Weak Fields for ECC

Alfred Menezes[1], Edlyn Teske[1], and Annegret Weng[2]

[1] {ajmeneze,eteske}@uwaterloo,ca, University of Waterloo, Canada
[2] weng@exp-math.uni-essen.de, University of Essen, Germany

Abstract. We demonstrate that some finite fields, including $\mathbb{F}_{2^{210}}$, are weak for elliptic curve cryptography in the sense that any instance of the elliptic curve discrete logarithm problem for *any* elliptic curve over these fields can be solved in significantly less time than it takes Pollard's rho method to solve the hardest instances. We discuss the implications of our observations to elliptic curve cryptography, and list some open problems.

1 Introduction

Elliptic curve cryptography (ECC) is being standardized by accredited standards organizations and governments around the world. The security of elliptic curve systems is based on the hardness of the *elliptic curve discrete logarithm problem* (ECDLP): given an elliptic curve E defined over a finite field $\mathbb{F}_q$, a point $P \in E(\mathbb{F}_q)$ of order r, and a second point $Q \in \langle P \rangle$, determine the integer $l \in [0, r-1]$ such that $Q = lP$. Elliptic curve systems are especially attractive because Pollard's rho method [33], the best algorithm known for the solving the general ECDLP, has a fully-exponential expected running time of $\sqrt{\pi r}/2$ point additions.

For a given underlying field $\mathbb{F}_q$, maximum resistance to Pollard's rho method can be attained by selecting an elliptic curve E for which r is prime and is as large as possible. The most favourable situation arises when $\#E(\mathbb{F}_q)$ is prime or almost prime, i.e., $\#E(\mathbb{F}_q) = dr$, where r is prime and the co-factor d is small (e.g., $d \in \{1, 2, 3, 4\}$). In this case, since $\#E(\mathbb{F}_q)$ lies in the Hasse interval $[(\sqrt{q}-1)^2, (\sqrt{q}+1)^2]$, we have $r \approx q$ and we say that the elliptic curve has a security level of $\frac{1}{2}\log_2 q$ bits.

Some ECC standards recommend or mandate a small selection of finite fields and elliptic curves. Among these, the most influential has been the FIPS 186-2 standard [8] for the elliptic curve digital signature algorithm (ECDSA) which recommends five prime fields $\mathbb{F}_p$ for specified primes p of bitlengths 192, 224, 256, 384, and 512, and the five characteristic two finite fields $\mathbb{F}_{2^{163}}$, $\mathbb{F}_{2^{233}}$, $\mathbb{F}_{2^{283}}$, $\mathbb{F}_{2^{409}}$, and $\mathbb{F}_{2^{571}}$. The recommended elliptic curves over these fields have security levels of approximately 80, 112, 128, 192, and 256 bits, which match the security levels of the SKIPJACK, Triple-DES, AES-Small, AES-Medium, and AES-Large symmetric-key encryption schemes. Fixing a small set of allowable fields has the advantages of facilitating interoperability, and permitting the optimization of hardware and software implementations by exploiting properties of the chosen fields.

It is therefore reasonable to expect that commercial deployments of ECC will converge upon a small selection of finite fields. This does not appear to be a serious limitation because of the following reasons. First, there are an enormous number of elliptic curves to choose from; more precisely, there are roughly $2q$ isomorphism classes of elliptic curves over $\mathbb{F}_q$. Second, the orders of these curves are roughly uniformly distributed over the Hasse interval in the case of prime fields, and over the even integers in the Hasse interval in the case of characteristic two finite fields. Consequently, elliptic curves of almost prime orders are plentiful and can be easily found. Finally, there are very few elliptic curves of almost prime order over a field $\mathbb{F}_q$ for which the ECDLP can be solved in subexponential (or faster) time—those that succumb to the Weil and Tate pairing attacks [12, 28], and the attack on prime-field anomalous curves [34, 35, 37]. It is easy to recognize these curves, and thus the aforementioned attacks can readily be circumvented.

Nonetheless, the possibility still remains that algorithms will subsequently be discovered for efficiently solving any instance of the ECDLP for *any* elliptic curve over a selected field. If ECC solutions employing that field were widely deployed (especially in hardware), then the consequences of such a discovery would be more drastic than if an attack were discovered on a special class of curves because a change in the underlying field would be required. Determining whether such finite fields exist is therefore an important problem in elliptic curve cryptography.

Definition 1 A finite field $\mathbb{F}_q$ is said to be *bad* for elliptic curve cryptography if the following conditions are satisfied:

1. for some elliptic curves E over $\mathbb{F}_q$, solving the ECDLP in $E(\mathbb{F}_q)$ using Pollard's rho method (and its parallelized versions [30]) is intractable using existing computer technology; and
2. algorithms are known which can feasibly solve (using existing computer technology) any ECDLP instance for any elliptic curve over $\mathbb{F}_q$.

No bad fields for ECC are presently known. The contribution of this paper is the observation that some finite fields are weak in the following sense.

Definition 2 A finite field $\mathbb{F}_q$ is said to be *weak* for elliptic curve cryptography if the following conditions are satisfied:

1. for some elliptic curves E over $\mathbb{F}_q$, solving the ECDLP in $E(\mathbb{F}_q)$ using Pollard's rho method (and its parallelized versions [30]) is intractable using existing computer technology; and
2. algorithms are known for which any ECDLP instance for any elliptic curve over $\mathbb{F}_q$ can be solved in significantly less time than it takes Pollard's rho method to solve the hardest ECDLP instances over $\mathbb{F}_q$.

While the ECDLP for elliptic curves over a weak field may in fact be intractable in general, demonstrating that a field is weak provides some evidence that the field may be bad, and therefore unsuitable for elliptic curve cryptography.

Of course our definition of a weak field is not precise since "significantly less" has not been quantified. We remark that the discovery [16, 44] of a $\sqrt{N}$-speedup of Pollard's rho method for solving the ECDLP in the group of $\mathbb{F}_{2^N}$-rational points on a Koblitz curve[1] caused some to view the security of these curves with suspicion. For Koblitz curves over $\mathbb{F}_{2^{163}}$ and $\mathbb{F}_{2^{283}}$, the speedup is by a factor of only 13 and 17, respectively. In this paper, we present reasonable arguments that the finite fields $\mathbb{F}_{2^N}$, where $N \in [185, 600]$ is divisible by 5, are weak fields for ECC. In particular, we show that the ECDLP for all elliptic curves over $\mathbb{F}_{2^{210}}$ (respectively, one-quarter of all elliptic curves over $\mathbb{F}_{2^{210}}$) can be solved 2^{13} times faster (respectively, 2^{20} times faster) than it takes Pollard's rho method to solve the hardest instances. These speedups are significantly greater than the aforementioned speedups for Koblitz curves, and moreover are applicable to *all* (respectively, one-quarter of all) elliptic curves over $\mathbb{F}_{2^{210}}$. While upto now it was believed that an elliptic curve over $\mathbb{F}_{2^{210}}$ whose group order is twice a prime offers a security level of 104 bits, our results show it can have a security level of at most 91 bits, that is, the same as a curve over $\mathbb{F}_{2^{183}}$ is able to offer. The field $\mathbb{F}_{2^{210}}$ is interesting because its arithmetic can be efficiently implemented by successive extensions, e.g., $\mathbb{F}_{2^2} \subseteq \mathbb{F}_{2^6} \subseteq \mathbb{F}_{2^{30}} \subseteq \mathbb{F}_{2^{210}}$. As another example, we show that the ECDLP for all elliptic curves over $\mathbb{F}_{2^{600}}$ can be solved about 2^{69} times faster than it takes Pollard's rho method to solve the hardest instances. Hence an elliptic curve over $\mathbb{F}_{2^{600}}$ can have a security level of at most 230 bits.

Organization. The remainder of this paper is organized as follows. In Section 2, we summarize the recent work on the Weil descent attack on the ECDLP. Our detailed arguments that the fields $\mathbb{F}_{2^N}$, where $N \in [185, 600]$ is divisible by 5, are weak are presented in Section 3. In Section 4, we examine the fields $\mathbb{F}_{2^N}$, where N is divisible by 4, for weakness. In Section 5, we further explore the special case $N = 210$. We draw our conclusions in Section 6 and list some interesting open problems.

2 Weil descent attack on the ECDLP

Frey [11] first proposed using Weil descent as a means to reduce the ECDLP in elliptic curves over finite fields $\mathbb{F}_{q^n}$ to the discrete logarithm problem in the jacobian variety of a curve of larger genus over the proper subfield $\mathbb{F}_q$. If a subexponential-time algorithm is known for the DLP for the resulting curve, then this could lead to an algorithm that solves the original ECDLP instance faster than Pollard's rho method.

Let l and n be positive integers, and let $N = ln$. 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

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

[1] A *Koblitz curve* is an elliptic curve defined over $\mathbb{F}_2$. There are two such curves: $y^2+xy = x^3+1$ and $y^2+xy = x^3+x^2+1$. These curves admit fast point multiplication algorithms (see [39]) and are therefore favoured over other curves defined over $\mathbb{F}_{2^N}$.

We assume that $\#E(K) = dr$ where d is small and r is prime, whence $r \approx q^n$. Let $b_i = \sigma^i(b)$, where $\sigma : K \to K$ is the Frobenius automorphism defined by $\alpha \mapsto \alpha^q$. The *magic number* for E relative to n is defined to be

$$m = m(b) = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, b_0^{1/2}), (1, b_1^{1/2}), \ldots, (1, b_{n-1}^{1/2})\}). \qquad (1)$$

Assume now that either n is odd, or $m(b) = n$, or $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$. Gaudry, Hess and Smart [18] showed how Weil descent can be used to reduce instances of the ECDLP in the subgroup of order r of $E(K)$ to instances of the hyperelliptic curve discrete logarithm problem (HCDLP) in a subgroup of order r of the jacobian $J_C(k)$ of a hyperelliptic curve C of genus $g = 2^{m-1} - 1$ or 2^{m-1} 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 $n-1$ hyperplanes to eventually obtain the hyperelliptic curve C from an irreducible reduced component in the intersection. The reduction algorithm, together with the fastest known algorithm for solving the HCDLP in $J_C(k)$, is called the *GHS attack* on the ECDLP.

Since subexponential-time algorithms are known for the HCDLP for large genus hyperelliptic curves [1], it is possible that the GHS attack can solve the original ECDLP instance faster than Pollard's rho method. In [29], it was shown that for all elliptic curves over $\mathbb{F}_{2^N}$ where $N \in [160, 600]$ is prime, the genus g of C is either too small (whereby the attack fails because $J_C(\mathbb{F}_2)$ is too small to yield any non-trivial information about the ECDLP in $E(\mathbb{F}_{2^N})$), or is too large ($g \geq 2^{16} - 1$, whereby the attack fails because the HCDLP in $J_C(\mathbb{F}_2)$ is intractable). In [22], the GHS attack was used to solve an instance of the ECDLP over $\mathbb{F}_{2^{124}}$ (which is infeasible to solve using Pollard's rho method) by reducing it to an instance of the HCDLP in a genus 31 hyperelliptic curve over $\mathbb{F}_{2^4}$ and solving the latter using the Enge-Gaudry algorithm [17, 7]. A convincing argument was presented that the GHS attack could also be used to solve instances of the ECDLP for a certain class of elliptic curves over $\mathbb{F}_{2^{155}}$ by reducing them to instances of the HCDLP in genus 31 hyperelliptic curves over $\mathbb{F}_{2^5}$. The effectiveness of the GHS attack for elliptic curves over $\mathbb{F}_{2^N}$ where $N \in [100, 600]$ is composite was extensively analyzed in [27], where the elliptic curves most susceptible were identified and enumerated. In Section 3 we examine in greater detail the effectiveness of the GHS attack on the ECDLP over fields $\mathbb{F}_{2^N}$ where N is a multiple of 5. In Section 4, we study the case where N is a multiple of 4. The special case $N = 210$ is further examined in Section 5.

3 The fields $\mathbb{F}_{2^N}$ with $N = 5l$

In this section, we argue that the fields $\mathbb{F}_{2^N}$ with $N = 5l$ are weak for ECC. We restrict our attention to $l \in [32, 160]$ (equivalently $N \in [160, 600]$), since these are the values of interest for cryptographic applications. We draw our conclusions by analyzing Pollard's rho method and the GHS attack for solving instances of the ECDLP over these fields. We emphasize that our conclusions are meaningful for practice because our analyses are exact—that is, they do not involve any asymptotics, crude approximations, or hidden constants.

3.1 Exact analysis of Pollard's rho method

The instances of the ECDLP over $\mathbb{F}_{2^N}$ most resistant to Pollard's rho method (using the random walk of Teske [40]) are for elliptic curves E that have almost prime order $\#E(\mathbb{F}_{2^N}) = 2r$ for some prime r. Since $r \approx 2^{N-1}$, Pollard's rho method has an expected running time of $\sqrt{\pi 2^{N-1}}/2 \approx 2^{(N-1)/2}$ steps, where the dominant operation in each step is an addition in $E(\mathbb{F}_{2^N})$. We note that even though the expression $\sqrt{\pi r}/2$ for the running time of Pollard's rho method is an asymptotic one (as $r \to \infty$), it has been proven under reasonable assumptions [41, Corollary 5.1] that the actual running time for any fixed value of r is within a very small constant multiple of the asymptotic time. Thus

$$T_\rho = 2^{(N-1)/2} = 2^{2.5l-0.5} \tag{2}$$

is indeed a very accurate approximation for the running time of Pollard's rho method for solving the hardest instances of the ECDLP over $\mathbb{F}_{2^N}$.

3.2 Exact analysis of the GHS attack

Let E be an elliptic curve defined over $\mathbb{F}_{2^N}$, and let $P \in E(\mathbb{F}_{2^N})$ have prime order r. The GHS attack first uses the GHS reduction to yield an explicit group homomorphism $\Phi : \langle P \rangle \to J_C(\mathbb{F}_{2^l})$, where C is a hyperelliptic curve defined over $\mathbb{F}_{2^l}$, and then uses the Enge-Gaudry index-calculus algorithm to solve the resulting HCDLP instance. For these parameters, the GHS reduction algorithm takes less than a minute on a workstation. Thus we do not include the running time of the GHS reduction in our analysis of the GHS attack.

If the coefficients of E belong to $\mathbb{F}_{2^l}$, then $\#E(\mathbb{F}_{2^l})$ divides $\#E(\mathbb{F}_{2^N})$ and hence r has bitlength at most $N - l$. In this case, Pollard's rho algorithm can solve each ECDLP instance in at most $T'_\rho = 2^{(N-l)/2}$ steps, which is significantly less than T_ρ. For example, if $(N, l) = (160, 32)$ then $T_\rho = 2^{79.5}$ and $T'_\rho = 2^{64}$, and if $(N, l) = (600, 120)$ then $T_\rho = 2^{299.5}$ and $T'_\rho = 2^{240}$. Therefore, we will henceforth assume that E is not isomorphic to an elliptic curve defined over $\mathbb{F}_{2^l}$. In particular the magic number m (defined in (1)) is not 1, and hence it follows from [29, Corollary 9] that $m = 5$. Therefore C has genus $g = 15$ or 16. In fact, the vast majority of the $2^{N+1} - 2^{l+1}$ isomorphism classes of elliptic curves defined over $\mathbb{F}_{2^N} \setminus \mathbb{F}_{2^l}$ yield a genus 16 curve.

Theorem 3 The GHS reduction yields a genus 15 hyperelliptic curve C defined over $\mathbb{F}_{2^l}$ for exactly $2^{4l+1} - 2$ isomorphism classes of elliptic curves defined over $\mathbb{F}_{2^N} \setminus \mathbb{F}_{2^l}$.

Proof. Let $q = 2^l$. Let $E : y^2 + xy = x^3 + ax^2 + b$ with $b \in \mathbb{F}_{2^N} \setminus \mathbb{F}_{2^l}$, and let $\mathrm{Ord}_b(x)$ denote the unique monic polynomial $f \in \mathbb{F}_2[x]$ of least degree such that

$f(\sigma)(b) = 0$. Let $t(x) = x^4 + x^3 + x^2 + x + 1$. Since $b \notin \mathbb{F}_{2^l}$, $\mathrm{Ord}_b(x) = x^5 - 1$ or $\mathrm{Ord}_b(x) = t(x)$. Now, by [20, Corollary 6] we have $g = 15$ if and only if $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_{2^l}}(b^{1/2}) = 0$, which is the case if and only if $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_{2^l}}(b) = 0$. On the other hand, since $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_{2^l}}(b) = t(\sigma)(b)$ it is easy to see that $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_{2^l}}(b) = 0$ if and only if $\mathrm{Ord}_b(x) \mid t(x)$, which is the case if and only if $\mathrm{Ord}_b(x) = t(x)$. By [29, Corollary 8], the latter is true for exactly $2^{4l} - 1$ elements $b \in \mathbb{F}_{2^N} \setminus \mathbb{F}_{2^l}$. □

The Enge-Gaudry algorithm [17, 7] for finding the logarithm of a divisor D_2 to the base D_1 in $J_C(\mathbb{F}_{2^l})$ has three stages. First, a smoothness bound $t \in [1, g]$ is selected and a *factor base* $\{P_1, P_2, \ldots, P_w\}$ is constructed which contains exactly one of D and $-D$ for each prime divisor D of degree less than or equal to t. In the second *relation generation* stage, a random walk is performed in the set of reduced divisors equivalent to divisors of the form $\alpha D_1 + \beta D_2$. Each t-smooth divisor encountered in this walk yields a relation $\alpha_i D_1 + \beta_i D_2 \sim R_i = \sum_j e_{ij} P_j$. After slightly more than w such relations have been generated and stored, one can find by linear algebra modulo r a non-trivial linear combination $\sum_i \gamma_i (e_{i1}, e_{i2}, \ldots, e_{iw}) = (0, 0, \ldots, 0)$. Thus $\sum_i \gamma_i R_i = 0$, and then $\log_{D_1} D_2 = -(\sum_i \gamma_i \alpha_1)/(\sum_i \gamma_i \beta_i) \bmod r$ can be easily computed.

There is a one-to-one correspondence between points in $C(\mathbb{F}_{2^l})$ and degree one divisors in $J_C(\mathbb{F}_{2^l})$. The divisor corresponding to a point $(x, y) \in C(\mathbb{F}_{2^l})$ is ramified if and only if $h(x) = 0$ where $v^2 + h(u)v = f(u)$ is the Weierstrass equation of C; otherwise the divisor splits. According to the Hasse-Weil bound, $\#C(\mathbb{F}_{2^l}) = 2^l + 1 - \gamma$, where $|\gamma| \le 2g\sqrt{2^l}$. Hence 2^l is a very good approximation for the number of degree one divisors in $J_C(\mathbb{F}_{2^l})$. We select the smoothness bound $t = 1$, and then the size of the factor base is $w \approx 2^{l-1}$. Creating the factor base takes negligible time compared to the relation generation and matrix stages, so we ignore that stage in our running time analysis.

The number of 1-smooth divisors in $J_C(\mathbb{F}_{2^l})$ is approximately $(2^l)^g/g!$ [17, Proposition 4]. In fact, the exact number can be efficiently computed.

Lemma 4 Let C be a hyperelliptic curve of genus g over $\mathbb{F}_q$, and suppose that there are A_1 split degree one divisors and B_1 ramified degree one divisors in $J_C(\mathbb{F}_q)$ (so $A_1 + B_1 = \#C(\mathbb{F}_q)$, and $w = A_1/2 + B_1$). Then the number of 1-smooth divisors in $J_C(\mathbb{F}_q)$ is

$$M(1) = \sum_{i=1}^{g} \left([x^i] \left(\frac{1+x}{1-x} \right)^{A_1/2} (1+x)^{B_1} \right),$$

where [ ] denotes the coefficient operator.

Proof. Similar to the proof of Lemma 2 in [22]. □

Now, $A_1 \in [2^l + 1 - 2g\sqrt{2^l}, 2^l + 1 + 2g\sqrt{2^l}]$, and $B_1 \in [0, g]$. Using either the maximum possible values for A_1 and B_1, or the minimum values for A_1 and B_1, we verified that $M(1) \approx (2^l)^g/g!$ is indeed a very good approximation for each $l \in [32, 120]$. By Weil's theorem, the size of $J_C(\mathbb{F}_{2^l})$ satisfies

$$(\sqrt{2^l} - 1)^{2g} \le \#J_C(\mathbb{F}_{2^l}) \le (\sqrt{2^l} + 1)^{2g}.$$

Thus $\#J_C(\mathbb{F}_{2^l}) \approx 2^{lg}$ is a very good approximation when $l \in [32, 120]$. Hence the expected number of random walk steps before w relations are obtained is

$$T_1 = w \cdot \#J_C(\mathbb{F}_{2^l})/M(1) \approx 2^{l-1}g!.$$

For $g = 16$, we have

$$T_1 \approx 2^{l+43}. \tag{3}$$

The two dominant operations in a random walk step are an addition in $J_C(\mathbb{F}_{2^l})$ and a smoothness testing. A polynomial $a(u)$ can be tested for 1-smoothness by first removing repeated factors (by performing a squarefree factorization) and then checking whether the resulting polynomial divides $u^{2^l} - u$. If $a(u)$ is found to be 1-smooth, then it can be factored using the Cantor-Zassenhaus algorithm [5]. We ignore the running time of the factorization step in our estimates because 1-smooth divisors are encountered relatively infrequently—once every $g! = 16! \approx 2^{44}$ random walk steps.

The system of linear equations has dimension slightly more than w and about g non-zero coefficients per equation. It can be solved using Lanczos's algorithm [6], whose running time is closely approximated by

$$T_2 = gw^2$$

arithmetic operations modulo r. We thus have

$$T_2 \approx 2^{2l+2}. \tag{4}$$

3.3 Comparisons

In order to compare the cost of Pollard's rho method for solving the ECDLP in $E(\mathbb{F}_{2^N})$ with the cost of the Enge-Gaudry algorithm for solving the HCDLP in $J_C(\mathbb{F}_{2^l})$, we need to estimate the relative cost of the basic operations in these algorithms. Let c_E denote the time to perform an elliptic curve addition in $E(\mathbb{F}_{2^N})$, c_J the time to perform an addition in $J_C(\mathbb{F}_{2^l})$ (where C has genus 16), c_S the time to test whether a monic polynomial $a \in \mathbb{F}_{2^l}[u]$ of degree 16 is 1-smooth, and c_r the time to perform a multiplication modulo r. Then the expected cost of Pollard's rho method is

$$R_\rho \approx c_E T_\rho = c_E 2^{2.5l-0.5},$$

the expected cost of the random walk stage of the Enge-Gaudry algorithm is

$$R_1 \approx (c_J + c_S)T_1 = (c_J + c_S)2^{l+43},$$

and the expected cost of the matrix stage of the Enge-Gaudry algorithm is

$$R_2 \approx c_r T_2 = c_r 2^{2l+2}. \tag{5}$$

A deficiency in the above comparison is that it only considers the total time taken, and not other scarce resources consumed such as memory, number or processors, and communications between processors. Pollard's rho method can be effectively parallelized (see [30]) so that its expected running time on a network of S processors is T_ρ/S steps. Moreover, the processors do not communicate with each other, and only occasionally transmit data to a central server. The amount of data stored at the server can be controlled without any noticeable impact on the running time (see [25]). Thus time is the only scarce resource consumed by (parallelized) Pollard's rho method.

The relation generation stage in the Enge-Gaudry algorithm can also be effectively parallelized with a speedup that is linear in the number of processors employed, and where the processors do not communicate with each other and only occasionally transmit data to a central server. However, is not known whether the matrix stage can be parallelized in this way. Moreover, the matrix may have large storage requirements. Thus, in practice, the matrix stage may be the bottleneck in an application of the Enge-Gaudry algorithm. Note, however, that Bernstein [3] and Wiener [43] have recently shown that the full cost[2] of solving a D-dimensional system of sparse linear equations over $\mathbb{F}_2$ can be reduced from $D^{3+o(1)}$ to $D^{7/3+o(1)}$. Consequently, we are of the opinion that our comparisons of Pollard's rho method and the Enge-Gaudry algorithm that only consider running times are adequate and meaningful for determining the effectiveness of the GHS attack on elliptic curve cryptographic schemes. This reasoning is more sound when the time cost c_rT_2 is significantly less than c_ET_ρ.

To complete the comparisons, we need relative estimates for c_E, c_J, c_S and c_r. When mixed affine-projective coordinates are employed, an elliptic curve operation in $E(\mathbb{F}_{2^N})$ requires 8 multiplications in $\mathbb{F}_{2^N}$. Thus $c_E \approx 8c_N$, where c_N is the time to perform a multiplication in $\mathbb{F}_{2^N}$, and we have

$$R_\rho \approx c_N 2^{2.5(l+1)}. \tag{6}$$

The dominant computation in smoothness testing is the evaluation of $u^{2^l} \bmod a$, where a is a monic polynomial of degree (at most) 16.[3] First, one iteratively computes and stores $u^{2i} \bmod a$ for $9 \le i \le 15$; this can be done with 224 multiplications in $\mathbb{F}_{2^l}$. Then, one can compute $u^{2^i} \bmod a$ for $5 \le i \le l$ by successive squarings; this can be done with $128(l-4)$ multiplications in $\mathbb{F}_{2^l}$. Thus $c_S = (128l - 288)c_l$, where c_l is the time to perform a multiplication in $\mathbb{F}_{2^l}$.

The fastest algorithm known for performing the jacobian arithmetic in a genus 16 hyperelliptic curve appears to be NUCOMP [23].[4] The precise operation count of NUCOMP has not been worked out. However, Jacobson [21] has reported that the cost c_J of a jacobian addition using NUCOMP is less than the

[2] The *full cost* of an algorithm is its running time multiplied by the number of processors employed.

[3] In practice, the squarefree factorization may not be performed. In that case, Gaudry's algorithm only considers 1-smooth divisors the points in whose supports all have coefficient 1. This does not significantly affect the expected number of random walk steps.

[4] Experiments carried out by Jacobson [21] indicate that NUCOMP is faster than Cantor's algorithm and its variants [4, 32] for hyperelliptic curves of genus ≥ 7.

cost c_S of computing $u^{2^l} \bmod a$. For example, he reports that $c_S \approx 2.3c_J$ when $l = 37$. The ratio c_S/c_J grows with l because the number of $\mathbb{F}_{2^l}$-multiplications for smoothness testing increases with l, while the number of $\mathbb{F}_{2^l}$-multiplications for jacobian addition is independent of l. Thus the approximation $R_1 \approx c_S T_1$ is justified, and hence

$$R_1 \approx (128l - 288)2^{l+43}c_l. \tag{7}$$

Finally, we need to estimate the relative costs c_N, c_l and c_r of a multiplication in $\mathbb{F}_{2^N}$, $\mathbb{F}_{2^l}$, and modulo r, respectively. We use the relative timings on a Pentium II 400 MHz reported by Hankerson [19] for his optimized implementation of multiplication in $\mathbb{F}_{2^N}$ and $\mathbb{F}_{2^l}$ using the methods of [26], and for integer multiplication with Barrett reduction [2]. Table 1 shows these costs for some selected fields.

N	l	R_ρ/c_N	R_1/c_l	R_2/c_r	c_N	c_l	c_r	R_ρ	R_1	R_2
160	32	$2^{82.5}$	2^{87}	2^{66}	7.7	1.0	5.8	$2^{85.5}$	2^{87}	2^{69}
185	37	2^{95}	2^{92}	2^{76}	7.9	1.0	5.8	2^{98}	2^{92}	2^{79}
210	42	$2^{107.5}$	2^{97}	2^{86}	10.3	1.0	8.0	$2^{110.5}$	2^{97}	2^{89}
255	51	2^{130}	2^{107}	2^{104}	11.0	1.0	7.7	2^{133}	2^{107}	2^{107}
385	77	2^{195}	2^{133}	2^{156}	15.0	1.0	9.4	2^{199}	2^{133}	2^{160}
515	103	2^{260}	2^{160}	2^{208}	15.3	1.0	11.1	2^{264}	2^{160}	2^{212}
600	120	$2^{302.5}$	2^{177}	2^{242}	17.7	1.0	12.5	$2^{306.5}$	2^{177}	2^{246}

Table 1. Time estimates for Pollard's rho method for solving an ECDLP instance in $E(\mathbb{F}_{2^N})$, and for the relation generation and matrix stages of the Enge-Gaudry algorithm for solving an HCDLP instance in $J_C(\mathbb{F}_{2^l})$ where C is a genus 16 hyperelliptic curve. c_N, c_l and c_r are the relative times for a multiplication in $\mathbb{F}_{2^N}$, $\mathbb{F}_{2^l}$, and modulo an N-bit prime, respectively. The estimates for R_ρ, R_1, R_2 were derived using formulas (6), (7), (5), respectively. In columns 3, 4, 5, the time units are $\mathbb{F}_{2^N}$-multiplications, $\mathbb{F}_{2^l}$-multiplications, and modulo-r multiplications, respectively. In columns 9, 10, 11, the time unit is an $\mathbb{F}_{2^l}$-multiplication.

Remark 5 (*miscellaneous notes on Table 1*)

(i) The relative times for c_N, c_l and c_r are, of course, dependent on the choice of algorithms, platform, and implementation. Nevertheless, we do not expect that these relative times will differ by large factors (e.g., greater than 4) from the "correct" times. For example, the ratios c_N/c_l for the seven (N, l) pairs of Table 1 that we obtained using the routines for field arithmetic in Victor Shoup's NTL package [36] are 2.3, 2.1, 3.8, 3.5, 6.0, 8.7, and 10.5.

(ii) We use the estimates for R_ρ, R_1 and R_2 to justify our main conclusion that the fields $\mathbb{F}_{2^N}$, where $N \in [185, 600]$ is divisible by 5, are weak for ECC. This statement becomes stronger as N increases. In particular, it is debatable whether our estimates justify the conclusion that the field $\mathbb{F}_{2^{185}}$ is weak for ECC. This field is of special interest because it is explicitly included in the OAKLEY key agreement protocol that was proposed for Internet applications [31].

(iii) By selecting only a proportion of degree one divisors in the factor base, one can decrease the cost of the matrix stage at the expense of increasing the cost of the relation generation stage. More precisely, if the factor base size is reduced by a factor of 2^d, then R_2 decreases by a factor of 2^{2d}, while R_1 increases by a factor of $2^{d(g-1)}$. For example, if we select $d = 4$ for the case $N = 600$, then we obtain $R_1 = 2^{237}$ and $R_2 = 2^{238}$. We can then derive our claim made at the end of Section 1 that the ECDLP for all elliptic curves over $\mathbb{F}_{2^{600}}$ can be solved about 2^{69} times faster than it takes Pollard's rho method to solve the hardest instances. Similarly, for $(N, d) = (385, 1.5)$ we have $(R_1, R_2) = (2^{155.5}, 2^{157})$, and for $(N, d) = (515, 3)$ we have $(R_1, R_2) = (2^{205}, 2^{206})$.

4 The fields $\mathbb{F}_{2^N}$ with $N = 4l$

Smart [38] presented some experimental evidence that the fields $\mathbb{F}_{2^N}$, where N is divisible by 4, are weak for ECC. In this section we repeat our analysis from Section 3 of the GHS attack for the ECDLP over these fields, and precisely quantify the weakness of the fields. We conclude that the fields $\mathbb{F}_{2^{4l}}$ exhibit some signs of being weak, but are not as weak as the fields $\mathbb{F}_{2^{5l}}$.

Let $N = 4l$. If E is an elliptic curve defined over $\mathbb{F}_{2^N} \setminus \mathbb{F}_{2^l}$, then the GHS reduction yields a hyperelliptic curve C of genus 7 or 8 over $\mathbb{F}_{2^l}$. The genus of C is 8 in a majority of the cases, and so we focus on this case.

Arguing as in Section 3, we have

$$\begin{aligned} R_\rho &\approx c_N 2^{2l+2.5}, \\ R_1 &\approx c_l (32l - 48) 2^{l+14}, \\ R_2 &\approx c_r 2^{2l+1}. \end{aligned}$$

Hence the running time of Pollard's rho algorithm is very close to the running time of the matrix stage. However, if the factor base size is reduced by a factor of 2^d, then R_2 decreases by a factor of 2^{2d}, while R_1 increases by a factor of 2^{7d} (cf. Remark 5(iii)). Table 2 list the costs R_ρ, R_1, R_2 for some selected fields and choices of d that roughly balance R_1 and R_2.

5 The field $\mathbb{F}_{2^{210}}$

In this section we argue that the field $\mathbb{F}_{2^{210}}$ is particularly weak for ECC. Recall from Section 3.3 that $R_\rho \approx c_N 2^{107.5}$, $R_1 \approx c_l 2^{97}$, and $R_2 \approx c_r 2^{86}$ for the parameters $(N, l) = (210, 42)$. We next consider the GHS attack with parameters $(N, n, m) = (210, 6, 5)$.

N	l	d	R_ρ/c_N	R_1/c_l	R_2/c_r
160	40	2	$2^{82.5}$	2^{78}	2^{77}
192	48	3	$2^{98.5}$	2^{94}	2^{91}
224	56	4	$2^{114.5}$	2^{109}	2^{104}
256	64	5	$2^{130.5}$	2^{124}	2^{119}
384	96	8	$2^{194.5}$	2^{178}	2^{177}
512	128	12	$2^{258.5}$	2^{238}	2^{233}
600	150	14	$2^{302.5}$	2^{274}	2^{273}

Table 2. Time estimates for Pollard's rho method for solving an ECDLP instance in $E(\mathbb{F}_{2^N})$, and for the relation generation and matrix stages of the Enge-Gaudry algorithm for solving an HCDLP instance in $J_C(\mathbb{F}_{2^l})$ where C is a a genus 8 hyperelliptic curve. The factor base in the Enge-Gaudry algorithm is comprised of $1/2^d$ of all degree-one prime divisors. c_N, c_l and c_r are the times for a multiplication in $\mathbb{F}_{2^N}$, $\mathbb{F}_{2^l}$, and modulo an N-bit prime, respectively.

5.1 Exact analysis of the GHS attack with $(N, n, m) = (210, 6, 5)$

About 2^{175} isomorphism classes of elliptic curves over $\mathbb{F}_{2^{210}}$ have magic number $m = 5$ relative to $n = 6$, as a consequence of which there exists an even more effective ECDLP solver for at least about 25% of all elliptic curves over $\mathbb{F}_{2^{210}}$. We first analyze the GHS attack in this case, and then discuss how to extend it beyond these 2^{175} isomorphism classes.

Let $E : y^2+xy = x^3+ax^2+b$ be an elliptic curve over $\mathbb{F}_{2^{210}}$ with magic number $m = 5$ relative to $n = 6$. First note that by [27, Lemma 8] and [20] we require that $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(a) = 0$ for the GHS reduction to yield a group homomorphism $\Phi : E(\mathbb{F}_{2^{210}}) \to J_C(\mathbb{F}_{2^{35}})$ into the jacobian of a hyperelliptic curve C defined over $\mathbb{F}_{2^{35}}$. We thus restrict ourselves to curves of the form $E : y^2 + xy = x^3 + b$. Then $m = 5$ if and only if $b \in \mathbb{F}_{2^{210}} \setminus \mathbb{F}_{2^{35}}$, while if $b \in \mathbb{F}_{2^{35}}$ we have $m = 1$ and $\#E(\mathbb{F}_{2^{35}}) \mid \#E(\mathbb{F}_{2^{210}})$. Again, the GHS reduction takes only a few seconds. The resulting hyperelliptic curve has genus 15 or 16. Similar to Theorem 3, this time using $t(x) = x^4 + x^2 + 1$ and taking into account that $\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(a) = 0$ we can show that there are exactly $2^{140} - 2^{70}$ isomorphism classes of elliptic curves defined over $\mathbb{F}_{2^{210}} \setminus \mathbb{F}_{2^{35}}$ the GHS attack yields a hyperelliptic curve C defined over $\mathbb{F}_{2^{35}}$ of genus $g = 15$. For exactly $(2^{140} - 2^{70})(2^{35} - 1) \approx 2^{175}$ isomorphism classes, a genus 16 curve is obtained.

Using the Enge-Gaudry index-calculus algorithm with a factor base of $w \approx 2^{34}$ degree-one prime divisors, it takes an expected number of $T_1 \approx 2^{34+35g}/M(1)$ random walk steps in the jacobian to complete the relation generation stage. For the case $g = 16$, we get $R_1 \approx c_{35}2^{90}$ and $R_2 \approx c_r 2^{72}$.

5.2 Extended GHS attack

We next discuss how to extend the GHS attack beyond the set of elliptic curves with magic number 5 relative to $n = 6$. We first classify the curves over $\mathbb{F}_{2^{210}}$ with $(n, m) = (6, 5)$.

Theorem 6 Let $N \equiv 0 \pmod 6$, and let $E : y^2 + xy = x^3 + ax^2 + b$ be an elliptic curve over $\mathbb{F}_{2^N}$ with magic number $m = 5$ relative to $n = 6$. Then $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = 0$.

Proof. Let $N = n \cdot l$, $q = 2^l$, and let $\sigma : \mathbb{F}_{2^N} \to \mathbb{F}_{2^N}$ denote the power-q Frobenius $\alpha \mapsto \alpha^q$. Since $x^6 - 1 = (x-1)^2(x^2+x+1)^2$ over $\mathbb{F}_2$, there are two possibilities to obtain magic number 5, namely $\mathrm{Ord}_b(x) = (x-1)^j(x^2+x+1)^2$ with $j = 0$ or $j = 1$. If $j = 0$, then $0 = \mathrm{Ord}_b(\sigma)(b) = b^{q^4} + b^{q^2} + b$. Thus, $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = \sum_{i=0}^{N-1} b^{2^i} = \sum_{i=0}^{2l-1}(b + b^{q^2} + b^{q^4})^{2^i} = 0$. If $j = 1$, then $0 = \mathrm{Ord}_b(\sigma)(b) = b^{q^5} + b^{q^4} + b^{q^3} + b^{q^2} + b^q + b = 0$. This implies $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = \sum_{i=0}^{l-1}(b + b^q + b^{q^2} + b^{q^3} + b^{q^4} + b^{q^5})^{2^i} = 0$. □

The following result is probably well known. We include a proof since we could not find it elsewhere.

Lemma 7 Let $E : y^2 + xy = x^3 + b$ be an elliptic curve over $\mathbb{F}_{2^N}$, where $N \geq 3$. Then $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = 0$ if and only if $\#E(\mathbb{F}_{2^N}) \equiv 0 \pmod 8$.

Proof. Since the 2^s-torsion group ($s \in \mathbb{N}$) of E over the algebraic closure $\overline{\mathbb{F}}_{2^N}$ is cyclic, we equivalently show that $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = 0$ if and only if $E(\mathbb{F}_{2^N})$ has a point of order 8. The 8th division polynomial of E is given by

$$f_8(x) = x^{28} + (b^2+b)x^{20} + (b^4+b^3)x^{12} + b^6x^4 = (x^6+bx^2)^2(x^{16}+bx^8+b^4),$$

where x^6+bx^2 is the 4th division polynomial. In the very last term, we substitute x^8 by z. Then E has a point of order 8 with x-coordinate defined over $\mathbb{F}_{2^N}$ if and only if $z^2 + bz + b^4$ factors over $\mathbb{F}_{2^N}$, which is the case if and only if $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b^2) = \mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = 0$. It remains to show that if $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = 0$, then the y-coordinate is also defined over $\mathbb{F}_{2^N}$. So assume $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = 0$, let $\beta \in \mathbb{F}_{2^N}$ such that $b = \beta^2 + \beta$, and let $t \in \mathbb{F}_{2^N}$ such that $\beta = t^8$. Then

$$z^2 + bz + b^4 = (z + t^{32} + t^{24} + t^{16} + t^8)(z + t^{32} + t^{24}),$$

and the eighth root $t^4 + t^3$ of $t^{32} + t^{24}$ is the x-coordinate of the 8-division point. It is easily verified that $y = t^8 + t^5 \in \mathbb{F}_{2^N}$ is an appropriate y-coordinate. □

Corollary 8 Let $E : y^2 + xy = x^3 + ax^2 + b$ be an elliptic curve over $\mathbb{F}_{2^{210}}$ with magic number $m = 5$ relative to $n = 6$ and for which the GHS reduction yields a group homomorphism $\Phi : E(\mathbb{F}_{2^{210}}) \to J_C(\mathbb{F}_{2^{35}})$ into the jacobian of a hyperelliptic curve C defined over $\mathbb{F}_{2^{35}}$ (of genus 15 or 16). Then $\#E(\mathbb{F}_{2^{210}}) \equiv 0 \pmod 8$.

Proof. By [27, Lemma 8] and [20], we require that $\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(a) = 0$ for the GHS reduction to work when $(n, m) = (6, 5)$. The statement then immediately follows from Theorem 6 and Lemma 7. □

Extending the GHS attack to the entire isogeny class of a weak curve over $\mathbb{F}_{2^{210}}$. We argue that for any elliptic curve E with $\#E(\mathbb{F}_{2^{210}}) \equiv 0 \pmod 8$ any ECDLP instance can be solved essentially in running time $R_1 \approx c_{35}2^{90}$.

An isogeny between two elliptic curves E and E' over a field K is a non-constant morphism $\Psi : E \to E'$ such that the neutral element of E is mapped to the neutral element of E'. The curves E and E' are called isogenous over K if Ψ is defined over K; we write $E \sim E'$. If K is a finite field, then $E \sim E'$ if and only if $\#E(K) = \#E'(K)$. The equivalence classes with respect to isogeny are called isogeny classes.

Let E be a non-supersingular elliptic curve over $\mathbb{F}_{2^N}$. We call $t = 2^N + 1 - \#E(\mathbb{F}_{2^N})$ its trace and $\Delta = t^2 - 4 \cdot 2^N$ its discriminant; note that $\Delta < 0$ and $\Delta \equiv 1 \pmod 8$. The endomorphism ring $\mathrm{End}(E)$ of E is an order in the maximal order $\mathcal{O}$ of the imaginary quadratic number field $\mathbb{Q}(\sqrt{\Delta})$. More precisely, $\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}$, where $\pi : E \to E$ is the 2^N-th power Frobenius map on E. The endomorphism class of E, denoted by $\mathcal{C}(E)$, is the set of all isogenous, non-isomorphic curves E' with $\mathrm{End}(E) = \mathrm{End}(E')$. There exists a one-to-one correspondence between the Picard group (denoted Cl(End(E))) of the order $\mathrm{End}(E)$ and $\mathcal{C}(E)$ ([10, Th. 3.4.6]).

For any elliptic curve E over $\mathbb{F}_{2^{210}}$ we can use an algorithm of Kohel [24] to compute a chain of isogenies defined over $\mathbb{F}_{2^{210}}$ from E to an elliptic curve E' with $\mathrm{End}(E') = \mathcal{O}$. This takes running time $O(s^3)$, where s is the largest prime dividing the conductor $c = [\mathcal{O} : \mathrm{End}(E)]$ of $\mathrm{End}(E)$. Note that c divides $[\mathcal{O} : \mathbb{Z}[\pi]]$. In practice, $[\mathcal{O} : \mathbb{Z}[\pi]]$ is small and smooth so that Kohel's algorithm takes negligible time compared to R_1. For the following, we therefore may assume that $\mathrm{End}(E)$ is maximal. Then Cl(End(E)) is the ideal class group of the maximal order $\mathcal{O}$, which we simply denote by Cl.

Now, there exist 2^{209} isomorphism classes of elliptic curves $E_{0,b}$ over $\mathbb{F}_{2^{210}}$ with $\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(b) = 0$ (i.e., with group order divisible by 8), and $2^{175} - 2^{105}$ elliptic curves $E_{0,b}$ over $\mathbb{F}_{2^{210}}$ with $(n, m) = (6, 5)$. It is therefore reasonable to expect that a randomly chosen elliptic curve over $\mathbb{F}_{2^{210}}$ with group order divisible by 8 has magic number 5 relative to $n = 6$ with probability approximately $2^{175}/2^{209} = 2^{-34}$. Moreover, we make the heuristic assumption that the same is true when E is chosen randomly from a fixed endomorphism class.

Assumption A. Let $E = E_{0,b}$ an elliptic curve over $\mathbb{F}_{2^{210}}$ with $\#E_{0,b}(\mathbb{F}_{2^{210}}) \equiv 0 \pmod 8$. Then any curve E' that is randomly chosen from $\mathcal{C}(E)$ (with respect to the uniform distribution) has magic number $m = 5$ relative to $n = 6$ with probability 2^{-34}.

Remark 9 (*further justification of Assumption A*) For arbitrary $N \equiv 0 \pmod 6$, let $N = 6l$ and $q = 2^l$. By [29, Theorem 5], there exist $q^5 - q^3 = 2^{5N/6} - 2^{N/2}$ isomorphism classes of elliptic curves $E_{0,b}$ over $\mathbb{F}_{2^N}$ with $(n, m) = (6, 5)$, while there exist 2^{N-1} isomorphism classes $E_{0,b}$ with $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(b) = 0$. Thus, the probability in the above Assumption A generalizes to $2^{-(N/6-1)}$. For $36 \le N \le 84$, this has been confirmed in extensive experiments.

Remark 10 (*restriction of Assumption A*) Of course, Assumption A is not accurate if Cl is very small, in the order of $210 \cdot 2^{34} \approx 2^{42}$ and smaller. This can happen only if $\#E(\mathbb{F}_{2^{210}})$ lies at the extreme ends of the Hasse interval and thus Δ is significantly smaller than its expected value 2^{212}, or if Δ has a very large square factor. But note that $\Delta < 2^{150}$ if and only if $|t| > \sqrt{2^{212} + 2^{150}}$, which affects only a very small fraction of *at most* $1/2^{63}$ of the elliptic curves over $\mathbb{F}_{2^{210}}$; the proportion of elliptic curves over $\mathbb{F}_{2^{210}}$ that have $\Delta < 2^{100}$ is at most $1/2^{113}$. If $\Delta > 2^{150}$ and $\Delta = f^2 d$ with $d \equiv 1 \pmod 8$ and squarefree, then $\#\mathrm{Cl} \leq 2^{42}$ only if f is (roughly) at least 2^{30}, which is most unlikely for non-subfield curves.

Given a curve E over $\mathbb{F}_{2^{210}}$ with group order divisible by 8, it is now possible to compute a curve E' over $\mathbb{F}_{2^{210}}$, isogenous to E and with $(n, m) = (6, 5)$ along with a chain of low-degree isogenies from E to E'. This is based on ideas from [15] to simulate a random walk in the endomorphism class of E, exploiting the above one-to-one correspondence between Cl and $\mathcal{C}(E)$. This works as follows: Let $E = E_{0,b}$, let $j(E) = b^{-1}$ be its j-invariant, and let p be a prime with $\left(\frac{\Delta}{p}\right) = 1$. Then p splits in $\mathcal{O}$, $(p) = \mathfrak{p}_1\mathfrak{p}_2$, and the modular polynomial $\Phi_p(j(E), X)$ has two roots j_1 and j_2 in $\mathbb{F}_{2^{210}}$ [13]. These roots can be computed by a probabilistic algorithm using $O(210p^2)$ operations in $\mathbb{F}_{2^{210}}$. The two isogenies mapping E to $E_{0,j_1^{-1}}$ and $E_{0,j_2^{-1}}$ correspond to the multiplication of a fixed ideal, say $\mathcal{O}$, by the two prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$ lying over p. As explained in [15], it is easy to determine whether j_1 corresponds to $\mathfrak{p}_1$ or $\mathfrak{p}_2$. Now, let $\mathcal{P}$ be the set of the 30 smallest primes p such that $\left(\frac{\Delta}{p}\right) = 1$, and such that the pairs of ideal classes corresponding to the prime ideals lying over p are pairwise distinct in Cl. A pseudo-random walk (E_i) in $\mathcal{C}(E)$ is defined as follows: Let $E_0 = E_{0,b}$ and $b_0 = b$ and $\mathfrak{a}_0 = \mathcal{O}$. For $i = 1, 2, \ldots$, let $p \in_R \mathcal{P}$ and $j = b_{i-1}$, and compute the two roots in $\mathbb{F}_{2^{210}}$ of $\Phi_p(j, X)$; let j' be one of these roots, and let $b_i = (j')^{-1}$. Simultaneously a chain $(\mathfrak{a}_i)$ of ideals in Cl is computed such that for each index k, the ideal $\mathfrak{a}_k$ corresponds to the isogeny mapping E to E_k.

The set $\mathcal{P}$ has been chosen such that the walk (E_i) indeed simulates a random walk in the endomorphism class of E. Experimentally, we found that $\max\{p \in \mathcal{P}\} \in [190, 530]$, where we considered 5000 randomly chosen discriminants, with only 2 discriminants yielding maximum values > 500 (and we obtained $\max\{p \in \mathcal{P}\} \in [150, 380]$ if we required only $\#\mathcal{P} = 20$). Thus, each random-walk step takes up to about $210 \cdot 500^2 \approx 2^{26}$ operations in $\mathbb{F}_{2^{210}}$, given that computing the roots of the modular polynomial is by far the most time-consuming step.

Now, under Assumption A, after expected 2^{34} random-walk steps in $\mathcal{C}(E)$ an elliptic curve E_k over $\mathbb{F}_{2^{210}}$ is encountered that is isogenous to E and whose magic number relative to $n = 6$ is $m = 5$. Thus, altogether it takes something on the order of 2^{60} operations in $\mathbb{F}_{2^{210}}$ to find a curve with $(n, m) = (6, 5)$ isogenous to a given curve over $\mathbb{F}_{2^{210}}$, along with an ideal $\mathfrak{a}$ that represents the isogeny between the two curves. We note that this running time is negligible compared to R_1 and R_2. Also, this step can be efficiently parallelized.

The remaining steps to compute the explicit isogeny between E and E_k are identical with Stages 2 and 3 of [15]: index-calculus techniques are used to represent $\mathfrak{a}$ as a product of just a few ideals of small norm, and finally Vélu's formulae are applied. This can be accomplished in time $O(2^{N/4+\varepsilon}) = const \cdot 2^{53}$, which also is negligible when compared to R_1 and R_2.

5.3 Further extension to elliptic curves with $\mathbf{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(b) \neq 0$

Next, we further extend the set of elliptic curves over $\mathbb{F}_{2^{210}}$ for which any ECDLP instance can be solved potentially faster than applying Pollard's rho method to the hardest ECDLP instances over $\mathbb{F}_{2^{210}}$. For this, we use Hess' recent generalization [20] of the GHS attack to reduce instances of the ECDLP to instances of a discrete logarithm problem in the divisor class group of a curve C over $\mathbb{F}_{2^{35}}$. Note that this curve C is in general not hyperelliptic. Nevertheless, subexponential-time methods for discrete logarithm computation are available for such curves of large genus (see [20] and the references given there). However we do not have an exact analysis of their running times.

Let $N = 6l$ for some integer l. Consider the elliptic curve $E : y^2 + xy = x^3 + ax^2 + b$ over $\mathbb{F}_{2^N}$ with $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(a) = 0$, $b \neq 0$, and let $\langle P \rangle$ be a subgroup of $E(\mathbb{F}_{2^N})$ of prime order r.

Let $q = 2^l$, and for $\gamma \in \mathbb{F}_{2^N}$ let $\mathrm{Ord}_\gamma(x)$ denote the unique monic polynomial $f \in \mathbb{F}_2[x]$ of least degree such that $f(\sigma)(\gamma) = 0$ where σ is the power-q Frobenius.

Let $\gamma_1, \gamma_2 \in \mathbb{F}_{2^N}$ such that $b = (\gamma_1\gamma_2)^2$. Let $c = 1/\gamma_1$; then $\gamma_2 = b^{1/2}c$. Let $s_i = \deg(\mathrm{Ord}_{\gamma_i})$ $(i = 1, 2)$ and $t = \deg(\mathrm{lcm}(\mathrm{Ord}_{\gamma_1}, \mathrm{Ord}_{\gamma_2}))$. Via a birational transformation the defining equation of E can be brought into the form $y^2 + y = 1/(cx) + a + b^{1/2}cx$, and then Hess' generalization [20, Theorems 4,5,7] of the GHS attack allows to effectively reduce the ECDLP in $\langle P \rangle$ to the DLP in a subgroup of order r of the divisor class group of an explicitly computable curve C over $\mathbb{F}_{2^N}$ of genus $g = 2^t - 2^{t-s_1} - 2^{t-s_2} + 1$. If $\mathrm{Ord}_{\gamma_1}(x) = \mathrm{Ord}_{\gamma_2}(x) = x^4 + x^2 + 1$, this yields a curve of genus $g = 15$, while if $\mathrm{Ord}_{\gamma_1}(x) = x^2 + x + 1$ and $\mathrm{Ord}_{\gamma_2}(x) = x^4 + x^2 + 1$ a curve of genus $g = 12$ is obtained.

There exists an efficient algorithm that, given $b \in \mathbb{F}_{2^N}^*$, decides whether such γ_1, γ_2 exist and also computes them if this is the case.

Algorithm 11 *(Finding decomposition of b)*
Input: $b \in \mathbb{F}_{2^N}^*$.
Output: $c \in \mathbb{F}_{2^N}^*$ such that $\mathrm{Ord}_{1/c}(x)$ and $\mathrm{Ord}_{b^{1/2}c}(x)$ divide $x^4 + x^2 + 1$, or "failure".

1. Let $\beta = b^{1/2}$. Let $q = 2^l$, where $l = N/6$.
2. Let $w(u) = u^2 + (\beta^{q^4-1} + \beta^{q^2-1} + 1)u + \beta^{q^2-1} \in \mathbb{F}_{q^6}[u]$.
3. { Check if $w(u)$ has roots in $\mathbb{F}_{2^N}$, and compute them. }
   If $\gcd(w(u), u^{q^6} - u) \neq 1$ then compute u_0, $u_1 \in \mathbb{F}_{q^6}$ such that $w(u_0) = w(u_1) = 0$. Else return "failure" and STOP.
4. For $i = 0, 1$, check if $u_i^{q^2+1} + u_i + 1 = 0$.
   If both u_i fail this test, return "failure" and STOP.
   Otherwise, assume u_0 passed the test.

5. Compute some $\gamma_1 \in \mathbb{F}_{2^N}^*$ such that $u_0 = \gamma_1^{q^2-1}$ (see Lemma 12 below).
6. Return $c = \gamma_1^{-1} \in \mathbb{F}_{2^N}^*$.

Lemma 12 Let q be a power of 2. Let $u_0 \in \mathbb{F}_{q^6}$ such that $u_0^{q^2+1} + u_0 + 1 = 0$. Then $\mathrm{ord}(u_0)$ divides $q^4 + q^2 + 1$, and there exists $\gamma \in \mathbb{F}_{q^6}^*$ such that $u_0 = \gamma^{q^2-1}$.

Proof. The first statement is immediate from $u_0^{q^4+q^2+1} = (u_0^{q^2+1})^{q^2} u_0 = (u_0 + 1)^{q^2} u_0 = u_0^{q^2+1} + u_0 = 1$. Now let α be a generator of $\mathbb{F}_{q^6}^*$. Let $z \in \mathbb{N}$ be such that $u_0 = \alpha^z$. Then $\alpha^{z(q^4+q^2+1)} = 1$. Thus, $(q^6 - 1) \mid z(q^4 + q^2 + 1)$ which implies $(q^2 - 1) \mid z$. Let $r = z/(q^2 - 1)$, then $\gamma = \alpha^r$ satisfies $\gamma^{q^2-1} = u_0$. □

Theorem 13 Algorithm 11 succeeds for $b \in \mathbb{F}_{2^N}^*$ if and only if there exist $\gamma_1, \gamma_2 \in \mathbb{F}_{q^6}^*$ such that $b = (\gamma_1\gamma_2)^2$ and $\mathrm{Ord}_{\gamma_1}(x)$ and $\mathrm{Ord}_{\gamma_2}(x)$ divide $x^4 + x^2 + 1$. If this is the case and c is the output of Algorithm 11, then $\gamma_1 = 1/c$ and $\gamma_2 = b^{1/2}c$ are suitable choices.

Proof. Let $\beta = b^{1/2}$. Let us first assume that there exist $\gamma_1, \gamma_2 \in \mathbb{F}_{q^6}^*$ such that $\beta = \gamma_1\gamma_2$ and $\mathrm{Ord}_{\gamma_1}(x)$ and $\mathrm{Ord}_{\gamma_2}(x)$ divide $x^4 + x^2 + 1$. Then

$$\gamma_1^{q^4} + \gamma_1^{q^2} + \gamma_1 = 0 \qquad \text{and} \qquad (\beta/\gamma_1)^{q^4} + (\beta/\gamma_1)^{q^2} + \beta/\gamma_1 = 0,$$

or, equivalently,

$$\gamma_1^{q^4-1} + \gamma_1^{q^2-1} + 1 = 0 \qquad \text{and} \qquad \gamma_1^{q^4-1}\beta + \gamma_1^{q^4-q^2}\beta^{q^2} + \beta^{q^4} = 0. \tag{8}$$

Let $v = \gamma_1^{q^2-1}$. Then (8) is equivalent to

$$v^{q^2+1} + v + 1 = 0 \text{ and } v^2 + (1 + \beta^{q^2-1} + \beta^{q^4-1})v + \beta^{q^2-1} = 0 \tag{9}$$

The last equation is equivalent with the quadratic equation $w(v) = 0$ where $w(u) \in \mathbb{F}_{q^6}[u]$ is the polynomial in Algorithm 11. Thus v is a root of $w(u)$ satisfying $v^{q^2+1} + v + 1 = 0$. The algorithm will terminate with some $(q^2 - 1)$-th root of v^{-1}.

Now assume Algorithm 11 has output c. Let $\gamma_1 = 1/c$ and $\gamma_2 = \beta c$. Then $b = (\gamma_1\gamma_2)^2$. Let $u = \gamma_1^{q^2-1}$. Then, by construction of Algorithm 11, u satisfies (9), which implies $\gamma_i^{q^4} + \gamma_i^{q^2} + \gamma_i = 0$ for $i = 1, 2$. Thus, $\mathrm{Ord}_{\gamma_i}(x) \mid (x^4 + x^2 + 1)$. □

Next we restrict ourselves to those values b such that some γ_i has $\mathrm{Ord}_{\gamma_i}(x) = x^2 + x + 1$. If both γ_i have $\mathrm{Ord}_{\gamma_i}(x) = x^2 + x + 1$ then b lies in $\mathbb{F}_{q^3}$ and the elliptic curve is a subfield curve.

Lemma 14 Let $b \in \mathbb{F}_{q^6}^*$ such that the quadratic equation in Step 3 of Algorithm 11 has solutions $c_1, c_2 \in \mathbb{F}_{q^6}^*$. Then b can be written in the form $(\gamma_1\gamma_2)^2$ with $\mathrm{Ord}_{\gamma_1}(x) = x^2 + x + 1$ and $\mathrm{Ord}_{\gamma_2}(x)$ dividing $x^4 + x^2 + 1$ if and only if either c_1 or c_2 has order dividing $q^2 + q + 1$.

Proof. Suppose first that b can be written in the form $(\gamma_1\gamma_2)^2$ with $\mathrm{Ord}_{\gamma_1}(x) = x^2+x+1$ and $\mathrm{Ord}_{\gamma_2}(x)$ dividing x^4+x^2+1. Note that this implies $\gamma_1^{q^3-1} = 1$. We either have $c_1 = \gamma_1^{q^2-1}$ or $c_2 = \gamma_1^{q^2-1}$. Suppose $c_1 = \gamma_1^{q^2-1}$. Then

$$c_1^{q^2+q+1} = \gamma_1^{(q^2-1)(q^2+q+1)} = \gamma_1^{(q^3-1)(q+1)} = 1.$$

Conversely, if $c^{q^2+q+1} = 1$ and $c = \gamma_1^{q^2-1}$, then $\gamma_1^{(q+1)(q^3-1)} = 1$. Set $\gamma' = \gamma_1^{q^3-1}$. Then $\gamma' \in \mathbb{F}_{q^2}^*$ and $\gamma'' = \frac{\gamma_1}{\gamma'}$ is another (q^2-1)-th root of c. Moreover, $(\gamma'')^{q^2} + (\gamma'')^q + \gamma'' = 0$. □

The following conjecture is based on experimental results that were conducted in order to determine the proportion of $b \in \mathbb{F}_{q^6}^*$ for which Algorithm 11 succeeds.

Conjecture 15 Suppose that the quadratic equation

$$u^2 + (\beta^{q^4-1} + \beta^{q^2-1} + 1)u + \beta^{q^2-1} = 0 \tag{10}$$

has two solutions u_1, u_2 in $\mathbb{F}_{q^6}$. Then u_1 and u_2 satisfy $u_i^{q^2+1} + u_i + 1 = 0$.

This conjecture has been verified with numerous experiments for $N = 30, 36, \ldots, 222$. We can only prove the following.

Lemma 16 Assume $u_1, u_2 \in \mathbb{F}_{q^6}$ are the solutions to (10) and $u_1^{q^2+1}+u_1+1 = 0$. Then also $u_2^{q^2+1} + u_2 + 1 = 0$.

Proof. We have

$$u_1^{q^2+1} + u_1 + 1 = 0 \quad \text{and} \quad u_2 = u_1 + \beta^{q^4-1} + \beta^{q^2-1} + 1. \tag{11}$$

Set $\alpha = \beta^{q^4-1} + \beta^{q^2-1} + 1$. Then with (11) it follows that

$$u_2^{q^2+1} + u_2 + 1 = \frac{\alpha^{q^2-1}}{u_1}\left(u_1^2 + \alpha^{1-q^2} + \alpha u_1\right)$$

which is equal to 0 since u_1 satisfies the equation (10). □

Now, it is reasonable to expect that $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}\left(\frac{\beta^{q^2-1}}{(\beta^{q^4-1}+\beta^{q^2-1}+1)^2}\right)$ is distributed uniformly at random in $\mathbb{F}_2$ for random $\beta \in \mathbb{F}_{q^6}^*$. In fact, Algorithm 11 seems to succeed for half of the $\beta = b^{1/2} \in \mathbb{F}_{q^6}^*$ (see Table 3 below). This implies that for around half of all elliptic curves defined over $\mathbb{F}_{2^N}$ with $N \equiv 0 \pmod 6$ the ECDLP can be reduced to the DLP on the jacobian of a curve of genus 15, or genus 12. Combined with the extended GHS attack as in Section 5.2, this reduction should be possible for any elliptic curve over $\mathbb{F}_{2^N}$ with $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(a) = 0$.

N	Equation (10) solvable in $\mathbb{F}_{2^N}$	Solutions satisfying $u^{q^2+1}+u+1=0$	Solutions with order dividing q^2+q+1 (leading to genus 12 curve)
30	5088	5088	6
36	4985	4985	68
42	4924	4924	72
48	5018	5018	34
54	4955	4955	8
60	5013	5013	13
114	5028	5028	0
120	4993	4993	0
126	4967	4967	0
204	4956	4956	0
210	5001	5001	0
216	5053	5053	0
222	5100	5100	0

Table 3. Experimental results on the success rate of Algorithm 11. For each N, the second column indicates for how many of 10000 randomly chosen $\beta \in \mathbb{F}_{2^N}$, (10) was solvable in $\mathbb{F}_{2^N}$. Column 3 indicates for how many such β the corresponding solutions u_1, u_2 were also roots of $u^{q^2+1}+u+1$, which suggests Conjecture 15. The last column lists the number of β's that lead to a genus 12 curve.

5.4 Comparisons

Table 4 shows the costs R_ρ, R_1, R_2 for the attacks on the ECDLP for elliptic curves defined over $\mathbb{F}_{2^{210}}$ as discussed in this section.

N	n	l	R_ρ/c_{210}	R_1/c_l	R_2/c_r	c_{210}	c_l	c_r	R_ρ	R_1	R_2
210	5	42	$2^{107.5}$	2^{97}	2^{86}	10.3	1.0	8.0	$2^{110.5}$	2^{97}	2^{89}
210	6	35	$2^{107.5}$	2^{90}	2^{72}	10.3	1.0	8.0	$2^{110.5}$	2^{90}	2^{75}

Table 4. Time estimates for Pollard's rho method for solving an ECDLP instance in $E(\mathbb{F}_{2^{210}})$, and for the relation generation and matrix stages of the Enge-Gaudry algorithm for solving an HCDLP instance in $J_C(\mathbb{F}_{2^{42}})$ and $J_C(\mathbb{F}_{2^{35}})$ where C is a genus 16 hyperelliptic curve. c_{210}, c_l and c_r are the relative times for a multiplication in $\mathbb{F}_{2^{210}}$, $\mathbb{F}_{2^l}$, and modulo an 210-bit prime, respectively.

Consequently, for all elliptic curves over $\mathbb{F}_{2^{210}}$, the ECDLP can be solved about 2^{13} times faster than it takes Pollard's rho method to solve the hardest instances. For about a quarter of all curves over $\mathbb{F}_{2^{210}}$ (those with $\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(a) = \mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(b) = 0$) the ECDLP can be solved about 2^{20} times faster than with Pollard's rho method. As argued in Section 5.3, for another 25% of all curves over $\mathbb{F}_{2^{210}}$ (those with $\mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(a) = 0, \mathrm{Tr}_{\mathbb{F}_{2^{210}}/\mathbb{F}_2}(b) = 1$), the ECDLP presumably can be solved significantly faster than with Pollard's rho method, although an exact analysis has not been conducted.

6 Conclusions

We have argued that the fields $\mathbb{F}_{2^N}$, where $N \in [185, 600]$ is divisible by 5, are weak for ECC. The fundamental open problem is to determine whether there are any fields that are bad for ECC. We have provided some evidence that the field $\mathbb{F}_{2^{210}}$ is a prime candidate for being bad.

Another candidate for a bad field is $\mathbb{F}_{2^{161}}$. For 2^{94} of the 2^{162} isomorphism classes of elliptic curves E over $\mathbb{F}_{2^{161}}$, the GHS reduction yields a hyperelliptic curve C of genus (7 or) 8 over $\mathbb{F}_{2^{23}}$, where the HCDLP is feasible. In our notation, we have $R_\rho = c_E 2^{80}$, $R_1 = (c_J + c_S)2^{37}$, and $R_2 = c_r 2^{47}$, where c_E denotes the time to perform an elliptic curve addition in $E(\mathbb{F}_{2^{161}})$, c_J is the time to perform an addition in $J_C(\mathbb{F}_{2^{23}})$, c_S is the time to test whether a monic polynomial $a \in \mathbb{F}_{2^{23}}[u]$ of degree 8 is 1-smooth, and c_r is the time to perform a multiplication modulo a 160-bit prime. If an arbitrary ECDLP instance over $\mathbb{F}_{2^{161}}$ can be efficiently mapped to an ECDLP instance for an isogenous elliptic curve that belongs to the aforementioned class of 2^{94} curves, then one would conclude that $\mathbb{F}_{2^{161}}$ is bad for ECC (see also [15] and [27, Remark 20]). No such mapping is known so far (see also [42]).

An important open question in hyperelliptic curve cryptography is whether there are algorithms for solving the HCDLP curve that are faster than the Enge-Gaudry algorithm. Because of the relevance to solving the ECDLP, improvements by a constant factor would be of interest. For example, the possibility of using sieving (see [9]) to generate relations needs to be further explored.

Galbraith [14] has shown that Weil descent can be used to attack the HCDLP over some low genus hyperelliptic curves defined over characteristic two finite fields of composite extension degrees. An open problem is to determine whether there are any weak fields for genus two hyperelliptic curve cryptography.

Acknowledgements

We would like to thank Mike Jacobson and Darrel Hankerson for answering our questions about the relative speeds of finite field, elliptic curve, and hyperelliptic curve operations. Thanks also to Mark Bauer for reviewing the 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. P. Barrett, "Implementing the Rivest Shamir and Adleman public key encryption algorithm on a standard digital signal processor", *Advances in Cryptology—CRYPTO '86*, LNCS 263 (1987), 311-323.
3. D. Bernstein, "Circuits for integer factorization: A proposal", preprint, 2001.
4. D. Cantor, "Computing in the jacobian of a hyperelliptic curve", *Mathematics of Computation*, 48 (1987), 95-101.
5. D. Cantor and H. Zassenhaus, "A new algorithm for factoring polynomials over finite fields", *Mathematics of Computation*, 36 (1981), 587-592.
6. D. Coppersmith, A. Odlyzko and R. Schroeppel, "Discrete logarithms in $GF(p)$", *Algorithmica*, 1 (1986), 1-15.
7. A. Enge and P. Gaudry, "A general framework for subexponential discrete logarithm algorithms", *Acta Arithmetica*, 102 (2002), 83-103.
8. FIPS 186-2, "Digital signature standard (DSS)", Federal Information Processing Standards Publication 186-2, National Institute of Standards and Technology, 2000.
9. R. Flassenberg and S. Paulus, "Sieving in function fields", *Experimental Mathematics*, 8 (1999), 339-349.
10. M. Fouquet, "Anneau d'endomorphismes et cardinalité des courbes elliptiques: aspects algorithmiques", PhD thesis, École polytechnique, Palaiseau Cedex, 2001.
11. G. Frey, "Applications of arithmetical geometry to cryptographic constructions", *Proceedings of the Fifth International Conference on Finite Fields and Applications*, Springer-Verlag, 2001, 128-161.
12. 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.
13. S. Galbraith, "Constructing isogenies between elliptic curves over finite fields", *LMS Journal of Computation and Mathematics*, 2 (1999), 118-138.
14. S. Galbraith, "Weil descent of jacobians", *Discrete Applied Mathematics*, 12 (2003), 165-180.
15. S. Galbraith, F. Hess and N. Smart, "Extending the GHS Weil descent attack", *Advances in Cryptology—EUROCRYPT 2002*, LNCS 2332 (2002), 29-44.
16. R. Gallant, R. Lambert and S. Vanstone, "Improving the parallelized Pollard lambda search on anomalous binary curves", *Mathematics of Computation*, 69 (2000), 1699-1705.
17. P. Gaudry, "An algorithm for solving the discrete log problem in hyperelliptic curves", *Advances in Cryptology—EUROCRYPT 2000*, LNCS 1807 (2000), 19-34.
18. P. Gaudry, F. Hess and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves", *Journal of Cryptology*, 15 (2002), 19-46.
19. D. Hankerson, personal communication, 2003.
20. F. Hess, "The GHS attack revisited", *Advances in Cryptology—EUROCRYPT 2003*, LNCS 2656 (2003), 374-387.
21. M. Jacobson, personal communication, 2003.
22. M. Jacobson, A. Menezes and A. Stein, "Solving elliptic curve discrete logarithm problems using Weil descent", *Journal of the Ramanujan Mathematical Society*, 16 (2001), 231-260.
23. M. Jacobson and A. van der Poorten, "Computational aspects of NUCOMP", *Algorithmic Number Theory—ANTS-IV*, LNCS 2369 (2002), 120-133.
24. D. Kohel, "Endomorphism rings of elliptic curves over finite fields", PhD thesis, University of California, Berkeley, 1996.

25. F. Kuhn and R. Struik, "Random walks revisited: Extensions of Pollard's rho algorithm for computing multiple discrete logarithms", *Selected Areas in Cryptography—SAC 2001*, LNCS 2259 (2001), 212-229.
26. J. López and R. Dahab, "High-speed software multiplication in $\mathbb{F}_{2^m}$", *Progress in Cryptology—INDOCRYPT 2000*, LNCS 1977 (2000), 203-212.
27. 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.
28. 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.
29. A. Menezes and M. Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart", *Topics in Cryptology—CT-RSA 2001*, LNCS 2020 (2001), 308-318.
30. P. van Oorschot and M. Wiener, "Parallel collision search with cryptanalytic applications", *Journal of Cryptology*, 12 (1999), 1-28.
31. H. Orman, "The OAKLEY key determination protocol", RFC 2412, 1998. Available from http://www.ietf.org.
32. S. Paulus and A. Stein, "Comparing real and imaginary arithmetics for divisor class groups of hyperelliptic curves", *Algorithmic Number Theory—ANTS-III*, LNCS 1423 (1998), 576-591.
33. J. Pollard, "Monte Carlo methods for index computation mod p", *Mathematics of Computation*, 32 (1978), 918-924.
34. 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.
35. 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.
36. V. Shoup, *NTL: A library for doing Number Theory.* Available from http://shoup.net/ntl.
37. N. Smart, "The discrete logarithm problem on elliptic curves of trace one", *Journal of Cryptology*, 12 (1999), 193-196.
38. N. Smart, "How secure are elliptic curves over composite extension fields?", *Advances in Cryptology—Eurocrypt 2001*, LNCS 2045 (2001), 30-39.
39. J. Solinas, "Efficient arithmetic on Koblitz curves", *Designs, Codes and Cryptography*, 19 (2000), 195-249.
40. E. Teske, "Speeding up Pollard's rho method for computing discrete logarithms", *Algorithmic Number Theory*, LNCS 1423 (1998), 541-554.
41. E. Teske, "On random walks for Pollard's rho method", *Mathematics of Computation*, 70 (2000), 809-825.
42. E. Teske, "An elliptic curve trapdoor system", *Cryptology ePrint Archive* Report 2003/058, 2003.
43. M. Wiener, "The full cost of cryptanalytic attacks", *Journal of Cryptology*, to appear.
44. M. Wiener and R. Zuccherato, "Faster attacks on elliptic curve cryptosystems", *Selected Areas in Cryptography—SAC '98*, LNCS 1556 (1999), 190-200.