For  $t \in \mathbb{F}_q$  define the curve  $C_t : y^2 = D_\ell(x, a) + t$  of genus  $n = \frac{1}{2}(\ell - 1)$ . Then for most choices of  $t$  (for all  $t$  for which  $C_t$  is ordinary), the curve  $C_t$  admits a map to an ordinary elliptic curve  $E$  defined over  $\mathbb{F}_{q^n}$ .

As remarked in [1], we believe that this construction can be generalized to a wider class of curves. Instead of using Dickson polynomials one could use the following functions, considered by Mestre in [14]: Let  $E_1$  and  $E_2$  be elliptic curves defined over  $k$ , and let  $\phi : E_1 \rightarrow E_2$  be an isogeny of odd prime degree  $\ell$ . Denote the map induced by  $\phi$  on the  $x$ -coordinates by  $\phi_x$ . So  $\phi_x$  is a rational function of degree  $\ell$ , and the theorem above is likely to be true for the curves  $y^2 = \phi_x(x) + t$  as well.

If one would be able to find maps explicitly, then that would imply the existence of weak curves over  $\mathbb{F}_{q^n}$  where  $q^2$  generates the squares in  $(\mathbb{Z}/(2n+1)\mathbb{Z})^*$ .

Although we do not have explicit maps  $C_t \rightarrow E$ , one can give an upperbound for the minimal degree of such maps. This upperbound follows from a special case of the geometric analogue of the Birch and Swinnerton-Dyer conjecture proved by Milne [15], combined with a classic geometry-of-numbers-argument. Suppose that there exists a non-constant map  $\phi : C_t \rightarrow E$ . Let  $F$  be the  $q^n$ -Frobenius endomorphism on  $E$ , and let  $\Delta$  be the discriminant of the subring  $\mathbb{Z}[F]$  of  $\text{End}(E)$ . Then  $\phi$  can be chosen of degree bounded by  $2n\sqrt{\Delta}$ .

From the Hasse bound, it follows that  $\Delta$  can be expected to be of size of the same order of magnitude as  $q^n$ . It follows that the upperbound on  $\deg \phi$  will be very high in cryptographic applications, and maps with such high degree cannot be written down. But it should be noted this bound is valid for every curve in a certain isogeny class. It is conceivable that for a suitable curve, the actual degree can be much smaller.

Even though this approach has not let to any examples yet of curves that in practice can be attacked, we do recommend not to use elliptic curves  $E$  defined over fields of the form  $\mathbb{F}_{q^{nm}}$ , where  $q$  and  $n$  are small and  $E/\mathbb{F}_{q^{nm}}$  can be defined over  $\mathbb{F}_{q^n}$  provided that  $q$  and  $n$  are numbers such that there exist elliptic curves that are possibly weak to the attack. The problem of finding explicit maps  $C \rightarrow E$  could be very difficult, but it is not well scrutinized.

The recommendation supports the first recommendation in the conclusions of the GHS attack: We thus conclude.

*Be suspicious about curves over composite fields!*

## References

- [1] I. Bouw, C. Diem, and J. Scholten. Ordinary elliptic curves of high rank over  $\overline{\mathbb{F}}_p(x)$  with constant  $j$ -invariant. Preprint.
- [2] C. Diem. A Study on Theoretical and Practical Aspects of Weil-Restrictions of Varieties. Thesis.
- [3] C. Diem. The GHS Attack in odd Characteristic. *J. Ramanujan Math. Soc.*, 18(1):1–32, 2003.
- [4] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta. Arith.*, 102:83–103, 2002.
- [5] S. Galbraith. Weil Descent Of Jacobians. In D. Augot and C. Carlet, editors, *Electronic Notes in Discrete Mathematics*, volume 6. Elsevier Science Publishers, 2001.
- [6] S. Galbraith, F. Hess, and N. Smart. Extending the GHS Weil-Descent Attack. In *Eurocrypt 2002*, LNCS 2332, pages 29–44. Springer-Verlag, New York and Berlin, 2002.
- [7] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology, Eurocrypt 2000*, LNCS 1807, pages 19–34, New York and Berlin, 2000. Springer-Verlag.
- [8] P. Gaudry, F. Hess, and N. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15, 2002.
- [9] F. Hess. The GHS Attack Revisited. In *Eurocrypt 2003*, LNCS 2656, 2003.
- [10] E. Howe. Isogeny classes of abelian varieties with no principal polarizations. In *Moduli of abelian varieties (Texel Island, 1999)*, volume 195 of *Progr. Math.*, pages 203–216. Birkhäuser, Basel, 2001.
- [11] M. Jacobson, A. Menezes, and A. Stein. Solving Elliptic Curve Discrete Logarithm Problems Using Weil Descent. *J. Ramanujan Math. Soc.*, 16, 2001.
- [12] M. Maurer, A. Menezes, and E. Teske. Analysis of the GHS Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree. *LMS Journal of Computation and Mathematics*, 5:127–174, 2002.
- [13] A. Menezes and M. Qu. Analysis of the Weil Descent Attack of Gaudry, Hess and Smart. In *Topics in Cryptology - CT-RSA 2001*, LNCS 2020, pages 308–318. Springer-Verlag, 2001.



- [14] J.-F. Mestre. Familles de courbes hyperelliptiques à multiplications réelles. In *Arithmetic algebraic geometry (Texel, 1989)*, volume 89 of *Progr. Math.*, pages 193–208. Birkhäuser Boston, Boston, MA, 1991.
- [15] J. S. Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.
- [16] H. Stichtenoth. *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin, 1993.
- [17] N. Thériault. Index Calculus attack for hyperelliptic curves of small genus. Preprint.
- [18] N. Thériault. Weil descent attack for Kummer extensions. Preprint.
- [19] N. Thériault. Weil descent attack for Artin-Schreier curves. Preprint.