J. Math. Cryptol. **4** (2010), 175–191
DOI 10.1515/JMC.2010.007

On the asymptotic effectiveness of Weil descent attacks

Koray Karabina, Alfred Menezes, Carl Pomerance and Igor E. Shparlinski

Communicated by Neal Koblitz

Abstract. In this paper we investigate the asymptotic effectiveness of the Gaudry–Hess–Smart Weil descent attack and its generalization to the discrete logarithm problem for elliptic curves over characteristic-two finite fields. In particular we obtain nontrivial lower and upper bounds on the smallest possible genus to which it can lead.

Keywords. Elliptic curve discrete logarithm problem, Weil descent attacks.

2010 Mathematics Subject Classification. 11T71, 94A60.

1 Introduction

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$, and let $P \in E(\mathbb{F}_q)$ be a point of order d; see [24] for a background on elliptic curves. Given $Q \in \langle P \rangle$, the elliptic curve discrete logarithm problem (ECDLP) is that of finding the integer $\lambda \in [0, d-1]$ such that $Q = \lambda P$. Intractability of the ECDLP is the basis for the security of all elliptic curve cryptographic systems [1, 2].

The fastest general-purpose algorithm known for solving the ECDLP is Pollard's rho method [21] which has a fully-exponential expected running time of $\sqrt{\pi d}/2 = O(q^{1/2})$. For a fixed field $\mathbb{F}_q$, resistance to Pollard's rho method is maximized by selecting an elliptic curve E for which d is prime and as large as possible, that is, $d \approx q$. Elliptic curves for which such a choice is possible are said to be *cryptographically interesting*. In the remainder of this paper we restrict our attention to cryptographically interesting elliptic curves.

ECDLP solvers that are faster *in practice* than Pollard's rho method are known for special classes of elliptic curves, including those for which the multiplicative order of q modulo d is small [7, 18], and for prime-field anomalous curves [22, 23, 25]. Another attack known on the ECDLP is the Gaudry–Hess–Smart (GHS)

This work started during a very enjoyable visit of I.S. to the University of Waterloo; its support and stimulating research atmosphere are gratefully appreciated. Research of C.P. was supported by NSF grant DMS-0703850, research of I.S. was supported by ARC grants DP0881473 and DP1092835.

Weil descent attack [10] which, for elliptic curves defined over characteristic-two finite fields $\mathbb{F}_{q^n}$, maps the ECDLP to the discrete logarithm problem (DLP) in the divisor class group of a hyperelliptic curve defined over the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^n}$, and thereafter employs a (hopefully faster) algorithm for solving the resulting DLP (see Section 2). The GHS attack has been shown to be faster than Pollard's rho method for some cryptographically interesting elliptic curves defined over $\mathbb{F}_{2^N}$ for some composite $N \in [160, 600]$; see [17]. Furthermore, it has been shown in [20] to be faster than Pollard's rho method for (almost) all cryptographically interesting elliptic curves defined over fields $\mathbb{F}_{2^{5\ell}}$ with $\ell \in [32, 120]$; see also [19].

In this paper, we study the asymptotic effectiveness of Weil descent attacks for solving the ECDLP. More precisely, we ask if there are any infinite families of characteristic-two finite fields $\mathbb{F}_{q^n}$ for which Weil descent attacks are effective in the sense that they can solve the ECDLP in $E(\mathbb{F}_{q^n})$ for (almost) all cryptographically interesting elliptic curves E defined over the fields $\mathbb{F}_{q^n}$ faster than the ECDLP solvers (such as Pollard's rho method) which do not employ the Weil descent methodology.

We obtain nontrivial upper bounds on the genus of the curve over $\mathbb{F}_q$ obtained as a result of the Weil descent. These bounds, although of independent interest, are unfortunately exponential in n and thus are too high to guarantee the efficiency of the corresponding attack. Furthermore, we show that for almost all elliptic curves over $\mathbb{F}_{q^n}$ there is a lower bound that is also exponential in n. This lower bound result shows that asymptotically, the Weil descent attacks are almost never computationally efficient and are slower than other known algorithms for the ECDLP.

The remainder of this paper is organized as follows. The GHS attack and its generalization by Hess are outlined in Section 2. The asymptotic effectiveness of the generalized GHS (gGHS) attack is examined in Section 3. This is closely related to the size of the genus g of the curve obtained as a result of the Weil descent. In turn g can be estimated in terms of a certain kind of decomposition of finite field elements; such decompositions are a central part of the generalized GHS attack. In Section 4, we establish some asymptotic bounds for the number of these decompositions which in particular imply their existence. Our lower and upper bounds on g are derived in Section 5.

2 Weil descent attacks

Let ℓ and n be positive integers, and let $N = \ell n$ and $q = 2^\ell$. For $a \in \mathbb{F}_{q^n}$, we use

$$\operatorname{Tr}_2(a) = \sum_{i=0}^{N-1} a^{2^i} \quad \text{and} \quad \operatorname{Tr}_q(a) = \sum_{i=0}^{n-1} a^{q^i} \tag{2.1}$$

to denote the absolute trace and the relative trace with respect to $\mathbb{F}_q$, respectively.

Let $\delta \in \mathbb{F}_{q^n}$ be an element with $\mathrm{Tr}_2(\delta) = 1$. Then there are $2(q^n - 1)$ isomorphism classes of ordinary elliptic curves defined over $\mathbb{F}_{q^n}$ with representatives

$$E : \; y^2 + xy = x^3 + ax^2 + b, \quad a \in \{0, \delta\}, \; b \in \mathbb{F}_{q^n}^*. \tag{2.2}$$

For a polynomial

$$f(X) = \sum_{i=0}^{m} c_i X^i \in \mathbb{F}_2[X]$$

we denote the corresponding *linearized polynomial*

$$f^{\pi}(X) = \sum_{i=0}^{m} c_i X^{q^i}.$$

For $\gamma \in \mathbb{F}_{q^n}$, let $\mathrm{Ord}_\gamma(X)$ denote the unique nonzero polynomial $f \in \mathbb{F}_2[X]$ of least degree satisfying $f^{\pi}(\gamma) = 0$. Note that $f \mid X^n + 1$.

Now, let E be a cryptographically interesting elliptic curve defined over $\mathbb{F}_{q^n}$ by (2.2). Let $\alpha, \beta \in \mathbb{F}_{q^n}$ be such that $b = (\alpha\beta)^2$. If $\mathrm{Tr}_2(a) = 1$, we further assume that

$$\mathrm{Tr}_q(\alpha) \neq 0 \quad \text{or} \quad \mathrm{Tr}_q(\beta) \neq 0. \tag{2.3}$$

Let $r = \deg(\mathrm{Ord}_\alpha)$, $s = \deg(\mathrm{Ord}_\beta)$, and

$$t = \deg \mathrm{lcm}(\mathrm{Ord}_\alpha, \mathrm{Ord}_\beta).$$

Via a birational transformation the defining equation of E can be brought into the form $y^2 + y = \alpha/x + a + \beta x$. Then Hess's generalization [11, Theorems 11,12] of the GHS attack constructs a curve C defined over $\mathbb{F}_q$ of genus

$$g = 2^t - 2^{t-r} - 2^{t-s} + 1. \tag{2.4}$$

Moreover, if

$$\mathbb{F}_q(\alpha, \beta) = \mathbb{F}_{q^n} \tag{2.5}$$

then Hess's generalized GHS attack [11] yields an explicit (and non-trivial) group homomorphism

$$\phi : E(\mathbb{F}_{q^n}) \to J_C(\mathbb{F}_q),$$

where J_C is the divisor class group of C. Note that if b is not contained in any proper subfield of $\mathbb{F}_{q^n}$, then (2.5) is satisfied. Note also that if $\alpha = 1$ or $\beta = 1$, then the generalized GHS attack specializes to the GHS attack, in which case the curve C is hyperelliptic. Since $\#J_C(\mathbb{F}_q) \approx q^g$ and $J_C(\mathbb{F}_q)$ should contain a subgroup of order $d \approx q^n$ for the attack to have a chance of working, we require that $g \geq n$.

Since $t \leq n$, we have $g \leq 2^n - 1$. In order to minimize the time to solve the resulting instance of the DLP in $J_C(\mathbb{F}_q)$, a decomposition $b = (\alpha\beta)^2$ should be chosen so that g is as small as possible. The running time of the generalized GHS attack is then determined by the time to find a suitable decomposition and the time to solve the DLP in $J_C(\mathbb{F}_q)$.

3 Analysis

At the time the GHS attack was first formulated, it was asymptotically effective for the case $n > 4$ fixed and $q \to \infty$; see [10, 12]. This was because the fastest algorithm known at the time for computing logarithms in the divisor class group of a genus-g hyperelliptic curve over $\mathbb{F}_q$ had (heuristic) running time $O(q^2)$ (for fixed g and $q \to \infty$), see [9], which was faster than the running time $O(q^{n/2})$ of Pollard's rho method for computing discrete logarithms in $E(\mathbb{F}_{q^n})$.

However, recent progress by Diem [3,4] and others on algorithms for computing discrete logarithms necessitates a reevaluation of the effectiveness of Weil descent attacks.

We now summarize the state-of-the-art rigorous algorithms for the ECDLP and the DLP in the divisor class group of curves:

(i) Assume that $n \geq 2$ is fixed. Then the ECDLP over $\mathbb{F}_{q^n}$ can be solved in expected time $q^{2-2/n}(\log q)^{O(1)}$, see [4].

(ii) Assume that $g \geq 2$ is fixed. Then the DLP in the divisor class groups of genus-g curves over $\mathbb{F}_q$ can be solved in expected time $q^{2-2/g}(\log q)^{O(1)}$, see [4].

(iii) Assume that $n \to \infty$ and $n = O(\sqrt{\log q})$. Then the ECDLP over $\mathbb{F}_{q^n}$ can be solved in expected time $q^{O(1)}$, see [3].

The algorithms in (i), (ii) and (iii) are based purely on index calculus. We see that since $g \geq n$ in order for $J_C(\mathbb{F}_q)$ to contain a subgroup of order n, the gGHS (and GHS) Weil descent attacks mentioned in Section 2 are asymptotically inferior for the case n fixed and $q \to \infty$. Note that this statement does not contradict the claims made in Section 1 about the usefulness of GHS attacks *in practice* since, for some fixed n and q in ranges of practical interest, Pollard's rho method [21] is indeed faster than the ECDLP solver in (i) and Gaudry's algorithm [9] for computing discrete logarithms in the resulting hyperelliptic curves is indeed faster than the DLP solver in (ii).

Furthermore, the fastest general rigorous algorithm known for computing discrete logarithms in the divisor class groups of genus-g algebraic curves over finite fields $\mathbb{F}_q$ is due to Hess [13] and has subexponential running time $L_{q^g}[1/2, (1+o(1))\kappa]$ for some constant $\kappa > 0$, provided that $\log q = o(g \log g)$, where as usual for $0 < c < 1$ and $\kappa > 0$ we define

$$L_{q^g}[c, \kappa] = e^{\kappa (\log q^g)^c (\log\log q^g)^{1-c}} = q^{\kappa g^c ((\log g + \log\log q)/\log q)^{1-c}}. \tag{3.1}$$

Hence

$$L_{q^g}[1/2, \kappa] \geq q^{\kappa \sqrt{g \log g}/\sqrt{\log q}}.$$

Since $\log q = o(g \log g)$, we conclude that the running time of Hess's algorithm is not polynomial in q, and hence the gGHS Weil descent strategy cannot be effective for the case $n = O(\sqrt{\log q})$.

Enge and Gaudry [5] have recently devised and analyzed a new subexponential-time algorithm for computing discrete logarithms in the divisor class group of a special class of curves. Their algorithm has (heuristic) expected running time $L_{q^g}[1/3 + \varepsilon, 1]$ for some fixed $\varepsilon > 0$, provided that $g \geq (\log q)^\delta$ for any fixed $\delta > 2$. By (3.1), we have

$$L_{q^g}[1/3 + \varepsilon, 1] = q^{(g (\log q)^{-2})^{1/3+\varepsilon} (\log g + \log\log q)^{2/3-\varepsilon} (\log q)^{3\varepsilon}}.$$

Since $g \geq (\log q)^\delta$ with $\delta > 2$, we conclude that the running time of the Enge-Gaudry algorithm is not polynomial in q, and hence the Weil descent strategy once again is ineffective for the case $n = O(\sqrt{\log q})$.

Let us now consider the case where n and q grow in such a way

$$n/\sqrt{\log q} \to \infty, \quad \text{as } q \to \infty, \tag{3.2}$$

(thus the algorithm of [3] does not apply). In this case, Pollard's rho method is the fastest known DLP solver for $E(\mathbb{F}_{q^n})$, having running time $O(q^{n/2})$. Let us make the optimistic assumption that Hess's algorithm [13] has running time $L_{q^g}[1/2, (1+o(1))\kappa]$, with some constant $\kappa > 0$, for *all* genus-g curves over $\mathbb{F}_q$ (that is, even without the condition $\log q = o(g \log g)$). Now, in order for the gGHS attack to be effective, we require that at least $L_{q^g}[1/2, \kappa] \leq q^{n/2}$. From (3.1), we get

$$g(\log g + \log\log q) = O(n^2 \log q). \tag{3.3}$$

Under the condition (3.2) we see that (3.3) implies $g = O(n^4)$.

Recall that the gGHS attack yields a curve of genus g, where $n \leq g \leq 2^{n-1} - 1$. This means that in order for this attack to be successful the genus of the curves obtained via the gGHS Weil descent have to be close to the lower end of the range.

Here we obtain a nontrivial bound on the smallest achievable genus g, which however is much higher than the above threshold $g = O(n^4)$. Furthermore, we show that for almost all curves, g is much larger.

4 The number of decompositions

In this section, we drop the restriction that the characteristic of $\mathbb{F}_q$ is 2. Thus we let $q = p^\ell$ for some prime p. For $\gamma \in \mathbb{F}_{q^n}$, the unique polynomial $f \in \mathbb{F}_p[X]$ of least degree satisfying $f^\pi(\gamma) = 0$ is denoted $\mathrm{Ord}_\gamma(X)$; note that f is a factor of $X^n - 1$. It is well known [16, Theorem 3.62] that if $h \in \mathbb{F}_p[X]$ is a degree-k divisor of $X^n - 1$, then $h^\pi(X) \mid X^{q^n} - X$ and the roots of $h^\pi(X)$ form a k-dimensional vector space of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.

Now, let $F, G \in \mathbb{F}_p[X]$ be two divisors of $X^n - 1$, and let $b \in \mathbb{F}_{q^n}$. In this section, we establish asymptotic bounds for the number $N_{F,G}(b)$ of pairs (α, β) with $b = \alpha\beta$, where α and β are roots of $F^\pi(X)$ and $G^\pi(X)$, respectively.

Theorem 4.1. *For any $b \in \mathbb{F}_{q^n}^*$, we have*

$$\left| N_{F,G}(b) - \frac{q^n - 1}{q^{2n-r-s}} \right| < 2q^{n/2}$$

where $r = \deg F$ and $s = \deg G$.

Proof. As we have mentioned, the condition $F(X) \mid X^n - 1$ implies that $F^\pi(X) \mid X^{q^n} - X$, and thus the set of all q^r roots of $F^\pi(X)$ forms an r-dimensional linear space $\mathcal{L}_F$. Let $\omega_1, \ldots, \omega_r$ be a basis of $\mathcal{L}_F$ over $\mathbb{F}_q$, which we extend to a basis $\omega_1, \ldots, \omega_n$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. Let $\rho_1, \ldots, \rho_n$ be the dual basis [16, Definition 2.30], so

$$\mathrm{Tr}_q(\omega_i \rho_j) = \begin{cases} 1, & \text{if } i = n - j + 1, \\ 0, & \text{otherwise}, \end{cases} \qquad 1 \le i, j \le n,$$

where as before Tr_q is the relative trace function with respect to $\mathbb{F}_q$ given by (2.1). Then $\alpha \in \mathbb{F}_{q^n}$ is a root of $F^\pi(X)$ if and only if

$$\mathrm{Tr}_q(\alpha\rho_j) = 0, \quad j = 1, \ldots, n - r. \tag{4.1}$$

Similarly, there are $n - s$ elements $\vartheta_1, \ldots, \vartheta_{n-s} \in \mathbb{F}_{q^n}$ that are linearly independent over $\mathbb{F}_q$ such that $\beta \in \mathbb{F}_{q^n}$ is a root of $G^\pi(X)$ if and only if

$$\mathrm{Tr}_q(\beta\vartheta_k) = 0, \quad k = 1, \ldots, n - s. \tag{4.2}$$

We now fix a nontrivial additive character χ of $\mathbb{F}_q$ and recall the orthogonality property of additive characters

$$\sum_{u \in \mathbb{F}_q} \chi(uz) = \begin{cases} 0, & \text{if } z \in \mathbb{F}_q^*, \\ q, & \text{if } z = 0. \end{cases}$$

Then, using (4.1) and (4.2) we write

$$N_{F,G}(b) = \sum_{\alpha \in \mathbb{F}_{q^n}^*} \frac{1}{q^{2n-r-s}} \times \sum_{\substack{u_1,\dots,u_{n-r} \in \mathbb{F}_q \\ v_1,\dots,v_{n-s} \in \mathbb{F}_q}} \chi\Big(\sum_{j=1}^{n-r} u_j \operatorname{Tr}_q(\alpha\rho_j) + \sum_{k=1}^{n-s} v_k \operatorname{Tr}_q(b\alpha^{-1}\vartheta_k)\Big).$$

After changing the order of summation and then separating the term $(q^n - 1)/q^{2n-r-s}$ corresponding to

$$u_1 = \cdots = u_{n-r} = v_1 = \cdots = v_{n-s} = 0,$$

we obtain

$$\Big| N_{F,G}(b) - \frac{q^n - 1}{q^{2n-r-s}} \Big| \le \frac{1}{q^{2n-r-s}} \sum\nolimits^*_{\substack{u_1,\dots,u_{n-r} \in \mathbb{F}_q \\ v_1,\dots,v_{n-s} \in \mathbb{F}_q}} \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi\Big(\operatorname{Tr}_q \Big(\alpha \sum_{j=1}^{n-r} u_j \rho_j + \alpha^{-1} b \sum_{k=1}^{n-s} v_k \vartheta_k\Big)\Big), \tag{4.3}$$

where Σ^* means that $u_1 = \cdots = u_{n-r} = v_1 = \cdots = v_{n-s} = 0$ is excluded from the summation. Using the Weil bound of Kloosterman sums

$$\Big| \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi(\operatorname{Tr}_q(\alpha\lambda + \alpha^{-1}\mu)) \Big| < 2q^{n/2},$$

which holds if at least one of $\lambda, \mu \in \mathbb{F}_{q^n}$ is nonzero [14, Theorem 11.11], we conclude the proof. □

The lower bound

$$N_{F,G}(b) > \frac{q^n - 1}{q^{2n-r-s}} - 2q^{n/2} > q^{r+s-n} - 2q^{n/2} - 1$$

implied by Theorem 4.1 is nontrivial if $r+s > 3n/2$ and $q \ge 5$. We next show that on average a weaker condition $r+s > 4n/3$ suffices. Namely, we now estimate

$$R_{F,G} = \sum_{b \in \mathbb{F}_{q^n}^*} \left| N_{F,G}(b) - \frac{q^n - 1}{q^{2n-r-s}} \right|^2 .$$

Theorem 4.2. *We have*

$$R_{F,G} < 3q^{n+\min(r,s)}$$

where $r = \deg F$ *and* $s = \deg G$.

Proof. Without loss of generality, we assume $s \le r$.

Using (4.3), we derive

$$R_{F,G} \le \frac{1}{q^{4n-2r-2s}}$$
$$\times \sum_{b \in \mathbb{F}_{q^n}^*} \Bigg(\sideset{}{^*}\sum_{\substack{u_1,\ldots,u_{n-r} \in \mathbb{F}_q \\ v_1,\ldots,v_{n-s} \in \mathbb{F}_q}} \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi\Big(\mathrm{Tr}_q \Big(\alpha \sum_{j=1}^{n-r} u_j \rho_j + \alpha^{-1} b \sum_{k=1}^{n-s} v_k \vartheta_k \Big)\Big)\Bigg)^2 .$$

Extending the outer summation over all $b \in \mathbb{F}_{q^n}$, squaring out and changing the order of summation, we obtain

$$R_{F,G} \le \frac{1}{q^{4n-2r-2s}}$$
$$\times \sideset{}{^*}\sum_{\substack{u_1,\ldots,u_{n-r} \in \mathbb{F}_q \\ v_1,\ldots,v_{n-s} \in \mathbb{F}_q}} \sideset{}{^*}\sum_{\substack{x_1,\ldots,x_{n-r} \in \mathbb{F}_q \\ y_1,\ldots,y_{n-s} \in \mathbb{F}_q}} \sum_{\alpha,\beta \in \mathbb{F}_{q^n}^*} \chi\Big(\mathrm{Tr}_q \Big(\alpha \sum_{j=1}^{n-r} u_j \rho_j + \beta \sum_{j=1}^{n-r} x_j \rho_j \Big)\Big)$$
$$\times \sum_{b \in \mathbb{F}_{q^n}} \chi\Big(\mathrm{Tr}_q \Big(b \Big(\alpha^{-1} \sum_{k=1}^{n-s} v_k \vartheta_k + \beta^{-1} \sum_{k=1}^{n-s} y_k \vartheta_k \Big)\Big)\Big).$$

The sum over b vanishes unless

$$\alpha^{-1} \sum_{k=1}^{n-s} v_k \vartheta_k + \beta^{-1} \sum_{k=1}^{n-s} y_k \vartheta_k = 0,$$

or, equivalently

$$\alpha \sum_{k=1}^{n-s} y_k \vartheta_k + \beta \sum_{k=1}^{n-s} v_k \vartheta_k = 0, \tag{4.4}$$

in which case it equals q^n.

If $v_1 = \cdots = v_{n-s} = 0$ then (4.4) implies that $y_1 = \cdots = y_{n-s} = 0$ (in which case (4.4) obviously holds for any α and β). Therefore at least one of $u_1, \ldots, u_{n-r}$ and at least one of $x_1, \ldots, x_{n-r}$ is nonzero, whence

$$\sum_{j=1}^{n-r} u_j \rho_j \neq 0 \quad \text{and} \quad \sum_{j=1}^{n-r} x_j \rho_j \neq 0.$$

This implies that

$$\sum_{\alpha,\beta \in \mathbb{F}_{q^n}^*} \chi\Big(\mathrm{Tr}_q \Big(\alpha \sum_{j=1}^{n-r} u_j \rho_j + \beta \sum_{j=1}^{n-r} x_j \rho_j\Big)\Big)$$
$$= \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi\Big(\mathrm{Tr}_q \Big(\alpha \sum_{j=1}^{n-r} u_j \rho_j\Big)\Big) \sum_{\beta \in \mathbb{F}_{q^n}^*} \chi\Big(\mathrm{Tr}_q \Big(\beta \sum_{j=1}^{n-r} x_j \rho_j\Big)\Big) = 1.$$

Hence the total contribution from such terms with $v_1 = \cdots = v_{n-s} = y_1 = \cdots = y_{n-s} = 0$ equals

$$\frac{1}{q^{4n-2r-2s}} q^n (q^{n-r} - 1)^2 \leq \frac{1}{q^{4n-2r-2s}} q^n q^{2(n-r)} = q^{2s-n}. \tag{4.5}$$

Now we note that if $\lambda, \mu \in \mathbb{F}_{q^n}$ and $\sigma, \tau \in \mathbb{F}_{q^n}^*$ are such that $\lambda\tau \neq \mu\sigma$ then

$$\sum_{\substack{\alpha,\beta \in \mathbb{F}_{q^n}^* \\ \alpha\sigma + \beta\tau = 0}} \chi(\mathrm{Tr}_q(\alpha\lambda + \beta\mu)) = \sum_{\alpha \in \mathbb{F}_{q^n}^*} \chi(\mathrm{Tr}_q(\alpha(\lambda - \mu\sigma\tau^{-1})))$$
$$= \sum_{\alpha \in \mathbb{F}_{q^n}} \chi(\mathrm{Tr}_q(\alpha(\lambda - \mu\sigma\tau^{-1}))) - 1 = -1.$$

Furthermore, for $\lambda\tau = \mu\sigma$, we can use the trivial bound

$$\Big| \sum_{\substack{\alpha,\beta \in \mathbb{F}_{q^n}^* \\ \alpha\sigma + \beta\tau = 0}} \chi(\mathrm{Tr}_q(\alpha\lambda + \beta\mu)) \Big| \leq q^n.$$

If at least one of $v_1, \ldots, v_{n-s}$ is nonzero, then (4.4) implies that at least one of $y_1, \ldots, y_{n-s}$ is nonzero as well. Thus we conclude that the total contribution from such terms does not exceed

$$\frac{1}{q^{4n-2r-2s}} (q^{2n} T + q^n q^{2n-2r} q^{2n-2s}) = \frac{1}{q^{2n-2r-2s}} T + q^n,$$

where T is the number of solutions to the equation

$$\sum_{j=1}^{n-r} u_j \rho_j \sum_{k=1}^{n-s} v_k \vartheta_k = \sum_{j=1}^{n-r} x_j \rho_j \sum_{k=1}^{n-s} y_k \vartheta_k.$$

Clearly

$$T \le q^{2(n-r)} q^{n-s} = q^{3n-2r-s}$$

(and also $T \le q^{3n-r-2s}$). Hence the total contribution from the terms such that at least one of $u_1, \dots, u_{n-r}$ and at least one of $x_1, \dots, x_{n-r}$ is nonzero is at most

$$\frac{1}{q^{2n-2r-2s}} q^{3n-2r-s} + q^n = q^{n+s} + q^n. \tag{4.6}$$

Combining (4.5) and (4.6), we obtain

$$R_{F,G} < q^{2s-n} + q^{n+s} + q^n$$

which concludes the proof. □

Clearly, we can always assume that $s \le r$. In the case we see that the bound of Theorem 4.2 is nontrivial if $2r + s > 2n$ and $q \ge 4$. In particular, this holds if $r + s > 4n/3$ and $q \ge 4$.

5 Bounds on the genus of the Weil descent curve

The results of Section 4 combined with (2.4) allow us to achieve a small genus curve for the Weil descent when $F = G$ and of appropriate degree r. Namely, if $q \to \infty$ we need $r > 3n/4$ and $r > 2n/3$ for Theorems 4.1 and 4.2, respectively. If q is fixed then we need $r - 3n/4 \to \infty$ and $r - 2n/3 \to \infty$ for Theorems 4.1 and 4.2, respectively.

More precisely, for an integer t with $0 < t < n$ and an integer n we denote by $r(t; n)$ the smallest $r \ge t$ for which $X^n + 1$ has a divisor $H(X) \in \mathbb{F}_2[X]$ of degree r. For example, the choices $t = \lfloor 3n/4 \rfloor + 1$ and $t = \lfloor 2n/3 \rfloor + 1$ are our principal interest (if $q \to \infty$), and so are $t = \lceil (3/4 + \varepsilon)n \rceil$ and $t = \lceil (2/3 + \varepsilon)n \rceil$ for some fixed small $\varepsilon > 0$ (if q is fixed).

First we need to study the possible factorization of cyclotomic polynomials

$$\Phi_d(X) = \prod_{\substack{j=1 \\ \gcd(j,d)=1}}^{d} (X - e^{2\pi \imath j/d}) \in \mathbb{Z}[X]$$

where $\iota = \sqrt{-1}$. Clearly Φ_d is of degree $\varphi(d)$, where $\varphi(d)$ denotes Euler's function, and is monic. In $\mathbb{Z}[X]$, Φ_d is irreducible, so it does not factor. But it may be considered as a polynomial in $\mathbb{F}_2[X]$ of degree $\varphi(d)$, and it may factor there.

Let $\lambda(d)$ denote Carmichael's function (so $\lambda(d)$ is the group exponent of $(\mathbb{Z}/d\mathbb{Z})^*$). Thus, for a prime power p^k we have

$$\lambda(p^k) = \begin{cases} p^{k-1}(p-1), & \text{if } p \geq 3 \text{ or } k \leq 2; \\ 2^{k-2}, & \text{if } p = 2 \text{ and } k \geq 3; \end{cases}$$

and finally,

$$\lambda(d) = \operatorname{lcm}(\lambda(p_1^{k_1}), \ldots, \lambda(p_\nu^{k_\nu})),$$

where $d = p_1^{k_1} \cdots p_\nu^{k_\nu}$ is the canonical prime number factorization of d.

Furthermore, for each odd number d, let $l(d)$ be the order of 2 in $(\mathbb{Z}/d\mathbb{Z})^*$, so that

$$l(d) \mid \lambda(d) \mid \varphi(d).$$

We now state a consequence of the normal order of Carmichael's function, see [6, Theorem 2].

Lemma 5.1. *Let $\mathbb{N}_0$ denote the set of natural numbers n for which*

$$\lambda(n) \leq \frac{n}{(\log n)^{\log\log\log n}}.$$

Then $\mathbb{N}_0$ has asymptotic density 1.

We now prove the following elementary result.

Lemma 5.2. *For a natural number d, write $d = 2^k d_0$ where d_0 is odd. Then in $\mathbb{F}_2[X]$ we have*

$$\Phi_d = (f_{d_0,1} f_{d_0,2} \cdots f_{d_0,h})^{\varphi(2^k)},$$

where each $f_{d_0,i}$ is irreducible of degree $l(d_0)$, they are distinct, and $h = \varphi(d_0)/l(d_0)$.

Proof. If $k > 0$, then the cyclotomic polynomial $\Phi_d(X)$ in $\mathbb{Z}[X]$ satisfies

$$\Phi_{2^k d_0}(X) = \Phi_{2d_0}(X^{2^{k-1}}) = \frac{\Phi_{d_0}(X^{2^k})}{\Phi_{d_0}(X^{2^{k-1}})},$$

so that in $\mathbb{F}_2[X]$, we have $\Phi_d(X) = \Phi_{d_0}(X)^{2^{k-1}} = \Phi_{d_0}(X)^{\varphi(2^k)}$, an identity that continues to hold when $k = 0$. Thus, in the sequel we may assume that $d = d_0$ is odd.

Since $X^d + 1$ is coprime to dX^{d-1} in $\mathbb{F}_2[X]$ when d is odd, it follows that $X^d + 1$ is squarefree. But $\Phi_d(X) \mid X^d + 1$, so Φ_d is squarefree too. Thus, the irreducible factors $f_{d,i}$ of Φ_d are distinct. Let $\zeta_d \in \overline{\mathbb{F}}_2$ have multiplicative order d. Thus, ζ_d is a primitive dth root of 1. Note that $\Phi_d(\zeta_d) = 0$, so that the minimal polynomial of ζ_d divides Φ_d. Hence, this mimimal polynomial must be one of the factors $f_{d,i}$. Now the degree l of this polynomial is the least postive integer with $\zeta_d^{2^l-1} = 1$ (actually this is true for any nonzero member of $\overline{\mathbb{F}}_2$). But since the multiplicative order of ζ_d is d, it follows that l is the least positive integer with $2^l \equiv 1 \pmod{d}$, that is, $l = l(d)$. Since this is true for each primitive dth root of 1, it follows that each $f_{d,i}$ has degree $l(d)$. This completes the proof. □

We now see from Lemma 5.2 that if n is prime and 2 is a primitive root modulo n then $X^n + 1 = (X + 1)\Phi_n(X)$ where $\Phi_n(X)$ is irreducible over $\mathbb{F}_2$. So, in this case $r(t;n) = n - 1$ for any nontrivial value of t. However, we now show that $r(t;n) = t + o(n)$ for every $t \in [1,n]$ as $n \to \infty$ through a certain set of numbers of asymptotic density 1.

We start with the following useful result.

Lemma 5.3. *For each natural number n and each integer $t \in [1,n]$, we have $r(t;n) < t + \lambda(n)$.*

Proof. Since $X^n + 1 = \prod_{d \mid n} \Phi_d(X)$, it follows from Lemma 5.2 that each irreducible factor of $X^n + 1$ in $\mathbb{F}_2[X]$ has degree at most $\lambda(n)$. Let $H(X)$ be a divisor of $X^n + 1$ in $\mathbb{F}_2[X]$ with degree as small as possible but with $\deg H \geq t$. If $\deg H \geq t + \lambda(n)$, then removing any irreducible factor from H creates a polynomial H_0 of smaller degree but still at least t. This contradicts the choice of H, so $\deg H < t + \lambda(n)$. □

We now immediately derive the following from Lemma 5.3.

Corollary 5.4. *For the set $\mathbb{N}_0$ from Lemma 5.1, if $n \in \mathbb{N}_0$ and $t \in [1,n]$, we have*

$$t \leq r(t;n) < t + \frac{n}{(\log n)^{\log\log\log n}}.$$

We are now ready to get our main results. First of all, we note that Lemma 5.1 and Corollary 5.4 yield:

Theorem 5.5. *There is a set of asymptotic density 1 such that as $n \to \infty$ through this set, we have $t \leq r(t;n) \leq t + o(n)$ for each $t \in [1,n]$.*

Now recalling (2.4) and combining Theorems 4.1 and 4.2 with Theorem 5.5 we derive:

Theorem 5.6. *There is a set of asymptotic density* 1 *such that as $n \to \infty$ through this set, the Weil descent on the elliptic curve* (2.2) *with* $\mathrm{Tr}_2(a) = 0$ *leads to a curve of genus*

- $g \le 2^{3n/4+o(n)}$ *for all coefficients* $b \in \mathbb{F}_{q^n}$*,*
- $g \le 2^{2n/3+o(n)}$ *for all but* $o(q^n)$ *coefficients* $b \in \mathbb{F}_{q^n}$*.*

Proof. To prove the estimate for all $b \in \mathbb{F}_{q^n}$ we take $t = \lceil 3n/4 + \log n \rceil$. Let $r = r(t; n)$ and let $H(X) \in \mathbb{F}_2[X]$ be the corresponding polynomial of degree r. Taking $F = G = H$ and applying Theorem 4.1 we obtain that $N_{F,G}(b) > 0$ for any $b \in \mathbb{F}_{q^n}$. Thus (2.4) and Theorem 5.5 imply the desired estimate on the genus.

To prove the estimate for almost all $b \in \mathbb{F}_{q^n}$ we take $t = \lceil 2n/3 + \log n \rceil$. We also note that if the polynomials $F = G$ are of degree $r = s > \lceil 2n/3 + \log n \rceil$ then Theorem 4.2 implies that the number L of $b \in \mathbb{F}_{q^n}$ with $N_{F,G}(b) = 0$ satisfies

$$L \left(\frac{q^n - 1}{q^{2n-2r}} \right)^2 \le R_{F,G} < 3q^{n+r}$$

thus $L = O(q^{2n-3r}) = o(q^n)$. For the remaining $b \in \mathbb{F}_{q^n}$, we now proceed as in the previous case. □

The next result establishes a lower bound for the genus that holds for most curves.

Theorem 5.7. *For all but* $o(q^n)$ *coefficients* $b \in \mathbb{F}_{q^n}$*, the Weil descent on the elliptic curve* (2.2) *leads to a curve of genus* $g \ge 2^{n/2+o(n)}$ *as* $n \to \infty$*.*

Proof. Clearly a polynomial $h \in \mathbb{F}_2[X]$ of degree t has at most $2^{o(t)}$ distinct polynomial divisors over $\mathbb{F}_2$ as $t \to \infty$. Therefore,

$$\mathrm{lcm}(\mathrm{Ord}_\alpha, \mathrm{Ord}_\beta) = h$$

for at most

$$\sum_{\substack{f \mid h \\ g \mid h}} q^{\deg f + \deg g} = \Big(\sum_{f \mid h} q^{\deg f} \Big)^2 \le q^{2t+o(t)}$$

pairs (α, β) of elements $\alpha, \beta \in \mathbb{F}_{q^n}^2$. Thus the total number of such pairs, which correspond to at least one polynomial $h \mid X^n - 1$ of degree $t \le T$, and therefore the total number of distinct values of $b = (\alpha\beta)^2$, is at most $q^{2T+o(T)}$. Therefore for any fixed $\varepsilon > 0$, $T = \lfloor (1-2\varepsilon)n/2 \rfloor$ and sufficiently large n, we have at most

$$q^{(1-2\varepsilon)n/2+o(n)} \le q^{(1-\varepsilon)n/2}$$

values of $b \in \mathbb{F}_{q^n}$, which admit a representation $b = (\alpha\beta)^2$ with

$$\deg \operatorname{lcm}(\mathrm{Ord}_\alpha, \mathrm{Ord}_\beta) \le T.$$

For the remaining values of b, recalling (2.4) we see that the Weil descent on the elliptic curve (2.2) leads to a curve of genus $g > 2^T$. Since ε is arbitrary, we conclude the proof. □

It is also interesting to estimate the number of coefficients b for which the genus is small enough to enable the Weil descent attack. It is shown by Hess [12, Lemma VIII.6] that for any constant $A > 0$, and all but at most $q^{4A\log_2 n+O(1)}$ coefficients $b \in \mathbb{F}_{q^n}$, the Weil descent on the elliptic curve (2.2) leads to a curve of genus $g \ge n^A$ as $n \to \infty$. Taking $A = 4$, we see that the gGHS attack can be useful for at most $q^{16\log_2 n+O(1)}$ elliptic curves over $\mathbb{F}_{q^n}$ as $n \to \infty$. As first observed by Galbraith, Hess and Smart [8], the class of vulnerable elliptic curves can potentially be enlarged by mapping the ECDLP for a given elliptic curve $\widetilde{E}/\mathbb{F}_{q^n}$ to an isogenous elliptic curve $E/\mathbb{F}_{q^n}$ (if one exists) for which the gGHS attack is effective. The attack on $\widetilde{E}$ will also be effective provided that E and an isogeny from $\widetilde{E}$ to E can be found in less time than it takes to mount the gGHS attack on E. Since an isogeny class contains at most $q^{n/2+O(\log n)}$ elliptic curves [15], the number of vulnerable curves is at most $q^{n/2+O(\log n)}$; this is negligible compared to the number $2(q^n - 1)$ of elliptic curves over $\mathbb{F}_{q^n}$.

We remark that in order to keep our argument technically simple, we assumed the condition $\mathrm{Tr}_2(a) = 0$ in Theorem 5.6 since in this case the condition (2.3) does not apply. This however can be accommodated in our approach at the cost of only minor technical complications. First, we define $N^*_{F,G}(b)$ exactly as $N_{F,G}(b)$ with the additional request that $\mathrm{Ord}_\alpha = F$ and $\mathrm{Ord}_\beta = G$ (in the definition of $N_{F,G}(b)$ we only have $\mathrm{Ord}_\alpha \mid F$ and $\mathrm{Ord}_\beta \mid G$). Then using the inclusion-exclusion principle, one can derive from Theorems 4.1 and 4.2 analogous results for $N^*_{F,G}(b)$.

Second, the results of Lemma 5.3 and Corollary 5.4 can easily be extended to the function $r^*(n,t)$ which is defined as the smallest $r \ge t$ for which $(X^n + 1)/(X + 1)^{2^\nu}$ has a divisor $f(X) \in \mathbb{F}_2[X]$ of degree $r - 2^\nu$, where 2^ν is the largest power of 2 dividing n. Note that the condition $(X + 1)^{2^\nu} \mid \mathrm{Ord}_\alpha$ guarantees that $\mathrm{Tr}_q(\alpha) \neq 0$ and we easily obtain an analogue of Theorem 5.6 without any extra condition on $\mathrm{Tr}_2(a)$.

We note that it would be very interesting to obtain a version of Theorem 5.6 which gives a nontrivial lower bound on the number of b which lead to curves of genus $g \leq n^A$ (as a counterpart to the aforementioned result of Hess [12, Lemma VIII.6]). Unfortunately our techniques do not seem to apply to this question.

Acknowledgments. The author would like to thank the anonymous referees for their valuable comments.

Bibliography

[1] R. Avanzi, H. Cohen, C. Doche, G. Frey, T. Lange, K. Nguyen and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, CRC Press, 2005.

[2] I. Blake, G. Seroussi and N. Smart, *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005.

[3] C. Diem, On the discrete logarithm problem in elliptic curves, *Compositio Mathematica*, to appear.

[4] C. Diem, On the discrete logarithm problem in class groups of curves, *Mathematics of Computation*, to appear.

[5] A. Enge and P. Gaudry, An $L(1/3+\varepsilon)$ algorithm for the discrete logarithm problem for low degree curves, *Advances in Cryptology – EUROCRYPT 2007*, Lecture Notes in Computer Science, **4515** (2007), 379–393.

[6] P. Erdős, C. Pomerance and E. Schmutz, Carmichael's lambda function, *Acta Arithmetica*, **58** (1991), 363–385.

[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, F. Hess and N. Smart, Extending the GHS Weil descent attack, *Advances in Cryptology – EUROCRYPT 2002*, Lecture Notes in Computer Science, **2332** (2002), 29–44.

[9] P. Gaudry, An algorithm for solving the discrete log problem in hyperelliptic curves, *Advances in Cryptology – EUROCRYPT 2000*, Lecture Notes in Computer Science, **1807** (2000), 19–34.

[10] P. Gaudry, F. Hess and N. Smart, Constructive and destructive facets of Weil descent on elliptic curves, *Journal of Cryptology*, **15** (2002), 19–46.

[11] F. Hess, Generalising the GHS attack on the elliptic curve discrete logarithm problem, *LMS Journal of Computation and Mathematics*, **7** (2004), 167–192.

[12] F. Hess, Weil descent attacks, *Advances in Elliptic Curve Cryptography*, Cambridge University Press, 2005, 151–180.

[13] F. Hess, Computing relations in divisor class groups of algebraic curves over finite fields, *Preprint*, 2009.

[14] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, American Mathematical Society, 2004.

[15] H. Lenstra, Factoring integers with elliptic curves, *Annals of Mathematics*, **126** (1987), 649–673.

[16] R. Lidl and H. Niederreiter, *Introduction to Finite Fields and Their Applications*, Cambridge University Press, 1994.

[17] M. Maurer, A. Menezes and E. Teske, Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree, *LMS Journal of Computation and Mathematics*, **5** (2002), 127–174.

[18] 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.

[19] A. Menezes and E. Teske, Cryptographic implications of Hess' generalized GHS attack, *Applicable Algebra in Engineering, Communication and Computing*, **16** (2006), 439–460.

[20] A. Menezes, E. Teske and A. Weng, Weak fields for ECC, *Topics in Cryptology – CT-RSA 2004*, Lecture Notes in Computer Science, **2964** (2004), 366–386.

[21] J. Pollard, Monte Carlo methods for index computation mod p, *Mathematics of Computation*, **32** (1978), 918–924.

[22] 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.

[23] 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.

[24] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, Berlin, 1995.

[25] N. Smart, The discrete logarithm problem on elliptic curves of trace one, *Journal of Cryptology*, **12** (1999), 193–196.

Received January 27, 2010; revised May 12, 2010.

Author information

Koray Karabina, Department of Combinatorics & Optimization, University of Waterloo, Canada.
E-mail: kkarabin@uwaterloo.ca

Alfred Menezes, Department of Combinatorics & Optimization, University of Waterloo, Canada.
E-mail: ajmeneze@uwaterloo.ca

Carl Pomerance, Mathematics Department, Dartmouth College, USA.
E-mail: carl.pomerance@dartmouth.edu

Igor E. Shparlinski, Department of Computing, Macquarie University, Australia.
E-mail: igor.shparlinski@mq.edu.au