A CRYPTOGRAPHIC APPLICATION OF WEIL DESCENT

S.D. GALBRAITH AND N.P. SMART

ABSTRACT. This paper gives some details about how Weil descent can be used to solve the discrete logarithm problem on elliptic curves which are defined over finite fields of small characteristic. The original ideas were first introduced into cryptography by Frey. We discuss whether these ideas are a threat to existing public key systems based on elliptic curves.

1. INTRODUCTION

Frey [4] introduced the cryptographic community to the notion of "Weil descent", which applies to elliptic curves defined over finite fields of the form $\mathbb{F}_{q^n}$ with $n > 1$. This paper gives further details on how these ideas might be applied to give an attack on the elliptic curve discrete logarithm problem. We also discuss which curves are most likely to be vulnerable to such an attack.

The basic strategy consists of the following four stages (which will be explained in detail in the remainder of the paper).

1. Construct the Weil restriction of scalars, A, of $E(\mathbb{F}_{q^n})$.
2. Find a curve, C, defined over $\mathbb{F}_q$ which lies on A.
3. Pull the discrete logarithm problem back from $E(\mathbb{F}_{q^n})$ to $Jac(C)(\mathbb{F}_q)$.
4. Solve the discrete logarithm problem on $Jac(C)(\mathbb{F}_q)$ using an index calculus method, based on the Hafner-McCurley algorithm.

We must emphasize that this paper does not represent a fully developed attack on the elliptic curve discrete logarithm problem. In fact the method described here is rather akin to the Xedni calculus explained by Silverman, see [18] and [10], for curves over large prime fields of odd characteristic, since although the method is available in theory in practice it is unlikely to ever be made to work, in the authors opinion, for curves of cryptographic interest.

In the first sections we give some details about abelian varieties, curves and the "Weil restriction" (which is an abelian variety). We also provide more details about the first 3 stages above. The ideas in these sections are well-known in algebraic geometry, but they are not well understood among the cryptographic community.

In Sections 4 we describe solutions to some of the underlying problems that the method presents. In Section 5 we give a down to earth explanation of the whole approach with a very simple example. In this example we construct the Weil restriction over $\mathbb{F}_{2^{n_1}}$ of an elliptic curve E over $\mathbb{F}_{2^{4n_1}}$.

In Section 6 we describe how the discrete logarithm problem in the divisor class group of a curve can be solved in heuristic sub-exponential time relative to the genus of the curve.

1991 *Mathematics Subject Classification.* Primary: 94A60, 11T71, Secondary: 11Y99, 14H52, 14Q15.

Key words and phrases. function fields, divisor class group, cryptography, elliptic curves.

In the final section we discuss some open problems and give an argument of why we do not expect most elliptic curves to be vulnerable to a Weil descent attack. In particular we will explain why we believe composite values of n may be weaker than prime values, thus possibly explaining the choice of some standards bodies in precluding composite values of n.

2. Curves, Divisor Class Groups and Jacobians

We gather a few relevant facts from algebraic geometry. The main references we use are Hartshorne [7], Mumford [15] and Milne [12].

A *curve* C over a field k is a complete, non-singular variety of dimension 1 over k. We often deal with curves which are given as a specific affine model, which can cause problems. For instance in this setting the curves are often singular, but we will nevertheless still call them curves. The usual approach for handling singularities on a curve, C/k, is to take a sequence of blow-ups, to produce a non-singular curve. This process may involve enlarging the ground field k. Nevertheless, for any C there is a non-singular curve, C', called the normalisation (see [7], Ex. II.3.8), which is defined over the same field k, and a degree one rational map $C' \to C$.

The *genus* g of a non-singular curve is an important invariant of the curve. For a singular curve one may define the *geometric genus* (see [7], Section II.8), which is a birational invariant, as the genus of the normalisation of the curve.

The Jacobian variety $Jac(C)$ of a non-singular curve C of genus g, over a field k, is an abelian variety over k of dimension g. One construction of the Jacobian is as a subset of the gth symmetric power, $C^{(g)}$, of the curve (see [12]). We gather two important facts about the Jacobian of a curve.

Proposition 1. *Suppose C is a non-singular curve over a field k with a point P defined over k. The following properties hold.*

1. *(Canonical map from C into $Jac(C)$) There is a canonical map $f^P : C \to Jac(C)$ which takes the point P to the identity element of $Jac(C)$.*
2. *(Universal property) Suppose A is an abelian variety over k and suppose there is some mapping of varieties $\phi : C \to A$ such that $\phi(P) = 0_A$, then there is a unique homomorphism $\psi : Jac(C) \to A$ such that $\phi = \psi \circ f^P$.*

The divisor class group $Pic^0_k(C)$ of a curve is the group of degree zero divisors on C, which are defined over k, modulo principal divisors. If C is a non-singular curve over k with a k-point, P, then $Jac(C)$ and $Pic^0_k(C)$ are isomorphic as abelian varieties (see [12], Theorem 7.6). It is convenient to view prime divisors on the normalisation as places of the function field. Since the function field of a singular curve is isomorphic to the function field of its normalisation it follows that we can define the divisor class group of a singular curve C and that it will be isomorphic to the divisor class group of its normalisation.

An abelian variety A over k is *simple* if it has no proper abelian sub-varieties defined over k. An abelian variety is *absolutely simple* if, even when considered over the algebraic closure $\bar{k}$, it is simple. An *isogeny* is a mapping of abelian varieties and so is, in particular, a group homomorphism with finite kernel.

We require the following result.

Proposition 2 (see [15], page 173, Theorem 1)**.** *Let A be an abelian variety over a field k and let B be an abelian subvariety of A. Then there is an abelian subvariety C of A such that A is isogenous to the product $B \times C$.*

A corollary of this statement is the fact that every abelian variety is isogenous to a product of simple abelian varieties in a unique way (up to ordering).

We now give an application of this property (also see [12], p. 199). Suppose that A is a *simple* abelian variety of dimension d and that we are given a curve C and a map $\phi : C \to A$ (in this paper the maps maps ϕ we will consider will usually have degree one and we will use the phrase "C lies on A" to represent this situation). Since the image of the map $\psi : Jac(C) \to A$ is an abelian subvariety of A it follows from the fact that A is simple that the map ψ is surjective and that A is an abelian subvariety of $Jac(C)$. In other words, one has the following result.

Corollary 3. *Let A be a simple abelian variety of dimension d over field k. Suppose we have a map $\phi : C \to A$ from a non-singular curve C to A. Then the genus of C is at least d. Furthermore, $g(C) = d$ if and only if A is isogenous to the Jacobian of C.*

3. Weil Descent

Let k denote a finite field and K denote a Galois extension of degree n. For example, we could have $k = \mathbb{F}_2$ and $K = \mathbb{F}_{2^n}$ or $k = \mathbb{F}_{2^{n_1}}$ and $K = \mathbb{F}_{2^m}$ with $m = n_1 n$, which are the two most important cases for the applications. Let $E(K)$ denote some elliptic curve over K, we assume we wish to solve a discrete logarithm problem in $E(K)$ given by

$$P_2 = [\lambda]P_1, \text{ with } P_1, P_2 \in E(K).$$

We include the case where E is defined over k in our discussion, this is the case of Koblitz curves. Koblitz curves are used in real life situations since they produce efficient cryptographic systems.

The "Weil restriction of scalars" of E over K is an abelian variety $W_{K/k}(E)$ of dimension n over the smaller field k.

The proof that such an object exists is fairly deep. Nevertheless, we can easily show how $W_{K/k}(E)$ can be constructed in our case (a specific example will be given later). First take a basis of K over k and expand the coordinate functions on the affine curve $E(K)$ in terms of the new basis, thus using $2n$ variables over k. Expanding out the formulae for the elliptic curve $E(K)$ and equating coefficients of the basis of K over k, we obtain n equations linking our $2n$ variables. This affine variety defines $W_{K/k}(E)$ and the group law is induced from the group law on the elliptic curve.

The following result is stated in [4];

Lemma 4. *If E is defined over k then*

$$W_{K/k}(E) \cong E(k) \times V$$

where V is an abelian variety of dimension $n-1$. If n is coprime to $\#E(k)$ then we have,

$$V = \{P \in W_{K/k}(E) : Tr_{K/k}(P) = \mathcal{O}\}$$

where the trace is computed using the mapping from $W_{K/k}(E)$ to $E(K)$.

Proof. If E is defined over k then it is clearly an abelian subvariety of $W_{K/k}(E)$. By Proposition 2 it follows that there is an abelian subvariety B over k such that $W_{K/k}(E)$ is isogenous to $E \times B$.

The construction of the Weil restriction implies that a generic point of $W_{K/k}(E)$ is $(\eta, \sigma(\eta), \ldots, \sigma^{n-1}(\eta))$ where η is a generic point of E/K. It follows that the subvariety V of $W_{K/k}(E)$ has codimension 1.

Finally, one sees that V is an abelian subvariety of $W_{K/k}(E)$ and, since n is co-prime to $\#E(k)$, the subvariety $V(k)$ has trivial intersection with $E(k)$. Therefore, V is isogenous to B. $\square$

We let A denote the 'interesting' abelian variety, defined over k, on which the discrete logarithm problem on $E(K)$ actually lies. In other words

Definition 1. *Define A by*

- *If E is not defined over k, then set $A = W_{K/k}(E)$. Hence $\dim A = n$.*
- *If E is defined over k, then set $A = V$, from Lemma 4. Hence $\dim A = n - 1$.*

In general we expect the abelian variety A to be simple. Indeed, since the original elliptic curve will have order divisible by a large prime, it is clear by considering the number of points on A that there must be a large simple abelian subvariety of A.

We may now give a sketch of the "Weil descent" attack on the elliptic curve discrete logarithm problem: Given an elliptic curve E over K construct the abelian variety A over k as above. Next find a (possibly singular) curve C defined over k lying on A such that C has a k-point P_0 at the point at infinity of A. By the universal property of Jacobians there is a mapping of abelian varieties $\psi : Jac(C') \to A$, where C' is the normalisation of C.

The points P_1 and P_2 of the discrete logarithm problem in $E(K)$ correspond to points on $A(k)$ in an obvious way, and these points may be pulled-back under ψ to obtain divisors D_1 and D_2 in $Pic_k^0(C)(k)$ (whose support is only on the non-singular points of C) such that $\psi(D_i) = P_i$. Finally, the discrete logarithm problem of D_2 with respect to D_1 on $Pic_k^0(C)$ can be solved using an index calculus method.

There are three main problems which must be overcome in order to apply this method.

1. It is necessary to find curves of small genus on A.
2. It is necessary to pull back points on A to divisors on C.
3. It is necessary to have an index calculus method for general divisor class groups.

The main contribution of this paper is to provide solutions to the latter two of these problems. The first problem is the very significant and we discuss it further at the end of the paper.

4. Pulling Back Along ψ

We shall need to describe the mapping ψ more explicitly. Let C be a curve of genus g over k and let $\phi : C \to A$ be the mapping of C into the abelian variety A. Suppose P_0 is the k-point on C (which we shall assume lies at infinity) which maps under $f = f^{P_0}$ to the identity element of A. Recall that elements of $Pic_k^0(C)$ may be represented in the form $D = E - d(P_0)$ where $E = \sum_{i=1}^{d} (Q_i)$ is an effective divisor of degree d and where the Q_i are points on $C(\bar{k})$ such that, as a divisor, E is defined over k. Note that one usually restricts to $d \leq g$ but the process described below works for arbitrary values of d.

Proposition 5. *The map $\psi : Pic_k^0(C) \to A(k)$ is given by*

$$\psi(E - d(P_0)) = \sum_{i=1}^{d} \phi(Q_i)$$

where the addition on the right hand side is addition on the abelian variety A (which can be efficiently computed via the addition law on $E(K)$).

Proof. The divisor $E - d(P_0)$ is equal to the sum (on $Pic_k^0(C)$) of the divisors $(Q_i) - (P_0)$. The canonical map $f : C(\bar{k}) \to Pic_{\bar{k}}^0(C)$ has the property that $f(Q_i) = (Q_i) - (P_0)$. The mapping $\psi : Pic_k^0(C) \to A$ has the universal property that $\phi = \psi \circ f$ and so $\psi((Q_i) - (P_0)) = \phi(Q_i) \in A(k)$. Since ψ is a group homomorphism which preserves the action of the Galois group $Gal(\bar{k}/k)$ the result follows. □

In practice we will be using a singular equation for the curve C. The mapping above still gives a complete description of the map from $\mathrm{Pic}_k^0(C)$ to A for the divisors whose support lies on the non-singular points of C.

To invert the map ψ we have to find a divisor which maps under ψ to a given point, P, of A. We now describe how to find such a divisor.

We will find p non-singular points on $C(k)$, where p is to be determined later. Call these $\{P_1, \ldots, P_p\}$ and map them to the variety A via the map ϕ, to obtain

$$Q_i = \phi(P_i),\ i = 1, \ldots, p.$$

Thinking of the coordinates of the points as variables, we see that we obtain p equations in $2p$ unknowns. Formally using the group law on A applied to these points Q_i we determine the equations for the coordinates of the sum

$$\sum_{i=1}^{p} Q_i$$

and then equate this to the given element P. Since A has dimension n this gives us, roughly, another n equations.

Hence in total we have $p + n$ equations in $2p$ unknowns, which defines a variety V. So as soon as $p > n$ we expect that this defines a variety of dimension at least $p - n$. For example, a curve when $p = n + 1$ and a surface when $p = n + 2$. Finding a point on this variety will produce the points P_i and in general these will be non-singular points on C.

Finding points on varieties in high-dimensional spaces is not a computationally trivial matter. There may also be computational issues which arise when constructing this variety. Nevertheless, we do not think that these would be the main obstacle to the success of our method, since finding a suitable curve, C, on A is more likely to provide an obstacle to the practicality of our method.

We construct the divisors $D_i = (Q_i) - (P_0)$, in $Pic_k^0(C)$, and then

$$\psi(\sum_{i=1}^{p} D_i) = P,$$

as required. A different point on the variety V will give rise to different divisors D_i.

Suppose now that we have found two divisors, D_1' and D_2', in $\mathrm{Pic}_k^0(C)$ such that $\psi(D_1') = P_1$ and $\psi(D_2') = P_2$ Let g denote the genus of C and let q denote the size of the field k. We let $h = \#\mathrm{Pic}^0_k(C)$ then by the Weil conjectures we know that

$$(1-\sqrt{q})^{2g} \le h = \left|\prod_{i=1}^{2g}(1-\omega_i)\right| \le (1+\sqrt{q})^{2g}.$$

For the moment suppose we have determined h. This number can be computed in polynomial time using the algorithm due to Pila [17] (also see [2] and [9]). The fact that we know that h is divisible by $\#E(K)$ gives us some extra information about h. In any case the value of h will come out in the wash of the method described in Section 6. We shall make the reasonable assumption that $(\#E(K))^2$ does not divide h.

We compute $D_i = [h/\#E(K)]D_i'$ in $\mathrm{Pic}^0_k(C)$, and attempt to solve the discrete logarithm problem

$$D_2 = [\lambda]D_1$$

for the unknown discrete logarithm λ, in the group $\mathrm{Pic}^0_k(C)$. This is then the solution to the original discrete logarithm problem on $E(K)$.

5. An Example

We give an example to illustrate some of the ideas described above. Let $k = \mathbb{F}_{2^{n_1}}$ and let K be such that K has a Type-1 Optimal Normal Basis over k. This means that $n+1$ should be a prime and that 2^{n_1} should be primitive in the finite field $\mathbb{F}_{n+1}$. Then the n roots of

$$(x^{n+1}-1)/(x-1) = x^n + x^{n-1} + \cdots + x + 1$$

form an Optimal Normal Basis of K over k.

As an example we take a field with $n = 4$, for simplicity. Let $\{\theta, \theta^2, \theta^4, \theta^8\}$ denote the Optimal Normal Basis of K over k, so we have $\theta^4+\theta^3+\theta^2+\theta+1 = 0$ and the element $1 \in K$ is given, in terms of the basis, by $1 = \theta+\theta^2+\theta^4+\theta^8$. Consider the following elliptic curve defined over K,

$$Y^2 + XY = X^3 + b \tag{1}$$

where $b \neq 0$ and b is given by

$$b = b_0\theta + b_1\theta^2 + b_2\theta^4 + b_3\theta^8.$$

By setting

$$\begin{aligned} X &= x_0\theta + x_1\theta^2 + x_2\theta^4 + x_3\theta^8, \\ Y &= y_0\theta + y_1\theta^2 + y_2\theta^4 + y_3\theta^8, \end{aligned}$$

where $x_i, y_i \in k$, substituting into (1) and equating powers of θ we obtain four equations in the eight unknowns, $\{x_0, \ldots, x_3, y_0, \ldots, y_3\}$. This defines the abelian variety A as a 4-dimensional variety in 8-dimensional affine space. Note that if one tries to construct a projective equation for A in the obvious manner then there are too many points at infinity. For the application we must remember that there is some projective equation for A which only has one point which does not lie on our affine equation.

The group law on A can be evaluated by translating a point

$$(x_0, x_1, x_2, x_3, y_0, y_1, y_2, y_3) \in A(k)$$

back to the point

$$(x_0\theta + x_1\theta^2 + x_2\theta^4 + x_3\theta^8, y_0\theta + y_1\theta^2 + y_2\theta^4 + y_3\theta^8) \in E(K)$$

and then using the addition formulae on the elliptic curve.

If we intersect A with $(\dim A)-1$ hyperplanes, in general position, which all pass through the zero element of A, then we should end up with a variety of dimension one. By using elimination theory we can then write down the equation of this variety.

In our example we have $\dim A = 4$, and the obvious hyperplanes to choose, given that we want the degree of the resulting curve to be small, are

$$x_0 = x_1 = x_2 = x_3.$$

Intersecting these with our variety A, we obtain the variety

$$V : \begin{cases} y_3^2 + y_0 x_0 + x_0^3 + b_0 = 0, \\ y_0^2 + y_1 x_0 + x_0^3 + b_1 = 0, \\ y_1^2 + y_2 x_0 + x_0^3 + b_2 = 0, \\ y_2^2 + y_3 x_0 + x_0^3 + b_3 = 0. \end{cases}$$

If we then eliminate y_3 by taking the resultant of the first and fourth of these equations, and eliminate y_1 by taking the resultant of the second and third, then we obtain the variety:

$$V' : \begin{cases} y_2^4 + x_0^6 + b_3^2 + y_0 x_0^3 + x_0^5 + b_0 x_0^2 = 0, \\ y_0^4 + x_0^6 + b_1^2 + y_2 x_0^3 + x_0^5 + b_2 x_0^2 = 0. \end{cases}$$

Finally by eliminating y_2 from these two equations and setting $x = x_0$ and $y = y_0$ we obtain the affine curve

$$C : y^{16} + x^{15} y + (x^{24} + x^{20} + x^{18} + x^{17} + b_0 x^{14} + b_3^2 x^{12} + b_2^4 x^8 + b_1^8).$$

The only singular point on this affine model is the point at $(x, y) = (0, 0)$. There is also a singularity at the point at infinity, above which there will be several points and one of these will correspond to the unique point at infinity on the variety A. The other points will correspond to points on the affine part of A.

To get a feel for this curve, take $k = \mathbb{F}_2$, this is far too small for real examples but it allows us to compute some invariants. We computed the genus, g, for this curve for all the possible values of the b_i, using the KANT package [3]. For the following values of the b_i, which represent exactly half of all possible values, we found that the genus was equal to 8

$$(b_0, b_1, b_2, b_3) = \begin{cases} (0,0,0,1), & (0,0,1,0), & (0,1,0,0), & (0,1,1,1), \\ (1,0,0,0), & (1,0,1,1), & (1,1,0,1), & (1,1,1,0). \end{cases}$$

In addition the unit rank was always 3 and the ramification at infinity was wild. The value of $(0,0,0,0)$ is precluded since the original elliptic curve must be non-singular. The other values of (b_0, b_1, b_2, b_3) produce curves which are reducible. As an example, consider $(b_0, b_1, b_2, b_3) = (0,0,1,1)$, in this case we obtain an irreducible factor given by the curve

$$C_1 : y^8 + x^4 y^4 + x^6 y^2 + x^7 y + x^{12} + x^9 + x^4 = 0.$$

This curve has genus 4, unit rank two and again the place at infinity is wildly ramified. Notice that since C_1 has genus four and the dimension of A is four, the Jacobian of the normalisation of C_1 must be isogenous to A.

6. Solving The Discrete Logarithm Problem in the Divisor Class Group of Certain Curves

Let k be a finite field of q elements and let $C(x,y) \in k[x,y]$ denote some irreducible multinomial such that

- $\deg_y C = N$.
- C is monic and separable in y.
- There is a k-rational point, P_0, on C at infinity.

We think of $C(x,y)$ as determining a curve in $\mathbb{P}^2_k$, which is possibly singular.

We let $F = k(x)[y]/(C)$ denote the function field of $C(x,y)$. The place at infinity, ∞, of $k(x)$ decomposes in F in the form

$$\infty = \prod_{i=1}^{s} \infty_i^{e_i},$$

with ∞_i having inertia degree f_i. For later use we set $e = \operatorname{lcm}(e_1, \ldots, e_s)$ and, by our third assumption above, we have $f = \gcd(f_1, \ldots, f_s) = 1$.

Let $\mathcal{O}_F$ denote the integral closure of $k[x]$ in F and let Cl denote the ideal class group of $\mathcal{O}_F$ and Ker denote the subgroup of $\operatorname{Pic}^0_k(C)$ generated by the divisor classes of all the degree zero divisors with support only at infinity. Since $f = 1$ we obtain the isomorphism

$$\operatorname{Pic}^0_k(C) \cong Cl \otimes \operatorname{Ker},$$

where an ideal $\mathfrak{a} \in Cl$ corresponds to the degree zero divisor class

$$D_{\mathfrak{a}} - (\deg \mathfrak{a}) P_0,$$

where $D_{\mathfrak{a}}$ is the effective divisor associated to $\mathfrak{a}$ in the obvious manner.

In this section we shall prove

Theorem 6. *If D_1 and D_2 are elements of $\operatorname{Pic}^0_k(C)$ such that $D_2 = [m]D_1$ then we can find m, i.e. solve the discrete logarithm problem in $\operatorname{Pic}^0_k(C)$, in heuristic expected running time*

$$O\left(N \cdot L_{e^g}(1/2, 3.54\sqrt{\log q})\right),$$

as $g \to \infty$.

Crucial to our algorithm is the following theorem which guarantees that the factor base we eventually choose will generate the whole of $\operatorname{Pic}^0_k(C)$.

Theorem 7. *The group $\operatorname{Pic}^0_k(C)$ is generated, under the isomorphism above, by the group Ker and the prime ideals $\mathfrak{B}$ lying above primes $\mathfrak{p} \in k[x]$ with*

$$f_{\mathfrak{B}} \deg \mathfrak{p} \leq \left\lceil \frac{2\log(4g-2)}{\log q} \right\rceil$$

where $f_{\mathfrak{B}}$ is the inertia degree of $\mathfrak{B}$ and g is the genus of K.

Proof. The proof of the analogous result in [14] extends to our more general situation. $\square$

We set

$$\beta = \left\lceil \left(\frac{g \log g}{2 \log q}\right)^{1/2} \right\rceil$$

and let S_f denote the set of places (i.e. prime ideals), $\mathfrak{B}$, lying above a prime $\mathfrak{p} \in k[x]$ such that

$$\deg \mathfrak{p} \leq \beta.$$

Since for all $\mathfrak{B}$ we have $f_{\mathfrak{B}} \geq 1$, we can, for sufficiently large values of g, assume that the set of such ideals, S_f, along with the group Ker, generate the group $\mathrm{Pic}_k^0(C)$ under the above isomorphism.

For each irreducible polynomial $\mathfrak{p} \in k[x]$ there are at most N finite places lying above $\mathfrak{p}$. Letting $N_q(i)$ denoting the number of monic irreducible polynomials in $k[x]$ of degree less than or equal to β, we obtain

$$\#S_f \leq N \sum_{i=0}^{\beta} N_q(i) \leq N \sum_{i=0}^{\beta} \frac{q^i - q}{i} = O\left(\frac{N}{\beta} q^{\beta}\right).$$

Let S_∞ denote the set of places above ∞ and set $S = S_f \cup S_\infty$. The set of S-units of F, i.e. the functions whose support lies solely on S, is denoted by $\mathcal{O}_S^*$. Setting $t = \#S$ and letting $S^* = S \backslash \{\mathfrak{B}_\infty\}$, for some fixed place $\mathfrak{B}_\infty \in S_\infty$ (e.g., $\mathfrak{B}_\infty = P_0$), we consider the map

$$\Phi : \left\{ \begin{array}{ccc} \mathcal{O}_S^* & \longrightarrow & \mathbb{Z}^{t-1} \\ f & \longmapsto & (f_{\mathfrak{B}} v_{\mathfrak{B}}(f) \deg \mathfrak{p}))_{\mathfrak{B} \in S^*} \end{array} \right. ,$$

where $v_{\mathfrak{B}}$ denotes the valuation function at the place $\mathfrak{B}$. It is easy to see that the image of Φ is a lattice $\Lambda \in \mathbb{Z}^{t-1}$ isomorphic to $\mathrm{Pic}_k^0(C)$ and with determinant

$$\det(\Lambda) = \frac{\#\mathrm{Pic}_k^0(C)}{\prod_{\mathfrak{B} \in S}(f_{\mathfrak{B}} \deg \mathfrak{p})}.$$

6.1. **Smoothing a divisor.** For our purposes a divisor will be called *smooth* if its support lies wholly on the set S. In this section let D denote some given divisor of degree zero which represents some class in $\mathrm{Pic}_k^0(C)$. We wish to construct a divisor D' and a function γ such that $\mathrm{Supp}(D') \subset S$ and $D' = D + \mathrm{div}(\gamma)$.

The basic idea is to add to D a random sum, R, of divisors of degree zero with support in S, so $D_1 = D + R$. We then 'reduce' the resulting divisor to obtain a divisor, D_2, and a function, γ, such that $D_2 = D + R + \mathrm{div}(\gamma)$. If we are 'lucky' then the support of D_2 will lie in S and we will have obtained the required smooth divisor $D_2 - R \sim D$. If we are not lucky then we need to take another random sum, R.

To detect whether D_2 has support on S we can ignore the infinite component and concentrate on the finite part. Determining the support is then simply a matter of polynomial factorization over finite fields which can be performed in probabilistic polynomial time.

All that we need now do is explain the method of reduction, and how this effects the degree of the resulting ideal which corresponds to D_2.

Under our assumption on the existence of a point P_0 at infinity, the Riemann-Roch theorem then tells us that every element of $\mathrm{Pic}_k^0(C)$ is represented by a divisor of the form

$$E - g(P_0),$$

where E is an effective divisor of degree g. Hence, by using an efficient effective Riemann-Roch algorithm (see for instance, [8] or [19]) the divisor D_2 can be made to have the form $D_2 = E - g(P_0)$ where $\deg E = g$. The divisor D_2 is therefore smooth if the polynomial in $k[x]$ of degree at most g, corresponding to the finite part of E factors into a product of irreducibles all with degree less than or equal to β.

If $q \geq (g \log^2 g)^{1/\beta}$ and $\beta < g$ then the probability of obtaining a factorization over the factor base in one iteration of our smoothing algorithm is given by (see [11])

$$Pr_{\beta,g} = \left(\frac{\beta}{g}\right)^{(1+o(1))(g/\beta)}$$

as $\beta \to \infty$ and $g/\beta \to \infty$. Since this is the probability that a polynomial of degree g, defined over k, has all its factors of degree less than or equal to β.

6.2. **Generating the lattice of relations.** We shall describe a method of solving the discrete logarithm problem which is a variant of the Hafner-McCurley method used in quadratic number (and function) fields, see [6] and [16]. The analogous method based on the NFS/FFS can be deduced in an analogous way by extending the work of [1] and [5]. In practice the NFS/FFS style method may be more efficient since one can perform sieving with this method (whilst it is hard to see how to do this with the Hafner-McCurley based variant). However it is simpler to analyze the Hafner-McCurley based variant which we shall now describe.

We repeat the following steps until we obtain a lattice of full rank whose determinant does not decrease upon running the following algorithm a few more times. Indeed at this point we can use any partial information we have from our discussion in Section 3 on the group order of $\mathrm{Pic}_k^0(C)$. This will give us an even stricter stopping criteria and will determine the size of $\mathrm{Pic}_k^0(C)$ as a by product.

1. We apply our smoothing algorithm to the trivial divisor $D = 0$ to obtain a function γ and a divisor D such that $\gamma = \mathrm{div}(D)$ and $\mathrm{Supp}(D) \subset S$.
2. Note $\gamma \in \mathcal{O}_S^*$ so we can compute the image of γ under Φ and so obtain an element of the lattice Λ. The valuations of γ at infinity can be easily computed in the case of tame ramification at infinity, i.e when e is coprime to the characteristic of k, via Puiseux expansions. For the non-tame case Hamburger-Noether expansions need to be used.

We expect to require just over $\#S$ elements of the lattice until we obtain a lattice of full rank, hence we expect to need to take in total around T random power products in the smoothing algorithm before we are finished, where

$$T = \frac{N \cdot q^\beta}{\beta Pr_{\beta,g}} = \frac{N}{\beta} q^\beta \left(\frac{g}{\beta}\right)^{(1+o(1))(g/\beta)}.$$

We notice that

$$\frac{g}{\beta} \approx \left(\frac{g}{2 \log q \log g}\right)^{1/2},$$

and so we deduce that

$$\begin{aligned}
\log T &= \log N - \log \beta + \beta \log q + (1+o(1)) \left(\frac{g}{\beta}\right) \log \left(\frac{g}{\beta}\right) \\
&\approx \log N + \left(\frac{g \log g}{2 \log q}\right)^{1/2} + (1+o(1)) \left(\frac{2g \log q}{\log g}\right)^{1/2} \left(\frac{1}{2} \log g\right) \\
&\approx \log N + (g \log g)^{1/2} \left(\sqrt{2 \log q} + o(1)\right).
\end{aligned}$$

Hence the time needed to compute a full lattice of relations Λ is

$$\approx O\left(N \cdot L_{e^g}(1/2, \sqrt{2\log q} + o(1))\right).$$

We store each computed lattice vector as a column in a matrix A. Hence, at the end of the algorithm, we hope that we have

$$\Lambda = \{A\mathbf{x} : \mathbf{x} \in \mathbb{Z}^c\}$$

where c is the column dimension of A.

We need to then compute the Hermite Normal Form of A, to obtain a matrix H which spans the same lattice as A but which is in upper triangular form. This can essentially be done in time, [13],

$$O\left(cr^2(r^2+c)\log^2(r|A|)\right)$$

where $|A| = \max_{i,j} |a_{i,j}|$, and r is the row dimension of A, which we assume to be also equal to the rank of A. Since we are using the Hafner-McCurley method we cannot assume that our matrix will be sparse. And as we have

$$c \approx r = (\#S - 1) \approx O(\frac{N}{\beta} q^\beta),$$

the time needed to perform the matrix step is,

$$O\left(q^{5\beta}\right) = \left(L_{e^g}(1/2, 5\left(\frac{\log q}{2}\right)^{1/2})\right).$$

6.3. **Computing Individual Logarithms.** Given the one-off cost of computing the matrix H above we can then solve any discrete logarithm problem in $\mathrm{Pic}_k^0(C)$ with relative ease. We are given $D_1, D_2 \in \mathrm{Pic}_k^0(C)$ and we wish to find the integer m such that

$$D_2 = [m]D_1.$$

For $i = 1$ and 2 we use our smoothing method to obtain a function γ_i such that $D_i - \mathrm{div}(\gamma_i)$ is a divisor with support only on S. Hence in $\mathrm{Pic}_k^0(C)$ we can write

$$D_i \equiv \sum_{\mathfrak{B}_j \in S} d_j \mathfrak{B}_j.$$

We then set $\mathbf{d}_i = (d_j)_{\mathfrak{B}_j \in S^*}$ and compute the matrix

$$B = \begin{pmatrix} -1 & 0 & \mathbf{0}^t \\ 0 & -1 & \mathbf{0}^t \\ \mathbf{d}_1 & \mathbf{d}_2 & H \end{pmatrix}$$

Using an analogue of the Hermite Normal Form algorithm we determine a matrix C, and hence a unimodular matrix V such that

$$C = BV = \begin{pmatrix} z & x & * \\ 0 & y & * \\ \mathbf{0} & \mathbf{0} & * \end{pmatrix}.$$

We then know that D_1 has order dividing z in the group $\mathrm{Pic}_k^0(C)$. Indeed we expect that z is the order of D_1 in $\mathrm{Pic}_k^0(C)$, and in practice we can assume that z is a large prime number. We also deduce from the matrix C that

$$[x]D_1 + [y]D_2 \equiv 0.$$

But we know $D_2 = [m]D_1$ and so

$$[x + ym]D_1 \equiv 0.$$

So we obtain the linear congruence for m,

$$m = -x/y \pmod{z}.$$

Therefore, we can determine a unique solution for m if $\gcd(y, z) = 1$. Since in practice we can assume that z is a large prime, we will obtain m unless z divides y. But this can only happen if either the matrix A of the earlier section does not generate the full lattice or the group $\mathrm{Pic}_0^k(C)$ has order divisible by z^2.

It is reasonable to assume that neither z^2 divides $\#\mathrm{Pic}_0^k(C)$ nor that A generates a sublattice, hence we conclude that we have determined the unique solution to our discrete logarithm problem.

6.4. **Discussion.** We believe that the above algorithm can be proved rigorously to have sub-exponential behaviour using the standard techniques applied to the Hafner-McCurley algorithm. We do not do this here since such a result has only theoretical interest, the existence of a heuristic proof is enough for the purposes of this article.

7. Open Problems and Conclusion

In this paper we have outlined a strategy for solving the elliptic curve discrete logarithm problem and have given some details about each of the main steps in this process. We now address the issue of whether such a strategy is a threat to the elliptic curve cryptosystems used in practice.

One important observation is that everything in this paper only applies to the case of elliptic curves over fields of the form $\mathbb{F}_{p^n}$ with $n > 1$. Elliptic curves over prime fields are totally immune to these ideas.

The method can be broken down into 4 main stages (see the Introduction). Stage 1 (computing an affine equation for the Weil restriction) causes no practical problems.

The actual solution of the discrete logarithm comes from Stage 4, where the index calculus algorithm described in Section 6 is applied. The motivating problem is to solve a discrete logarithm problem on an elliptic curve which has approximately q^n points, but we do this by solving a related discrete logarithm problem in a group of size q^g, where g is the genus of the curve C.

If g is very large compared to n then the discrete logarithm problem has been buried in a much larger group and so the method is not useful. For the Weil descent to be a danger it is therefore necessary that the genus, g, not grow too large in relation to the original degree, n. On the other hand, the index calculus method is subexponential only asymptotically (i.e., when the field size is fixed at q and when the value of g is "sufficiently large"). Therefore, for the Weil descent attack to work, the values of n and g must strike a balance between these conflicting forces.

For Stage 2 it is necessary to find a curve lying on the abelian variety A. As we have seen, it is important for Stage 4 that the genus g of C be large, but not too large compared with n. The method used in our example to find such a curve involves eliminating variables. This leads to a curve whose degree is exponential in n (and so we expect the genus to also be exponential as long as C is not too singular). If the genus of C grows exponentially with n then the complexity of the Weil descent attack would be subexponential in q^g but this is exponential in terms of the elliptic curve group size q^n.

It is not known to the authors what values might be expected for the smallest possible genus for a curve C on such an A. This question is equivalent to asking about the expected dimension for a Jacobian with a given abelian variety as a factor. It is therefore an interesting problem to determine if there is a curve C of genus $O(n^d)$ on any such A for some fixed d. If such curves exist then it would be very interesting to have a method for obtaining equations for them in terms of the variables describing the variety A. When n is small there is a higher chance that there will be small genus curves lying on the abelian variety A (this was seen in our example, when half the time A was actually a Jacobian). When n is large it seems to be very unlikely that A have curves on it of genus close to n and so it is unlikely that the Weil descent method would give a practical attack.

For Stage 3 it is necessary to find a point on a large dimensional variety over a small finite field. When n is small then this problem is not difficult to solve. It is not known to the authors how difficult this is to achieve when n is large. This question deserves further study.

The Hafner-McCurley style algorithm we described may not be as efficient as a function field sieve style method. Also, the algorithm we propose requires very efficient algorithms to add divisors on arbitrary curves. There is still much research to be done before these problems have truly efficient solutions.

In conclusion, there are several problems which require further analysis before the Weil descent method can be fully assessed. We expect that, for a random elliptic curve E over a field $\mathbb{F}_{q^n}$ with n reasonably large, it will be possible to show that there is a low probability that there are relatively small genus curves on the Weil restriction of E over $\mathbb{F}_q$. This means that it is unlikely that the method could ever be used to solve the elliptic curve discrete logarithm problem on the sort of curves used in practice. Nevertheless, it seems that the Weil descent is most likely to succeed for elliptic curves defined over $\mathbb{F}_{2^n}$ where the degree n has a small factor (say of size around 5–15). This may explain why some standards bodies have only recommended the use of elliptic curves over prime fields $\mathbb{F}_p$ and fields of the form form $\mathbb{F}_{2^p}$ for prime p.

References

[1] L. Adleman, J. De Marrais, and M.-D. Huang. A subexponential algorithm for discrete logarithms over the rational subgroup of the Jacobians of large genus hyperelliptic curves over finite fields. In *ANTS-1 : Algorithmic Number Theory*, L.M. Adleman and M-D. Huang, editors. Springer-Verlag, LNCS 877, 28–40, 1994.

[2] L.M. Adleman, M.-D. Huang. Primality testing and abelian varieties over finite fields. Springer LNM 1512, 1992.

[3] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger. KANT V4. *J. Symbolic Computation*, **24**, 267–283, 1997.

[4] G. Frey. Weil descent. Talk at Waterloo workshop on the ECDLP, 1998. **http://cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html**

[5] S.D. Galbraith, S. Paulus and N.P. Smart. Arithmetic on super-elliptic curves. Preprint, 1998.

[6] J.L. Hafner and K.S. McCurley. A rigorous subexponential algorithm for computation of class groups. *J. AMS*, **2**, 837–850, 1989.

[7] R. Hartshorne. Algebraic geometry. Springer GTM 52, 1977.

[8] M.-D. Huang, D. Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. J. Symbolic Computation, **18**, 519–539, 1994.

[9] M.-D. Huang, D. Ierardi. Counting points on curves over finite fields. J. Symbolic Computation, **25**, 1–21, 1998.
[10] M. Jacobson, N. Koblitz, J.H. Silverman, A. Stein and E. Teske. Analysis of the Xedni calculus attack. *Preprint*, 1999.
[11] R. Lovorn Bender and C. Pomerance. Rigourous discrete logarithm computations in finite fields via smooth polynomials. In *Computational Perspectives on Number Theory. Proc. of a Conference in honor of A.O.L. Atkin* Vol 7 of AMS/International Press Studies in Advanced Mathematics, Providence, 221–232, 1998.
[12] J.S. Milne. Jacobian Varieties. In *Arithmetic Geometry*, G. Cornell and J.H. Silverman, editors. Springer-Verlag, 167–212, 1986.
[13] A. Müller. Effiziente Algorithmen für Probleme der linearen Algebra über $\mathbb{Z}$. Masters Thesis, Universität Saarlandes, Saabrucken, 1994.
[14] V. Müller, A. Stein and C. Thiel. Computing discrete logarithms in real quadratic function fields of large genus. *Math. Comp.*, **68**, 807–822, 1999.
[15] D. Mumford. Abelian varieties. Oxford, 1970.
[16] S. Paulus. An algorithm of sub-exponential type computing the class group of quadratic orders over principal ideal domains. In *ANTS-2 : Algorithmic Number Theory*, H. Cohen, editor. Springer-Verlag, LNCS 1122, 243–257, 1996.
[17] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. Math. Comp., **55**, 745–763, 1990.
[18] J.H. Silverman. The Xedni calculus and the elliptic curve discrete logarithm problem. *Preprint*, 1998.
[19] E.J. Volcheck. Computing in the Jacobian of a plane algebraic curve. in ANTS-I, Springer LNCS 877, 221-233, 1994.

E-mail address: `stevenga@dcs.rhbnc.ac.uk`

Mathematics Department, Royal Holloway University of London, Egham, Surrey TW20 0EX, U.K.

E-mail address: `nsma@hplb.hpl.hp.com`

Hewlett-Packard Laboratories, Filton Road, Stoke Gifford, Bristol, BS12 6QZ, United Kingdom