Analysis of the Weil Descent Attack of Gaudry, Hess and Smart *

Alfred Menezes[1,2] and Minghua Qu[2]

[1] Dept. of Combinatorics and Optimization, University of Waterloo, Canada
amenezes@certicom.com
[2] Certicom Research, Canada
mqu@certicom.com

Abstract. We analyze the Weil descent attack of Gaudry, Hess and Smart [11] on the elliptic curve discrete logarithm problem for elliptic curves defined over finite fields of characteristic two.

1 Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. The elliptic curve discrete logarithm problem (ECDLP) in $E(\mathbb{F}_q)$ is the following: given E, $P \in E(\mathbb{F}_q)$, $r = \text{ord}(P)$ and $Q \in \langle P \rangle$, find the integer $s \in [0, r-1]$ such that $Q = sP$. The ECDLP is of interest because its apparent intractability forms the basis for the security of elliptic curve cryptographic schemes.

The elliptic curve parameters have to be carefully chosen in order to circumvent some known attacks on the ECDLP. In order to avoid the Pohlig-Hellman [18] and Pollard's rho [19, 16] attacks, r should be a large prime number, say $r > 2^{160}$. To avoid the Weil pairing [14] and Tate pairing [7] attacks, r should not divide $q^k - 1$ for each $1 \leq k \leq C$, where C is large enough so that it is computationally infeasible to find discrete logarithms in $\mathbb{F}_{q^C}$ ($C = 20$ suffices in practice). Finally, the curve should not be $\mathbb{F}_q$-anomalous (i.e., $\#E(\mathbb{F}_q) \neq q$) in order to avoid the attack of [20–22]. For the remainder of this paper, we assume that the elliptic curve parameters satisfy these conditions. In particular, we assume that $r \approx q$.

Recently Gaudry, Hess and Smart [11], building on earlier work of Frey [5, 6] and Galbraith and Smart [8], devised a new attack which utilizes the Weil descent. Their attack is especially interesting because it provides some evidence that certain underlying fields $\mathbb{F}_q$ such as $\mathbb{F}_{2^{155}}$ may lead to an easier ECDLP for a significant proportion of all elliptic curves over $\mathbb{F}_q$. Thus these specific finite fields may be inappropriate for use in elliptic curve cryptographic schemes. The purpose of this paper is to analyze the Weil descent attack of Gaudry, Hess and Smart for elliptic curves define over finite fields of characteristic two, and determine when the attack may be feasible.

The remainder of the paper is organized as follows. The Weil descent attack of Gaudry, Hess and Smart is outlined in §2 and analyzed in §3. In §4, we present some consequences of our analysis. Finally, §5 makes some concluding remarks.

* Revised on April 22, 2001.

2 Weil Descent Attack

Let l and n be positive integers. Let $q = 2^l$, and let $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$. Consider the (non-supersingular) elliptic curve E defined over K by the equation

$$E \; : \; y^2 + xy = x^3 + ax^2 + b, \quad a \in K, \, b \in K^*.$$

Assume that either n is odd, or $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$, or $m(b) = n$ where $m(b)$ is defined below in (1). Gaudry, Hess and Smart [11] showed how Weil descent can be used to reduce the elliptic curve discrete logarithm problem in $E(K)$ to the discrete logarithm problem in a subgroup of order $r \approx q^n$ of the Jacobian $J_C(k)$ of a hyperelliptic curve C of genus g defined over k. One first constructs the Weil restriction $W_{E/k}$ of scalars of E, which is an n-dimensional abelian variety over k. Then, $W_{E/k}$ is intersected with $n-1$ carefully-chosen hyperplanes to obtain the hyperelliptic curve C. We call their reduction algorithm the *GHS attack* on the elliptic curve discrete logarithm problem. Note that $\#J_C(k) \approx q^g$, and a group operation in $J_C(k)$ can be performed in $O(g^2 \log^2 q)$ bit operations using Cantor's algorithm [2,3,17]. The genus g of C is either 2^{m-1} or $2^{m-1} - 1$, where m is determined as follows.

Theorem 1 ([11]) Let $b_i = \sigma^i(b)$, where $\sigma : K \to K$ is the Frobenius automorphism defined by $\alpha \mapsto \alpha^q$. Then

$$m(b) = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, b_0^{1/2}), \ldots , (1, b_{n-1}^{1/2})\}). \tag{1}$$

The discrete logarithm problem in $J_C(k)$ can be solved using one of the following three methods:

1. Pollard's rho algorithm [19,16] which has an expected running time of $O(g^2 q^{n/2} \log^2 q)$ bit operations.
2. The refinement by Enge and Gaudry [4] of the subexponential-time algorithm by Adleman, DeMarrais and Huang [1] which has an expected running time of $L_{q^g}[\sqrt{2}]$ bit operations for $g/\log q \to \infty$, where $L_x[c] = O(\exp((c + o(1))\sqrt{\log x}\sqrt{\log\log x}))$.
3. Gaudry's algorithm [10] which has an expected running time of $O(g^3 q^2 \log^2 q + g^2 g! q \log^2 q)$ bit operations. If g is fixed, then this running time is $O(q^{2+\epsilon})$. In fact, the algorithm can be modified to one with a running time of $O(q^{\frac{2g}{g+1}+\epsilon})$ as $q \to \infty$ [11].

Gaudry's algorithm is faster than Pollard's rho algorithm when $\frac{n}{2} > \frac{2g}{g+1}$ but becomes impractical for large genera, e.g., $g \geq 10$, because of the large multiplicative factor $g!$. For larger g, the algorithm of Enge and Gaudry should be employed. Since its running time is subexponential in q^g, this algorithm is infeasible when q^g is very large, e.g., $q^g \approx 2^{1024}$.

The GHS attack is deemed to be *successful* if the genus g of C is small enough so that either Gaudry's algorithm or Enge and Gaudry's algorithm is more efficient than Pollard's rho algorithm. For example if $q = 2^{31}$ and $n = 5$

then $1 \leq m \leq 5$, so $1 \leq g \leq 16$. In this case it is possible that the GHS attack succeeds for a significant proportion of all elliptic curves over $\mathbb{F}_{2^{155}}$—however further analysis and experimentation is needed before one can conclude this with certainty. We say that the GHS attack *fails* if either q^g is too large, say $q^g \geq 2^{1024}$, or if $g = 1$, in which case $J_C(k)$ is isogenous to $E(k)$. For the case $q = 2$, these conditions translate to $m \geq 11$ or $m = 1$. We stress that failure of the GHS attack does not imply failure of the Weil descent methodology—there may be other useful curves which lie on the Weil restriction $W_{E/k}$ that were not constructed by the GHS method.

3 Analysis

We henceforth assume that $q = 2^l$, i.e., $k = \mathbb{F}_{2^l}$, and that n is a positive integer. Further we assume that either n is odd, or $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$, or $m(b) = n$. By Theorem 1, to determine the practicality of the GHS attack for elliptic curves over $\mathbb{F}_{q^n}$ we have to examine the admissible values of $m(b)$ where $b \in \mathbb{F}_{q^n}$ and $b_i = b^{q^i}$ for $0 \leq i \leq n-1$. Notice that formula (1) for $m(b)$ is independent of the representation used for the elements of K since if $\phi : K \to K$ is an automorphism and $\phi(\beta) = \gamma$, then $\dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{\beta, \beta^q, \ldots, \beta^{q^{n-1}}\}) = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{\gamma, \gamma^q, \ldots, \gamma^{q^{n-1}}\})$. Let $\overline{b} = b^{1/2}$. We have

$$m(b) = m(\overline{b}^2) = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, \overline{b}_0), \ldots, (1, \overline{b}_{n-1})\}),$$

where $\overline{b}_i = \overline{b}^{q^i}$. Since $m(b) = i$ or $i+1$ if $\dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{\overline{b}_0, \ldots, \overline{b}_{n-1}\}) = i$, it suffices to examine the admissible values of

$$\overline{m}(b) = \overline{m}(\overline{b}^2) = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{\overline{b}_0, \ldots, \overline{b}_{n-1}\}).$$

Before proceeding, we review some concepts from linear algebra. We view $\mathbb{F}_{q^n}$ as an ln-dimensional vector space over $\mathbb{F}_2$, and the Frobenius map $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_q$ as a linear transformation of $\mathbb{F}_{q^n}$ over $\mathbb{F}_2$. A polynomial $f \in \mathbb{F}_2[x]$ is said to annihilate σ if $f(\sigma) = 0$, where 0 is the zero map on $\mathbb{F}_{q^n}$. The unique monic polynomial of least degree with this property is called the minimal polynomial of σ over $\mathbb{F}_2$.

Lemma 2 The minimal polynomial of σ over $\mathbb{F}_2$ is $f(x) = x^n - 1$.

Proof. Since $\sigma^n(b) = b^{q^n} = b$ for all $b \in \mathbb{F}_{q^n}$, we have $f(\sigma) = 0$. Now, assume that the non-zero polynomial $g(x) = \sum_{i=0}^{n-1} g_i x^i \in \mathbb{F}_2[x]$ of degree less than n annihilates σ. Then

$$g(\sigma)b = \left(\sum_{i=0}^{n-1} g_i \sigma^i\right) b = \sum_{i=0}^{n-1} g_i b^{q^i} = 0$$

for all $b \in \mathbb{F}_{q^n}$. This is impossible since the polynomial $G(x) = \sum_{i=0}^{n-1} g_i x^{q^i}$ can have at most q^{n-1} roots in $\mathbb{F}_{q^n}$. Thus the minimal polynomial of σ over $\mathbb{F}_2$ is $x^n - 1$. $\square$

For $b \in \mathbb{F}_{q^n}$, the unique monic polynomial $f \in \mathbb{F}_2[x]$ of least degree such that $f(\sigma)b = 0$ is denoted $\mathrm{Ord}_b(x)$. It is easy to see that $\mathrm{Ord}_b(x)|(x^n - 1)$ and $\deg(\mathrm{Ord}_b(x)) = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{b, \sigma(b), \ldots, \sigma^{n-1}(b)\}) = \overline{m}(b^2)$. By considering the cyclotomic cosets of 2 modulo n, we can easily determine the degrees of the irreducible factors of $x^n - 1$ over $\mathbb{F}_2$. We will use this factorization to obtain the possible values of $\mathrm{Ord}_b(x)$, and then determine the admissible values of $m(b)$.

Let $n = 2^e n_1$ where n_1 is odd. Let $h = 2^e$ and $x^n - 1 = (f_0 f_1 \cdots f_s)^h$, where $f_0 = x - 1$ and the f_i's are distinct irreducible polynomials over $\mathbb{F}_2$ with $\deg(f_i) = d_i$.

Lemma 3 Let $W_i = \{b \in \mathbb{F}_{q^n} \mid f_i^h(\sigma)b = 0\}$ for $0 \le i \le s$. Then $\dim_{\mathbb{F}_2} W_i = l \cdot \deg(f_i^h) = l \cdot h \cdot \deg(f_i)$ and $\mathbb{F}_{q^n} = W_0 \oplus W_1 \cdots \oplus W_s$.

Proof. Clearly W_i is a subspace of $\mathbb{F}_{q^n}$. Let $\overline{W}_i = \{f_i^h(\sigma)b \mid b \in \mathbb{F}_{q^n}\}$. Then $\mathbb{F}_{q^n} = W_i \oplus \overline{W}_i$. Now, let $r = \deg(f_i^h)$ and $F_i(x) = (x^n - 1)/f_i^h(x)$ for $0 \le i \le s$. Let $f_i^h(x) = \sum_{i=0}^{r} u_i x^i$ and $F_i(x) = \sum_{i=0}^{n-r} v_i x^i$. For any $c \in \overline{W}_i$ we have $F_i(\sigma)c = 0$. Thus $\sum_{i=0}^{n-r} v_i c^{q^i} = 0$, whence c is a root of $V(x) = \sum_{i=0}^{n-r} v_i x^{q^i}$. Since $\deg(V) = q^{n-r}$, we have $|\overline{W}_i| \le q^{n-r}$. Similarly, for any $b \in W_i$, we have $f_i^h(\sigma)b = 0$, whence b is a root of $U(x) = \sum_{i=0}^{r} u_i x^{q^i}$; hence $|W_i| \le q^r$. Since $|W_i| \cdot |\overline{W}_i| = q^n$, we must have $|W_i| = q^r$ and $|\overline{W}_i| = q^{n-r}$. Thus $\dim_{\mathbb{F}_2} W_i = l \cdot \deg(f_i^h)$ and $\overline{W}_i = \{c \in \mathbb{F}_{q^n} \mid F_i(\sigma)c = 0\}$.

To show that $\mathbb{F}_{q^n} = W_0 \oplus W_1 \cdots \oplus W_s$, we only need to show that if $c = c_0 + c_1 + \cdots + c_s$ where $c_i \in W_i$, then $c = 0$ iff $c_i = 0$ for all $0 \le i \le s$. This is true since for all $0 \le i \le s$, $F_i(\sigma)c = F_i(\sigma)(c_0 + c_1 + \cdots + c_s) = F_i(\sigma)c_i = 0$ iff $c_i = 0$. □

Lemma 4 For $j \in [0, h]$, let $W_i^{(j)}$ be the null space of $f_i^j(x)$. For $j \in [1, h]$, let W_{ij} be any subspace of $W_i^{(j)}$ such that $W_i^{(j)} = W_i^{(j-1)} \oplus W_{ij}$. Then $W_i = W_{i1} \oplus W_{i2} \oplus \cdots \oplus W_{ih}$ where $|W_{ij}| = q^{d_i}$, and $\mathbb{F}_{q^n} = \sum_{i=0}^{s} \sum_{j=1}^{h} W_{ij}$.

Proof. Analogous to the proof of Lemma 3. □

For each $c \in \mathbb{F}_{q^n}$, we can write $c = \sum_{i=0}^{s} \sum_{j=1}^{h} c_{ij}$ where $c_{ij} \in W_{ij}$. For each $i \in [0, s]$, let j_i be the largest index $j \in [1, h]$ such that $c_{ij} \ne 0$; if no such index exists then let $j_i = 0$. We define the *type* of c to be $(j_0, j_1, \ldots, j_s)$.

Theorem 5 Let $c \in \mathbb{F}_{q^n}$. Then the admissible values for $\overline{m}(c^2)$ are $\sum_{i=0}^{s} j_i d_i$ where each $j_i \in [0, h]$. Moreover, there are precisely $\prod_{i=0, j_i \ne 0}^{s} (q^{j_i d_i} - q^{(j_i - 1)d_i})$ elements $c \in \mathbb{F}_{q^n}$ of type $(j_0, j_1, \ldots, j_s)$ with $\overline{m}(c^2) = \sum_{i=0}^{s} j_i d_i$.

Proof. We have $f_i^j(x)|\mathrm{Ord}_c(x)$ if and only if $j_i \ge j$. Now, let $g(x) = \prod_{i=0}^{s} f_i^{j_i}(x)$ be a divisor of $x^n - 1$ with $\deg(g) = \sum_{i=0}^{s} j_i d_i$. Define

$$C = \left\{ \sum_{i=0}^{s} \sum_{j=1}^{h} c_{ij} \mid c_{ij} \in W_{ij},\ \ c_{ij_i} \ne 0 \text{ if } j_i \ne 0,\ \ c_{ij} = 0 \text{ for } j > j_i \right\};$$

note that $\#C = \prod_{i=0, j_i \neq 0}^{s} (q^{j_i d_i} - q^{(j_i - 1) d_i})$. Then for $c \in \mathbb{F}_{q^n}$, $\mathrm{Ord}_c(x) = g(x)$ if and only if $c \in C$. The result now follows. $\square$

Theorem 6 Let $b \in \mathbb{F}_{q^n}$. Then

$$m(b^2) = \begin{cases} \overline{m}(b^2), & \text{if } j_0 \neq 0, \\ \overline{m}(b^2) + 1, & \text{if } j_0 = 0. \end{cases}$$

Proof. Suppose that $\overline{m}(b^2) = T$. Then

$$\mathrm{Span}_{\mathbb{F}_2}\{b_0, b_1, \dots, b_{n-1}\} = \mathrm{Span}_{\mathbb{F}_2}\{b_0, b_1, \dots, b_{T-1}\}.$$

Let $\mathrm{Ord}_b(x) = k_0 + k_1 x + \cdots + k_{T-1} x^{T-1} + x^T$.

Suppose first that $j_0 = 0$. Then $x - 1$ does not divide $\mathrm{Ord}_b(x)$. It follows that $k_0 + k_1 + \cdots + k_{T-1} = 0$. From $k_0 b_0 + k_1 b_1 + \cdots + k_{T-1} b_{T-1} = b_T$ we have

$$(0, b_T) = k_0(1, b_0) + k_1(1, b_1) + \cdots + k_{T-1}(1, b_{T-1}).$$

Thus $(0, b_T)$ and hence also $(1, 0)$ are in $\mathrm{Span}_{\mathbb{F}_2}\{b_0, \dots, b_{n-1}\}$. It follows that

$$\mathrm{Span}_{\mathbb{F}_2}\{(1, b_0), \dots, (1, b_{n-1})\} = \mathrm{Span}_{\mathbb{F}_2}\{(1, b_0), \dots, (1, b_{T-1}), (1, 0)\}.$$

Hence $m(b^2) = T + 1$.

Suppose now that $j_0 \neq 0$. Then $x - 1$ divides $\mathrm{Ord}_b(x)$. It follows that $k_0 + k_1 + \cdots + k_{T-1} = 1$. From $k_0 b_0 + k_1 b_1 + \cdots + k_{T-1} b_{T-1} = b_T$ we have

$$(1, b_T) = k_0(1, b_0) + k_1(1, b_1) + \cdots + k_{T-1}(1, b_{T-1}).$$

Since $b_{T+j} = k_0 b_j + k_1 b_{1+j} + \cdots + k_{T-1} b_{T-1+j}$ for $j \geq 0$, it follows that

$$\begin{aligned} (1, b_{T+j}) &= k_0(1, b_j) + k_1(1, b_{1+j}) + \cdots + k_{T-1}(1, b_{T-1+j}) \\ &= u_0(1, b_0) + u_1(1, b_1) + \cdots + u_{T-1}(1, b_{T-1}) \end{aligned}$$

for some $(u_0, u_1, \dots, u_{T-1})$. Hence $m(b^2) = T$. $\square$

We next consider the case where n is an odd prime.

Lemma 7 Let n be an odd prime, and let $t = \mathrm{ord}_n(2)$ be the order of 2 modulo n. Let $n = st + 1$. Then $x^n - 1$ factors over $\mathbb{F}_2$ as $x^n - 1 = (x - 1) f_1 f_2 \cdots f_s$ where the f_i's are distinct irreducible polynomials of degree t.

Proof. Since $\gcd(nx^{n-1}, x^n - 1) = 1$, $x^n - 1$ has no repeated factors. Let f_i be an irreducible factor of $x^n - 1$ with $\deg(f_i) = c > 1$, and let $\alpha \in \mathbb{F}_{2^c}$ be a root of f_i. Since $2^t \equiv 1 \pmod{n}$ and $\alpha^n = 1$, we have $\alpha^{2^t - 1} = 1$, whence $\alpha \in \mathbb{F}_{2^t}$ and $c | t$. Conversely, since $\alpha^{2^c - 1} = 1$, we have $2^c \equiv 1 \pmod{n}$, whence $t | c$. Hence $c = t$. $\square$

Corollary 8 Let n be an odd prime, and let $t = \mathrm{ord}_n(2)$. Let $n = st + 1$, and let $b \in \mathbb{F}_{q^n}$. Then the admissible values for $\overline{m}(b^2)$ are it and $it + 1$, for $0 \le i \le s$. Moreover, for each $0 \le i \le s$, there are $\binom{s}{i}(q^t - 1)^i$ elements $b \in \mathbb{F}_{q^n}$ with $\overline{m}(b^2) = it$, and $(q-1)\binom{s}{i}(q^t - 1)^i$ elements $b \in \mathbb{F}_{q^n}$ with $\overline{m}(b^2) = it + 1$.

Proof. Follows from Theorem 5 since $h = 1$, $d_0 = 1$, and $d_i = t$ for $i \in [1, s]$. $\square$

Corollary 9 Let n be an odd prime, and let $t = \mathrm{ord}_n(2)$. Let $n = st + 1$, and let $b \in \mathbb{F}_{q^n}$. Then

$$m(b^2) = \begin{cases} \overline{m}(b^2), & \text{if } \overline{m}(b^2) = it + 1 \text{ for some } 0 \le i \le s, \\ \overline{m}(b^2) + 1, & \text{if } \overline{m}(b^2) = it \text{ for some } 0 \le i \le s. \end{cases}$$

Moreover, for each $0 \le i \le s$, the number of elements $b \in \mathbb{F}_{q^n}$ with $m(b^2) = it + 1$ is $q\binom{s}{i}(q^t - 1)^i$.

Proof. Follows from Theorem 6. $\square$

4 Consequences

We use the results of §3 to study the feasibility of the GHS attack on the ECDLP for elliptic curves defined over $\mathbb{F}_{2^n}$. We are particularly interested in the odd primes $n \in [160, 600]$ which are the field dimensions of interest when implementing elliptic curve cryptographic schemes. We also consider the case $n = 155$ which is included in an IETF standard [12] for key establishment.

For odd primes n, we define $M(n) = \mathrm{ord}_n(2) + 1$. Observe that $M(n)$ is the smallest attainable value $m(b) > 1$ for $b \in \mathbb{F}_{2^n}$. Table 1 lists the values of $M(n)$ for all primes $n \in [100, 600]$. Since $M(n) \ge 17$ for all primes $n \in [160, 600]$, we conclude that the GHS attack is infeasible for *all* elliptic curves defined over $\mathbb{F}_{2^n}$ where n is prime and $n \in [160, 600]$.

Table 1. Values of $M(n)$ for primes $n \in [100, 600]$.

n	$M(n)$	n	$M(n)$	n	$M(n)$	n	$M(n)$	n	$M(n)$	n	$M(n)$	n	$M(n)$
101	101	163	163	229	77	293	293	373	373	443	443	521	261
103	52	167	84	233	30	307	103	379	379	449	225	523	523
107	107	173	173	239	120	311	156	383	192	457	77	541	541
109	37	179	179	241	25	313	157	389	389	461	461	547	547
113	29	181	181	251	51	317	317	397	45	463	232	557	557
127	8	191	96	257	17	331	31	401	201	467	467	563	563
131	131	193	97	263	132	337	22	409	205	479	240	569	285
137	69	197	197	269	269	347	347	419	419	487	244	571	115
139	139	199	100	271	136	349	349	421	421	491	491	577	145
149	149	211	211	277	93	353	89	431	44	499	167	587	587
151	16	223	38	281	71	359	180	433	73	503	252	593	149
157	53	227	227	283	95	367	184	439	74	509	509	599	300

Remark 10 (*fraction of elliptic curves over $\mathbb{F}_{2^n}$ with $m = n$*) If n is an odd prime then by Corollary 9 the fraction of $b \in \mathbb{F}_{2^n}$ for which $m(b) = n$ is

$$\frac{2\binom{s}{s}(2^t-1)^s}{2^n} = \left(1 - \frac{1}{2^t}\right)^s \geq \left(1 - \frac{1}{n}\right)^s$$

since $t = \mathrm{ord}_n(2) \geq \lceil \log_2 n \rceil$. In particular, if $\mathrm{ord}_n(2) = n-1$ (equivalently, $1+x+x^2+\cdots+x^{n-1}$ is irreducible over $\mathbb{F}_2$), then $m(b) = 1$ or n for all $b \in \mathbb{F}_{2^n}$. In this case, the GHS attack will fail in the worst possibly way for *all* $b \in \mathbb{F}_{2^n}$. The prime numbers $n \in [100, 600]$ for which $\mathrm{ord}_n(2) = n-1$ are 101, 107, 131, 139, 149, 163, 173, 179, 181, 197, 211, 227, 269, 293, 317, 347, 349, 373, 379, 389, 419, 421, 443, 461, 467, 491, 509, 523, 541, 547, 557, 563 and 587.

Remark 11 (*infeasibility of the GHS attack on elliptic curves over the NIST binary fields*) In February 2000, FIPS 186-1 was revised by NIST to include the elliptic curve digital signature algorithm (ECDSA) with further recommendations for the selection of underlying finite fields and elliptic curves; the revised standard is called FIPS 186-2 [15]. FIPS 186-2 has 10 recommended finite fields: 5 prime fields, and the binary fields $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{233}}$, $\mathbb{F}_{2^{283}}$, $\mathbb{F}_{2^{409}}$, and $\mathbb{F}_{2^{571}}$. The binary fields $\mathbb{F}_{2^n}$ were selected so that n is at least twice the key lengths of common symmetric-key block ciphers, and so that there exists a Koblitz curve[1] of almost prime order over $\mathbb{F}_{2^n}$. Since for Koblitz curves E, $\#E(\mathbb{F}_{2^l})$ divides $\#E(\mathbb{F}_{2^n})$ whenever l divides n, this requirement imposes the condition that n be prime. Note that $m = 1$ for Koblitz curves, so $g = 1$ and hence the GHS attack will always fail. Table 2 lists the values of $M(n)$ for $n \in \{163, 233, 283, 409, 571\}$. From this table, we can conclude that the GHS attack is infeasible for *all* elliptic curves defined over the NIST binary fields.

Table 2. Values of $M(n)$ for NIST-recommended fields $\mathbb{F}_{2^n}$.

n	163	233	283	409	571
$M(n)$	163	30	95	205	115

Remark 12 (*smallest possible value of $M(n)$*) Let n be an odd prime. Since $t = \mathrm{ord}_n(2) \geq \lceil \log_2 n \rceil$, we have $M(n) \geq \lceil \log_2 n \rceil + 1$. It is easy to see that the lower bound is attained precisely when n is a Mersenne prime. The only Mersenne prime in the interval $[100, 600]$ is $n = 127$.

Remark 13 (*Koblitz curves vs. random curves*) As noted in Remark 11, Koblitz curves are attractive for practical use because the Frobenius endomorphism

[1] Koblitz curves [13] are elliptic curves defined over $\mathbb{F}_2$. They are attractive for practical use because there are very fast special-purpose algorithms for performing elliptic curve arithmetic [23].

$\sigma : E(\mathbb{F}_{2^n}) \to E(\mathbb{F}_{2^n})$ defined by $(x, y) \mapsto (x^2, y^2)$ can be used to devise very fast algorithms for elliptic curve point multiplication. The special structure associated with Koblitz curves has also yielded a speedup[2] of Pollard's rho algorithm for the ECDLP on these curves [9, 24]. It is interesting to note that Koblitz curves are more resilient to the GHS attack than random curves since the GHS attack is a priori guaranteed to fail for a Koblitz curve (since $m = 1$), while it might succeed (albeit with an extremely low probability) for a randomly selected curve if m is small (e.g., the elliptic curve over $\mathbb{F}_{2^{127}}$ with $m = 7$).

Remark 14 (*constructing elliptic curves over $\mathbb{F}_{2^n}$ with a given admissible value m*) Given an admissible value m, an elliptic curve $y^2 + xy = x^3 + b$ over $\mathbb{F}_{2^n}$ having this m value can be efficiently constructed by first factoring $x^n - 1$, then finding bases for the subspaces W_i (see Lemma 3), and finally selecting $b \in \mathbb{F}_{2^n}$ with $m(b) = m$.

Remark 15 (*GHS attack on elliptic curves over $\mathbb{F}_{2^{155}}$*) Since $\mathbb{F}_{2^{155}}$ has three proper subfields, namely $\mathbb{F}_2$, $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^{31}}$, there are three ways of applying the GHS attack to the ECDLP for elliptic curves over $\mathbb{F}_{2^{155}}$.

(i) If we take $q = 2^{31}$ and $n = 5$, then $t = \mathrm{ord}_5(2) = 4$. Thus $m(b) = 1$ or 5 for all $b \in \mathbb{F}_{2^{155}}$, so the GHS attack reduces the ECDLP to the DLP in the Jacobian of a hyperelliptic curve of genus 1, 15 or 16 over $\mathbb{F}_{2^{31}}$. If the genus is 15 or 16, then the resulting hyperelliptic curve DLP is outside the feasible limits of Gaudry's algorithm [10], and likely also outside the feasible limits of the Adleman-DeMarrais-Huang (ADH) algorithm and its variants [1, 4]; however further experimentation is needed before the latter can be concluded with certainty.

(ii) If we take $q = 2^5$ and $n = 31$, then $t = \mathrm{ord}_{31}(2) = 5$ and $s = 6$. Thus $m(b) = 1, 6, 11, 16, 21, 26$ or 31 for all $b \in \mathbb{F}_{2^{155}}$. Thus there are some curves over $\mathbb{F}_{2^{155}}$ for which the GHS attack reduces the ECDLP to the DLP in the Jacobian of a hyperelliptic curve of genus 31 or 32 over $\mathbb{F}_{2^5}$. By Corollary 9, the number of $b \in \mathbb{F}_{2^{155}}$ for which this holds is $2^5 \cdot 6 \cdot (2^{25} - 1) \approx 2^{32}$. The subexponential-time ADH algorithm and its variants can likely solve these resulting hyperelliptic curve DLPs efficiently since the group size is $\approx 2^{155}$; again further experimentation is required before this can be concluded with certainty.

(iii) Suppose that we take $q = 2$ and $n = 155$. Now, $x^{155} - 1$ has 14 distinct irreducible factors over $\mathbb{F}_2$: 1 factor of degree 1, 1 factor of degree 4, 6 factors of degree 5, and 6 factors of degree 20. Since the order of the elliptic curve group is $\approx 2^{155}$, we need to reduce the ECDLP to the DLP in the Jacobian of a hyperelliptic curve of genus $g \geq 155$. Thus we need $2^{m-1} \geq 155$, i.e., $m \geq 9$. By Theorems 5 and 6, the elliptic curves $y^2 + xy = x^3 + b^2$ where $\deg(\mathrm{Ord}_b(x)) = 9$ have $m(b^2) = 10$. Hence the GHS attack reduces the ECDLP in these curves to the DLP in the Jacobian of a hyperelliptic curve

[2] The speedup is by a factor of $\sqrt{n}$ for Koblitz curves over $\mathbb{F}_{2^n}$.

over $\mathbb{F}_2$ of genus 511 or 512. As in (i), this is likely outside the feasible limits of the ADH algorithm and its variants.

We conclude that only a small fraction of elliptic curves over $\mathbb{F}_{2^{155}}$ may be susceptible to the GHS attack, namely those elliptic curves in (ii) for which $m = 6$.

5 Conclusions

We have shown that the Weil descent attack of Gaudry, Hess and Smart on the elliptic curve discrete logarithm problem over $\mathbb{F}_{2^n}$ for primes $n \in [160, 600]$ is infeasible for all elliptic curves defined over $\mathbb{F}_{2^n}$. We stress that failure of the GHS attack does not imply failure of the Weil descent methodology—there may be other useful curves which lie on the Weil restriction $W_{E/k}$ that were not constructed by the GHS method.

Acknowledgements

The authors would like to thank Steven Galbraith and Neal Koblitz for their helpful comments on an earlier draft of this paper.

References

1. L. Adleman, J. DeMarrais and M. Huang, "A subexponential algorithm for discrete logarithms over the rational subgroup of the jacobians of large genus hyperelliptic curves over finite fields", *Algorithmic Number Theory*, LNCS **877**, 1994, 28-40.
2. D. Cantor, "Computing in the jacobian of a hyperelliptic curve", *Mathematics of Computation*, **48** (1987), 95-101.
3. A. Enge, "The extended Euclidean algorithm on polynomials, and the efficiency of hyperelliptic cryptosystems", *Designs, Codes and Cryptography*, to appear.
4. A. Enge and P. Gaudry, "A general framework for subexponential discrete logarithm algorithms", *Rapport de Recherche Lix/RR/00/04*, June 2000. Available from http://ultralix.polytechnique.fr/Labo/Pierrick.Gaudry/papers.html
5. G. Frey, "How to disguise an elliptic curve (Weil descent)", Talk at ECC '98, Waterloo, 1998. Slides available from http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html
6. G. Frey, "Applications of arithmetical geometry to cryptographic constructions", *Proceedings of the Fifth International Conference on Finite Fields and Applications*, to appear. Also available from http://www.exp-math.uni-essen.de/zahlentheorie/preprints/Index.html
7. G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, **62** (1994), 865-874.
8. S. Galbraith and N. Smart, "A cryptographic application of Weil descent", *Codes and Cryptography*, LNCS **1746**, 1999, 191-200.

9. R. Gallant, R. Lambert and S. Vanstone, "Improving the parallelized Pollard lambda search on binary anomalous curves", to appear in *Mathematics of Computation.*
10. P. Gaudry, "An algorithm for solving the discrete log problem on hyperelliptic curves", *Advances in Cryptology – Eurocrypt 2000*, LNCS **1807**, 2000, 19-34.
11. P. Gaudry, F. Hess and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves", preprint, January 2000. Available from http://ultralix.polytechnique.fr/Labo/Pierrick.Gaudry/papers.html
12. Internet Engineering Task Force, *The OAKLEY Key Determination Protocol*, IETF RFC 2412, November 1998.
13. N. Koblitz, "CM-curves with good cryptographic properties", *Advances in Cryptology – Crypto '91*, LNCS **576**, 1992, 279-287.
14. A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, **39** (1993), 1639-1646.
15. National Institute of Standards and Technology, *Digital Signature Standard*, FIPS Publication 186-2, February 2000.
16. P. van Oorschot and M. Wiener, "Parallel collision search with cryptanalytic applications", *Journal of Cryptology*, **12** (1999), 1-28.
17. S. Paulus and A. Stein, "Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves", *Algorithmic Number Theory*, LNCS **1423**, 1998, 576-591.
18. S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", *IEEE Transactions on Information Theory*, **24** (1978), 106-110.
19. J. Pollard, "Monte Carlo methods for index computation mod p", *Mathematics of Computation*, **32** (1978), 918-924.
20. T. Satoh and K. Araki, "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves", *Commentarii Mathematici Universitatis Sancti Pauli*, **47** (1998), 81-92.
21. I. Semaev, "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p", *Mathematics of Computation*, **67** (1998), 353-356.
22. N. Smart, "The discrete logarithm problem on elliptic curves of trace one", *Journal of Cryptology*, **12** (1999), 193-196.
23. J. Solinas, "Efficient arithmetic on Koblitz curves", *Designs, Codes and Cryptography*, **19** (2000), 195-249.
24. M. Wiener and R. Zuccherato, "Faster attacks on elliptic curve cryptosystems", *Selected Areas in Cryptography*, LNCS **1556**, 1999, 190-200.