CRYPTOGRAPHIC IMPLICATIONS OF HESS' GENERALIZED GHS ATTACK

ALFRED MENEZES AND EDLYN TESKE

ABSTRACT. A finite field K is said to be *weak* for elliptic curve cryptography if all instances of the discrete logarithm problem for all elliptic curves over K can be solved in significantly less time than it takes Pollard's rho method to solve the hardest instances. By considering the GHS Weil descent attack, it was previously shown that characteristic two finite fields $\mathbb{F}_{q^5}$ are weak. In this paper, we examine characteristic two finite fields $\mathbb{F}_{q^n}$ for weakness under Hess' generalization of the GHS attack. We show that the fields $\mathbb{F}_{q^7}$ are potentially partially weak in the sense that any instance of the discrete logarithm problem for half of all elliptic curves over $\mathbb{F}_{q^7}$, namely those curves E for which $\#E(\mathbb{F}_{q^7})$ is divisible by 4, can likely be solved in significantly less time than it takes Pollard's rho method to solve the hardest instances. We also show that the fields $\mathbb{F}_{q^3}$ are partially weak, that the fields $\mathbb{F}_{q^6}$ are potentially weak, and that the fields $\mathbb{F}_{q^8}$ are potentially partially weak. Finally, we argue that the other fields $\mathbb{F}_{2^N}$ where N is not divisible by 3, 5, 6, 7 or 8, are not weak under Hess' generalized GHS attack.

1. INTRODUCTION

The *elliptic curve discrete logarithm problem* (ECDLP) is the following: 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 $\lambda \in [0, r-1]$ such that $Q = \lambda P$. Intractability of the ECDLP is the basis for the security of all elliptic curve cryptographic systems.

The best general-purpose algorithm known for solving the ECDLP is Pollard's rho method [20, 19] which has a fully-exponential expected running time of $\sqrt{\pi r}/2$ point additions. For a fixed field $\mathbb{F}_q$, maximum resistance to Pollard's rho method is attained by selecting an elliptic curve E for which r is prime and as large as possible, i.e., $r \approx q$. The challenge faced by cryptanalysts is to devise faster ECDLP solvers for such curves. This has been accomplished for some special classes of elliptic curves, including those for which the order of q modulo r is small [4, 16], and for prime-field anomalous curves [21, 22, 23].

Date: September 8, 2004.
1991 *Mathematics Subject Classification.* 94A60.
Key words and phrases. Elliptic curve cryptography, Weil descent, Isogenies.

Recently Gaudry [8] used an index-calculus approach to solve the ECDLP on curves defined over $\mathbb{F}_{q^n}$ where n is composite. His method is asymptotically faster than Pollard's rho method when n is divisible by a small number greater than 2. For example, if $3|n$, then the running time of Gaudry's algorithm is $O(q^{10n/21+\epsilon})$, whereas Pollard's rho method has a running time of $O(q^{n/2+\epsilon})$. However, it has yet to be determined whether Gaudry's algorithm is indeed faster than Pollard's rho method for finite fields of sizes that might be deployed in practice, namely where $q^n \in [2^{160}, 2^{600}]$.

Weil descent. Frey [3] first proposed using Weil descent as a means to reduce the ECDLP in elliptic curves over extension fields $\mathbb{F}_{q^n}$ to the discrete logarithm problem (DLP) in the jacobian variety $J_C(\mathbb{F}_q)$ of an algebraic curve C of genus $g \geq 2$ over the proper subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^n}$. The hope was that index-calculus techniques could then be employed to solve the DLP in $J_C(\mathbb{F}_q)$ significantly faster than it takes Pollard's rho method to solving the original ECDLP instance in $E(\mathbb{F}_q)$. Later, Gaudry, Hess and Smart (GHS) [9] showed how Frey's methodology could be implemented in the case where the characteristic of $\mathbb{F}_{q^n}$ is 2 to obtain a hyperelliptic curve C. Their reduction was cryptographically significant because subexponential-time index-calculus algorithms are known [1, 7, 2] for solving the DLP in the jacobians of hyperelliptic curves. The GHS attack was shown to be ineffective in the case $\mathbb{F}_{q^n} = \mathbb{F}_{2^N}$ where $N \in [160, 600]$ is prime [17]. The case where $N \in [160, 600]$ is composite was studied in [15], and the elliptic curves most susceptible to the GHS attack were identified and enumerated.

Menezes, Teske and Weng [18] provided an exact (non-asymptotic) analysis of the GHS attack for the case $\mathbb{F}_{q^n} = \mathbb{F}_{2^{5l}}$. They showed that these fields were *weak* in the sense that any instance of the ECDLP 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. For example, the speedup for the case $\mathbb{F}_{q^n} = \mathbb{F}_{2^{600}}$ is by a factor of 2^{69}. We emphasize that the ECDLP over fields $\mathbb{F}_{2^{5l}}$ with $l \in [32, 120]$ is still intractable using existing computer technology (otherwise we would call these fields *bad*). Nevertheless, the results are cryptographically meaningful because they provide some evidence that the fields $\mathbb{F}_{2^{5l}}$ may be bad and therefore unsuitable for elliptic curve cryptography.

Our work. Recently, Hess [13] generalized the GHS attack whereby the curve C obtained is not necessarily hyperelliptic. The purpose of this paper is to explore the cryptographic implications of this generalized GHS attack. Our objective is to find new examples of weak fields. We stress that we are not interested in families of fields that are asymptotically weak, i.e., where the ECDLP can be solved faster than Pollard's rho method as the field size tends to infinity. Instead, we are interested in fields $\mathbb{F}_{2^N}$ where $N \in [160, 600]$ because these are the fields that might be used in practice.

Our analysis is incomplete because the curves C produced by the generalized GHS reduction have not been explicitly described and, in particular, we

do not have concrete measures of the cost of performing arithmetic in $J_C(\mathbb{F}_q)$ and of solving DLP instances in $J_C(\mathbb{F}_q)$ using index-calculus methods. We do, however, make reasonable assumptions about these costs and argue that our conclusions are cryptographically meaningful (cf. §3.3). If a field is found to be weak under these assumptions, then we call the field *potentially weak*. We call a field $\mathbb{F}_{2^N}$ *(potentially) partially weak* if the ECDLP for only a non-negligible proportion of all elliptic curves over $\mathbb{F}_{2^N}$ can be solved significantly faster than it takes Pollard's rho method to solve the hardest instances (under the aforementioned assumptions). By 'non-negligible proportion', we mean something like one-half or one-quarter. If a field can be shown to be (potentially) partially weak, then one could reasonably suspect that the field is (potentially) weak and therefore unsuitable for elliptic curve cryptography.

Subject to these assumptions, our results are the following:

(1) The fields $\mathbb{F}_{2^{7l}}$ and $\mathbb{F}_{2^{8l}}$ are potentially partially weak.
(2) The fields $\mathbb{F}_{2^{6l}}$ are potentially weak.
(3) The fields $\mathbb{F}_{2^{3l}}$ are partially weak.
(4) The weakness of $\mathbb{F}_{2^{7l}}$, $\mathbb{F}_{2^{6l}}$ and $\mathbb{F}_{2^{3l}}$ supports the contention in [18] that the field $\mathbb{F}_{2^{2\cdot 10}}$ is particularly weak.
(5) The fields $\mathbb{F}_{2^N}$ where N is not divisible by 3, 5, 6, 7 or 8, are not (potentially) weak under Hess' generalized GHS attack.

Organization. The remainder of this paper is organized as follows. Hess' generalized GHS attack is outlined in §2. §3 summarizes the running time of Pollard's rho method and the Enge-Gaudry algorithm, and discusses our assumptions about $J_C(\mathbb{F}_q)$. §4 reviews material on computing isogenies between elliptic curves. The vulnerability of the fields $\mathbb{F}_{2^{7l}}$, $\mathbb{F}_{2^{6l}}$ and $\mathbb{F}_{2^{3l}}$ to the generalized GHS attack are examined in §§5, 6 and 7, respectively. The results for $\mathbb{F}_{2^{2\cdot 10}}$ are summarized in §8. The remaining cases $\mathbb{F}_{2^N}$ where N is not divisible by 3, 6 or 7 are considered in §9. We draw our conclusions in §10 and list some open problems.

Notation. Let l and n be positive integers, and let $N = ln$. Let $q = 2^l$, and let $k = \mathbb{F}_q$ and $K = \mathbb{F}_{q^n}$. The absolute trace function $\mathrm{Tr} : K \to \mathbb{F}_2$ is defined by $\mathrm{Tr}(a) = \sum_{i=0}^{N-1} a^{2^i}$. The relative trace function $\mathrm{Tr}_{K/k} : K \to k$ is defined by $\mathrm{Tr}_{K/k}(a) = \sum_{i=0}^{n-1} a^{q^i}$. In general, for a subfield $K_1 = \mathbb{F}_{q^s}$ of K where $s|n$, the relative trace function $\mathrm{Tr}_{K/K_1} : K \to K_1$ is defined by $\mathrm{Tr}_{K/K_1}(a) = \sum_{i=0}^{\frac{n}{s}-1} a^{q^{is}}$. Let $\alpha \in K$ be an element with $\mathrm{Tr}(\alpha) = 1$. The $2(q^n - 1)$ isomorphism classes of non-supersingular elliptic curves defined over K have representatives

$$E_{a,b} = E \ : \ y^2 + xy = x^3 + ax^2 + b, \quad a \in \{0, \alpha\}, \ \ b \in K^*. \tag{1}$$

The set of all such representatives is denoted by $\mathcal{E}$. The subset of curves $E_{a,b} \in \mathcal{E}$ with $\mathrm{Tr}(a) = 0$ (resp. $\mathrm{Tr}(a) = 1$) is denoted $\mathcal{E}_0$ (resp. $\mathcal{E}_1$).

2. Generalized GHS Weil descent attack

Consider the elliptic curve $E = E_{a,b} \in \mathcal{E}$. We assume that $\#E(K) = dr$ where r is prime and d is small, whence $r \approx q^n$. These are the elliptic curves of interest in cryptographic applications[1]. Let $P \in E(K)$ be a point of order r.

For $\gamma \in K$, let $\mathrm{Ord}_\gamma(X)$ denote the unique polynomial $f \in \mathbb{F}_2[X]$ of least degree satisfying $f(\sigma)(\gamma) = 0$. Here, $\sigma : K \to K$ is the Frobenius automorphism defined by $\alpha \mapsto \alpha^q$. Also, if $f(X) = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}_2[X]$, then $f(\sigma)(\gamma) = \sum_{i=0}^{d} a_i \gamma^{q^i}$. Let $\gamma_1, \gamma_2 \in K$ such that $b = (\gamma_1\gamma_2)^2$. The following result from [18] is sometimes useful for determining when a suitable decomposion of b exists. Here, Φ denotes the Euler phi function for polynomials. For a divisor $m(X) \in \mathbb{F}_2[X]$ of $X^n + 1$, $\Phi(m(X))$ is the number of elements $\gamma \in \mathbb{F}_{q^n}$ with $\mathrm{Ord}_\gamma = m(X)$.

Theorem 1. *Let $n = n_1 n_2$, $K = \mathbb{F}_{q^n}$, $K_1 = \mathbb{F}_{q^{n_1}}$, and $k = \mathbb{F}_q$. Let $\beta \in K$.*

(i) *There exist γ_1, $\gamma_2 \in K$ with $\beta = \gamma_1\gamma_2$ and*

$$\mathrm{Ord}_{\gamma_1} | (X^{n_1} + 1) \text{ and } \mathrm{Ord}_{\gamma_2} | \frac{(X+1)(X^n+1)}{X^{n_1}+1}. \tag{2}$$

(ii) *If $\mathrm{Tr}_{K/K_1}(\beta) \neq 0$ then $\gamma_1 = \mathrm{Tr}_{K/K_1}(\beta)$ and $\gamma_2 = \beta/\gamma_1$ satisfy (2).*

(ii) *If $\mathrm{Tr}_{K/K_1}(\beta) = 0$ then $\gamma_1 = 1$ and $\gamma_2 = \beta$ satisfy (2).*

(iv) *Suppose that $\beta = \delta_1\delta_2$, where $\mathrm{Ord}_{\delta_1} = m_1(X) | (X^{n_1}+1)$ and $\mathrm{Ord}_{\delta_2} = m_2(X) | (X+1)(X^n+1)/(X^{n_1}+1)$, and suppose that $\mathrm{Tr}_{K/K_1}(\beta) \neq 0$. Let $B = \{\gamma_1\gamma_2 : \mathrm{Ord}_{\gamma_1} = m_1(X) \text{ and } \mathrm{Ord}_{\gamma_2} = m_2(X)\}$. Then $\#B = \Phi(m_1(X))\Phi(m_2(X))/(q-1)$.*

Now let $s_1 = \deg(\mathrm{Ord}_{\gamma_1})$, $s_2 = \deg(\mathrm{Ord}_{\gamma_2})$, and

$$t = \begin{cases} \deg(\mathrm{lcm}(\mathrm{Ord}_{\gamma_1}, \mathrm{Ord}_{\gamma_2})), & \text{if } \mathrm{Tr}(a) = 0, \\ \deg(\mathrm{lcm}(\mathrm{Ord}_{\gamma_1}, \mathrm{Ord}_{\gamma_2}, X+1)), & \text{if } \mathrm{Tr}(a) = 1. \end{cases}$$

If $\mathrm{Tr}(a) = 1$, then we further assume that

$$\text{either } \mathrm{Tr}_{K/k}(\gamma_1) \neq 0 \text{ or } \mathrm{Tr}_{K/k}(\gamma_2) \neq 0. \tag{3}$$

Via a birational transformation the defining equation of E can be brought into the form $y^2 + y = \gamma_1/x + a + \gamma_2 x$. Then Hess' generalization [13, Theorems 11,12] of the GHS reduction constructs an explicit group homomorphism

$$\phi : E(K) \to J_C(k), \tag{4}$$

where C is a curve defined over k of genus

$$g = 2^t - 2^{t-s_1} - 2^{t-s_2} + 1. \tag{5}$$

[1] In particular, we are not interested in *subfield curves*, i.e., elliptic curves E defined over K whose isomorphism class has a representative $E_{a,b}$ such that $L = \mathbb{F}_2(a,b)$ is a proper subfield of K. For such curves, $\#E(L) | \#E(K)$ and hence the ECDLP in $E(K)$ can already be solved in significantly fewer than $\sqrt{q^n}$ steps.

Remark 2. (*generalized GHS versus GHS*) The generalized GHS reduction specializes to the GHS reduction [9] by selecting $\gamma_1 = 1$ and $\gamma_2 = b^{1/2}$. Then condition (3) is equivalent to: either n is odd or $(X+1)^u | \mathrm{Ord}_b$, where $u = v_2(n)$. Furthermore, if we define

$$m = \begin{cases} \deg(\mathrm{Ord}_b), & \text{if } (X+1)|\mathrm{Ord}_b, \\ \deg(\mathrm{Ord}_b)+1, & \text{if } (X+1) \nmid \mathrm{Ord}_b, \end{cases}$$

then C is a hyperelliptic curve of genus g where

$$g = \begin{cases} 2^{m-1}, & \text{if } (X+1)|\mathrm{Ord}_b, \\ 2^{m-1}-1, & \text{if } (X+1) \nmid \mathrm{Ord}_b. \end{cases}$$

Generalized GHS attack. The procedure for finding $\lambda = \log_P Q$ where P is a point of order r on the elliptic curve $E_{a,b}$, and $Q \in \langle P \rangle$, is the following:

(1) Select a divisor $n \geq 2$ of N.
(2) Select $\gamma_1, \gamma_2 \in K$ such that $b = (\gamma_1\gamma_2)^2$ (and such that $\mathrm{Tr}_{K/k}(\gamma_1) \neq 0$ or $\mathrm{Tr}_{K/k}(\gamma_2) \neq 0$ if $\mathrm{Tr}(a) = 1$).
(3) Use the generalized GHS reduction [13] to construct a curve C and map the points P, Q to divisors D_P, D_Q in $J_C(k)$.
(4) Compute $\lambda = \log_{D_P} D_Q$ in $J_C(k)$.

Remark 3. (*selection of n, γ_1 and γ_2*) The parameters n, γ_1, γ_2 should be selected so that the running time of the best DLP solver for $J_C(k)$ is minimized. Since $\#J_C(k) \approx q^g$ and $J_C(k)$ should contain a subgroup of order $r \approx q^n$, we also require that $g \geq n$. In the ideal situation, we would have $g \approx n$ because then $\#J_C(k) \approx \#E(K)$. Note that since Ord_{γ_1} and Ord_{γ_2} are divisors of $X^n + 1$, we have $t \leq n$ and $g \leq 2^n - 1$. Thus, the optimum selection of n, γ_1, and γ_2 will depend on the degrees of the irreducible factors of $X^n + 1$ over $\mathbb{F}_2$ over all divisors $n \geq 2$ of N.

Remark 4. (*efficiency of determining C and ϕ*) The running time complexity of the algorithms in [13] for finding the defining equation of C and for computing ϕ has not been determined. However, if n is relatively small, as will be the case in §§5–9, then this time will be dominated by the time it takes to solve the DLP in $J_C(k)$. Hence our analyses will ignore the running times for computing C and ϕ.

3. Analysis of discrete logarithm algorithms

3.1. **Pollard's rho method.** The instances of the ECDLP over $\mathbb{F}_{2^N}$ most resistant to Pollard's rho method 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 $E(\mathbb{F}_{2^N})$. When mixed affine-projective coordinates are employed, an elliptic curve operation requires 8 multiplications in $\mathbb{F}_{2^N}$. Thus the expected running time of Pollard's rho method is $R_\rho \approx c_N 2^{0.5(N+5)}$, where c_N is the cost of a multiplication in $\mathbb{F}_{2^N}$. Since we will only be concerned with rough (but reasonably

good) approximations, we will ignore the factor c_N and henceforth use the estimate

$$R_\rho \approx 2^{0.5(N+5)}. \tag{6}$$

3.2. **Enge-Gaudry index-calculus algorithm.** Let C be a hyperelliptic curve of genus g defined over $k = \mathbb{F}_q = \mathbb{F}_{2^l}$. The Enge-Gaudy algorithm [7, 2] is a subexponential-time index-calculus method for solving the DLP in $J_C(\mathbb{F}_q)$.

First, a *factor base* of size w is chosen. For curves of low genus, the factor base will consist of (half) of all degree one divisors in $J_C(\mathbb{F}_q)$, so $w \approx q/2$. Next, in the *relation generation* stage, slightly more than w linear relations of factor base elements are found. The expected running time of this stage is $R_{\rm RG} \approx (c_J + c_S)\frac{q}{2}g!$, where c_J is the cost of an addition in $J_C(\mathbb{F}_q)$, and c_S is the cost of testing whether a monic polynomial $a(u) \in \mathbb{F}_q[u]$ of degree (at most) g is 1-smooth. As discussed in [18], the cost c_J has experimentally been found to be less than c_S for the values of g and $\mathbb{F}_q$ of interest in this paper. The dominant computation in smoothness testing is the evaluation of $u^{2^l} \bmod a$, which can be done by first iteratively computing $u^{2i} \bmod a$ for $1 \leq i \leq g-1$, and then computing $u^{2^i} \bmod a$ for $1 \leq i \leq l$ by successive squarings. This can be done with $2g(\lceil g/2 \rceil - 1) + lg\lceil g/2 \rceil \approx g^2 l/2$ multiplications in $\mathbb{F}_{2^l}$. Ignoring the cost of a multiplication in $\mathbb{F}_{2^l}$, we get the estimate

$$R_{\rm RG} \approx \frac{g^2 lq}{4} g!. \tag{7}$$

Finally, a linear system of dimension slightly more than w and having about g non-zero coefficients per equation is solved using Lanczos' algorithm. This *linear algebra* stage has running time $R_{\rm LA} \approx c_r \frac{gq^2}{4}$, where c_r is cost of a multiplication modulo an N-bit integer. We will henceforth ignore the factor c_r and use the approximation

$$R_{\rm LA} \approx \frac{gq^2}{4}. \tag{8}$$

3.3. **Hess' index-calculus algorithm.** Suppose now that C is a curve of genus g over $k = \mathbb{F}_q = \mathbb{F}_{2^l}$ that was the result of Hess' generalized GHS reduction (see §2). The curve C is in general not hyperelliptic. This makes an exact analysis of the generalized GHS attack difficult for two reasons.

The first is that a precise cost of performing arithmetic in $J_C(k)$ is not known. Hess' algorithm [11] for performing an addition in $J_C(k)$ takes $O(g^4)$ k-operations, which is slower than Cantor's algorithm for hyperelliptic curves which takes $O(g^2)$ k-operations. In our analyses, we will make the following assumption.

Assumption A. Let C be a (non-hyperelliptic) curve that is produced by the generalized GHS reduction. The cost of an addition operation in $J_C(k)$

is approximately the same as the cost of an addition operation in the case that C is hyperelliptic.

The second difficulty is that good estimates of the running times of index-calculus algorithms for solving the DLP in $J_C(k)$ are not available. Hess' algorithm [12] has a subexponential running time of $O(L_{q^g}[\frac{1}{2}])$, where $L_n[d] = \exp((c + o(1))(\log n)^d(\log\log n)^{1-d})$, but an exact analysis has not been done. Nevertheless, when analyzing the generalized GHS attack, we will make the following assumption.

Assumption B. Let C be a (non-hyperelliptic) curve that is produced by the generalized GHS reduction. The cost of finding discrete logarithms in $J_C(k)$ is approximately the same as the cost of the Ege-Gaudry algorithm in the case that C is hyperelliptic.

Under these assumptions, the expected time so solve an instance of the DLP in $J_C(k)$ is $R_{\mathrm{RG}} + R_{\mathrm{LA}}$, where R_{RG}, R_{LA} are as defined in (7), (8).

Remark 5. (*reasonableness of Assumptions A and B*) One would expect that the best algorithms for adding in $J_C(k)$ and computing logarithms are significantly slower (and certainly not any faster) when C is non-hyperelliptic than the algorithms when C is hyperelliptic. However, the conclusions drawn in this paper under Assumptions A and B remain valid even if the non-hyperelliptic algorithms were several orders of magnitude slower than their hyperelliptic counterparts. Thus we maintain that our results about the potential or partial weakness of a field are meaningful in practice.

4. Random walks in isogeny classes of elliptic curves

Two elliptic curves E, $E' \in \mathcal{E}$ are said to be isogenous (over K) if $\#E(K) = \#E'(K)$; we write $E \sim E'$. The equivalence classes with respect to isogeny are called isogeny classes.

Suppose now that $\mathcal{W} \subset \mathcal{E}$ is a set of elliptic curves that are vulnerable to the generalized GHS attack, and suppose that $E \notin \mathcal{W}$. A strategy, first proposed by Galbraith, Hess and Smart [6], for attacking an ECDLP instance for E is to find an elliptic curve $E' \in \mathcal{W}$ that is isogenous to E, and then map the ECDLP instance to E' using an isogeny $\psi : E \to E'$.

One approach for finding E' is to perform a random walk in the set of elliptic curves isogenous to E. For each elliptic curve E'' encountered in this walk, we must be able to efficiently determine whether $E'' \in \mathcal{W}$. In the remainder of this section, we outline the random walk method from [6] (see also [18]). The problem of deciding whether $E'' \in \mathcal{W}$ is tackled in §§5–9 for particular choices of $\mathcal{W}$.

Recall that $t = q^n + 1 - \#E(K)$ is the trace of E, and $\Delta = t^2 - 4 \cdot q^n$ its discriminant. 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 q^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 $\mathrm{End}(E) = \mathrm{End}(E')$.

For any elliptic curve $E \in \mathcal{E}$ we can use an algorithm of Kohel [14] to compute a chain of isogenies defined over K from E to an elliptic curve $E' \in \mathcal{E}$ 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 the other steps of the generalized GHS attack considered in §§5–9. For the following, we therefore may assume that $\mathrm{End}(E)$ is maximal. Then there is one-to-one correspondence between $\mathcal{C}(E)$ and the ideal class group Cl of the maximal order $\mathcal{O}$.

In our random walk, we have to make the following heuristic assumption about the distribution of vulnerable curves among endomorphism classes.

Assumption C. Let $\mathcal{X} \subseteq \mathcal{E}$ be the set of elliptic curves that belong to an isogeny class of some curve in $\mathcal{W}$, and let $\#\mathcal{W}/\#\mathcal{X} = 2^{-v}$. Let $E \in \mathcal{X}$. Then the proportion of curves in $\mathcal{C}(E)$ that belong to $\mathcal{W}$ is 2^{-v}.

Remark 6. (*restriction of Assumption C*) Of course, Assumption C is not accurate if $\#E(K)$ lies at the extreme ends of the Hasse interval, or if Δ has a very large square factor; in either case $\#\mathcal{C}(E) = \#\mathrm{Cl}$ is very small. However, the former affects only a very small fraction of the elliptic curves over K, while the latter is most unlikely for non-subfield curves.

Given a curve $E \in \mathcal{X}$, it is now possible to compute a curve $E' \in \mathcal{W}$ isogenous to E along with a chain of low-degree isogenies from E to E'. This is based on ideas from [6] to simulate a random walk in the endomorphism class of E, exploiting the aforementioned one-to-one correspondence between Cl and $\mathcal{C}(E)$. The random walk works as follows: Let $E = E_{a,b}$, 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 K [5]. These roots can be computed by a probabilistic algorithm using $O(Np^2)$ operations in K. The two isogenies mapping E to $E_{a,j_1^{-1}}$ and $E_{a,j_2^{-1}}$ 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 [6], 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 16 smallest odd 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 $E_0 = E_{a,b}$ and $b_0 = b$ and $\mathfrak{a}_0 = \mathcal{O}$. For $i = 1, 2, \ldots$, let $p \in_R \mathcal{P}$ and $j = b_{i-1}^{-1}$, and compute the two roots in K 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 i, the ideal $\mathfrak{a}_i$ corresponds to the isogeny mapping E to E_i.

Based on [24], and on extensive experimental evidence in this particular application, the choice of $\mathcal{P}$ is so that the walk (E_i) simulates a random walk in the endomorphism class of E. Also, considering 20000 randomly chosen discriminants of various bitlengths, we found that $\max\{p \in \mathcal{P}\} < 313$ for all cases. Thus, each random walk step takes on average up to about $\frac{1}{3}N(\max\{p \in \mathcal{P}\})^2 \approx N \cdot 2^{15}$ operations in K, given that computing the roots of the modular polynomial is by far the most time-consuming step.

Now, under Assumption C, after expected 2^v random-walk steps in $\mathcal{C}(E)$ an elliptic curve $E' \in \mathcal{W}$ is encountered that is isogenous to E. Thus, altogether it takes something on the order of

$$R_{\mathrm{W}} = N2^{v+15} \tag{9}$$

operations in K to find a curve in $\mathcal{W}$ isogenous to a given curve, along with an ideal $\mathfrak{a}$ that represents the isogeny between the two curves. We note that this step can be efficiently parallelized.

The remaining steps to compute the explicit isogeny between E and E' are identical with Stages 2 and 3 of [6]: 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 $O(2^{N/4+\varepsilon})$. Since this time is less than the expected running time of the random walk for the scenarios in this paper, the time to compute the isogeny will be ignored.

Remark 7. (*further speed-up of the random walk*) The analysis above is generous since, for example, for more than half of all randomly chosen discriminants, only primes ≤ 157 were needed to generate a set $\mathcal{P}$ of 16 split primes. Working with $\max\{p \in \mathcal{P}\} = 157$ yields a gain of a factor 3.6. In case $\mathcal{P}$ contains primes larger than 157, one might want to choose not to use those primes as often as the smaller primes, or not to use them at all. This may require slightly more random walk steps to find a curve $E' \in \mathcal{W}$, but the steps are cheaper on average. Also, using Karatsuba arithmetic to compute the roots of $\Phi_p(j, X)$ may accelerate this step by another factor of 10 for the larger primes.

5. The case $n = 7$

Suppose now that $n = 7$, $N = 7l$, $K = \mathbb{F}_{2^{7l}}$, $q = 2^l$, and $k = \mathbb{F}_q$. The factorization of $X^7 + 1$ over $\mathbb{F}_2$ is:

$$X^7 + 1 = (X + 1)(X^3 + X + 1)(X^3 + X^2 + 1).$$

We argue that the fields $\mathbb{F}_{2^{7l}}$ are potentially partially weak for elliptic curve cryptography by showing that the set $\mathcal{X}$ of all non-subfield curves in $\mathcal{E}_0$ are (potentially) vulnerable to the generalized GHS attack.

5.1. **Elliptic curves over $\mathbb{F}_{2^{7l}}$ with $\mathrm{Tr}(a) = 0$.** Let $\mathcal{W}_0$ be the set of elliptic curves $E_{a,b} \in \mathcal{E}_0$ with $b = (\gamma_1\gamma_2)^2$, where either $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3+X+1$ or $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3+X^2+1$. For each $E \in \mathcal{W}_0$ we have $s_1 = s_2 = t = 3$, and hence the generalized GHS reduction with $n = 7$ yields a curve C of genus $g = 7$ over $\mathbb{F}_{2^l}$. Note that $\#J_C(\mathbb{F}_{2^l}) \approx \#E(\mathbb{F}_{2^{7l}})$.

Our strategy for solving an instance of the ECDLP on a given elliptic curve $E_{a,b} \in \mathcal{X}$ is the following:

(1) Use Kohel's algorithm to compute a chain of isogenies defined over K to an elliptic curve $E' \in \mathcal{E}_0$ with $\mathrm{End}(E') = \mathcal{O}$.
(2) Perform a random walk in the set of elliptic curves isogenous to E' until an elliptic curve $E'' \in \mathcal{W}_0$ is found, and compute the corresponding isogeny between E' and E''.
(3) Use the isogenies to map the ECDLP instance in E to an ECDLP instance in E''.
(4) Perform the GHS reduction on E'' to obtain a curve C and an instance of the DLP in $J_C(k)$.
(5) Solve the instance of the DLP in $J_C(k)$.

Steps 1, 2 and 3 were outlined in §4, while steps 4 and 5 were considered in §2. To complete the description and analysis of step 2, we need to provide an algorithm for deciding whether an elliptic curve is in $\mathcal{W}_0$, and to estimate the expected number of random walk steps.

5.1.1. *Decomposition algorithm.*

Algorithm 8. (*Finding a decomposition of b*)
Input: $b \in \mathbb{F}_{q^7}^*$.
Output: $\gamma_1, \gamma_2 \in \mathbb{F}_{q^7}^*$ such that $b = (\gamma_1\gamma_2)^2$ and either $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X + 1$ or $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X^2 + 1$; or "failure".

(1) Let $\beta = b^{1/2}$ and $q = 2^l$.
(2) {Check for a decomposition with $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X + 1$.}
  (a) Let $w(u) = u^2 + (\beta^{q^3-1} + \beta^{q-1} + 1)u + \beta^{q-1} \in \mathbb{F}_{q^7}[u]$.
  (b) {Find the roots of $w(u)$ in $\mathbb{F}_{q^7}$, if any.}
  If $\gcd(w(u), u^{q^7} - u) \neq 1$ then find $u_0, u_1 \in \mathbb{F}_{q^7}$ such that $w(u_0) = w(u_1) = 0$; else go to step 3.
  (c) Let $S \subset \{u_0, u_1\}$ be the set of the u_i that satisfy $u_i^{q^2+q+1} + u_i + 1 = 0$. If $S = \emptyset$ then go to step 3.
  (d) For $u_i \in S$, check if $u_i^{(q^7-1)/(q-1)} = 1$. If no u_i satisfies this condition, then go to step 3; otherwise, assume u_0 passed the test.
  (e) Compute some $\gamma_1 \in \mathbb{F}_{q^7}^*$ such that $\gamma_1^{q-1} = u_0$ (cf. Lemma 9).
  (f) Let $\gamma_2 = \beta/\gamma_1$ and return (γ_1, γ_2).
(3) {Check for a decomposition with $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X^2 + 1$.}
  (a) Let $w(u) = u^2 + (\beta^{q^3-1} + \beta^{q^2-1} + 1)u + \beta^{q^2-1} \in \mathbb{F}_{q^7}[u]$.

(b) {Find the roots of $w(u)$ in $\mathbb{F}_{q^7}$, if any.}
If $\gcd(w(u), u^{q^7} - u) \neq 1$ then find $u_0, u_1 \in \mathbb{F}_{q^7}$ such that $w(u_0) = w(u_1) = 0$; else return("failure").
(c) Compute $s = (q+1)^{-1} \bmod q^7 - 1$.
(d) Let $S \subset \{u_0, u_1\}$ be the set of the u_i that satisfy $u_i^{q+s} + u_i + 1 = 0$. If $S = \emptyset$ then return("failure").
(e) For $u_i \in S$, check if $u_i^{s(q^7-1)/(q-1)} = 1$. If no u_i satisfies this condition, then return("failure"); otherwise, assume u_0 passed the test.
(f) Compute some $\gamma_1 \in \mathbb{F}_{q^7}^*$ such that $\gamma_1^{q-1} = u_0^s$ (cf. Lemma 9).
(g) Let $\gamma_2 = \beta/\gamma_1$ and return (γ_1, γ_2).

Lemma 9. *Let $u \in \mathbb{F}_{q^7}^*$ such that $u^{(q^7-1)/(q-1)} = 1$. Then we can compute $\gamma \in \mathbb{F}_{q^7}^*$ such that $u = \gamma^{q-1}$ in subexponential time.*

Proof. Let α be a generator of $\mathbb{F}_{q^7}^*$. By solving an instance of the DLP in $\mathbb{F}_{q^7}^*$ we can find an integer d such that $u = \alpha^d$. Since $u^{(q^7-1)/(q-1)} = 1$, it follows that $(q-1)|d$. Then $\gamma = \alpha^{d/(q-1)}$ satisfies $\gamma^{q-1} = u$. □

Note that step 2e or step 3f in Algorithm 8 will be executed exactly once in the random walk (see §4). Thus the time to solve the DLP instance in $\mathbb{F}_{q^7}^*$ will not be a bottleneck in the generalized GHS attack. Moreover, Algorithm 8 with the exclusion of steps 2e and 3f takes less time than a random walk step. Thus, we will ignore the cost of Algorithm 8 in our analysis.

Theorem 10. *Algorithm 8 outputs $\gamma_1, \gamma_2 \in \mathbb{F}_{q^7}^*$ such that $b = (\gamma_1\gamma_2)^2$ and either $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X + 1$ or $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X^2 + 1$ if and only if such γ_1, γ_2 exist.*

Proof. Let $\beta = b^{1/2}$. Let us first assume that there exist $\gamma_1, \gamma_2 \in \mathbb{F}_{q^7}^*$ such that $\beta = \gamma_1\gamma_2$ and $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X + 1$. Then

$$\gamma_1^{q^3} + \gamma_1^q + \gamma_1 = 0 \quad \text{and} \quad (\beta/\gamma_1)^{q^3} + (\beta/\gamma_1)^q + \beta/\gamma_1 = 0,$$

or, equivalently,

$$\gamma_1^{q^3-1} + \gamma_1^{q-1} + 1 = 0 \quad \text{and} \quad \beta^{q^3-1} + \frac{\gamma_1^{q^3-1}}{\gamma_1^{q-1}}\beta^{q-1} + \gamma_1^{q^3-1} = 0. \tag{10}$$

Let $v = \gamma_1^{q-1}$. Then $\gamma_1^{q^3-1} = 1+v$, $\gamma_1^{q^3-1}/\gamma_1^{q-1} = (1+v)/v$, and (10) becomes

$$v^{q^2+q+1} + v + 1 = 0 \quad \text{and} \quad v^2 + (1 + \beta^{q-1} + \beta^{q^3-1})v + \beta^{q-1} = 0. \tag{11}$$

The quadratic equation in (11) is the equation $w(v) = 0$, where $w(u) \in \mathbb{F}_{q^7}[u]$ is as in step 2a in Algorithm 8. Thus v is a root of $w(u)$ and also satisfies $v^{q^2+q+1} + v + 1 = 0$. Furthermore, v is a $(q-1)$-th power and therefore $\mathrm{ord}(v)|(q^7-1)/(q-1)$. Consequently, Algorithm 8 terminates in step 2f

with output (γ_1, γ_2) that satisfies the requisite conditions. Conversely if Algorithm 8 terminates in step 2f with output (γ_1, γ_2), then $b = (\gamma_1\gamma_2)^2$. Let $u = \gamma_1^{q-1}$. Then, by construction, u satisfies (11) which implies that $\gamma_i^{q^3} + \gamma_i^q + \gamma_i = 0$ for $i = 1, 2$. Since $\gamma_i \neq 0$, we have $\mathrm{Ord}_{\gamma_i} = X^3 + X + 1$.

To complete the proof, we have to prove the analogue results for step 3. Note that if there exist $\gamma_1, \gamma_2 \in \mathbb{F}_{q^7}^*$ such that $\beta = \gamma_1\gamma_2$ and $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X^2 + 1$, then

$$\gamma_1^{q^3-1} + \gamma_1^{q^2-1} + 1 = 0 \quad \text{and} \quad \beta^{q^3-1} + \frac{\gamma_1^{q^3-1}}{\gamma_1^{q^2-1}}\beta^{q^2-1} + \gamma_1^{q^3-1} = 0. \tag{12}$$

Let $v = \gamma_1^{q^2-1}$, and let $s = (q+1)^{-1} \mod q^7 - 1$. Then $\gamma_1^{q^3-1} = v^{q+s}$, $\gamma_1^{q^3-1}/\gamma_1^{q^2-1} = (1+v)/v$, and (12) becomes

$$v^{q+s} + v + 1 = 0 \quad \text{and} \quad v^2 + (1 + \beta^{q^2-1} + \beta^{q^3-1})v + \beta^{q^2-1} = 0.$$

The rest of the proof is similar to that for step 2. □

5.1.2. *Expected number of random walk steps.* Let

$$\begin{aligned} A &= \{\gamma_1 \in \mathbb{F}_{q^7} \,:\, \mathrm{Ord}_{\gamma_1} = X^3 + X + 1\}\,, \\ B &= \{\gamma_1\gamma_2 \,:\, \gamma_1, \gamma_2 \in A\}\,. \end{aligned}$$

We will argue heuristically that $\#B = (q^3-1)(q^2+q+2)/2$. For this, let $T = \#A = q^3 - 1$. Then $\#B \leq \#\{(\gamma_1, \gamma_2) \in A \times A\} = T^2$.

Now, if $\gamma_1, \gamma_2 \in A$, then $\lambda\gamma_1, \lambda^{-1}\gamma_2 \in A$ for each $\lambda \in \mathbb{F}_q^*$, and (γ_1, γ_2) and $(\lambda\gamma_1, \lambda^{-1}\gamma_2)$ represent the same $\beta \in B$. Thus, $\#B \leq T^2/(q-1)$.

Further, (γ_1, γ_2) and (γ_2, γ_1) always represent the same $\beta \in B$. Now assume $\gamma_1\gamma_2 = \delta_1\delta_2$ with $\gamma_1, \gamma_2, \delta_1, \delta_2 \in A$ and $\gamma_1 \neq \lambda\delta_1, \lambda\delta_2$ for all $\lambda \in \mathbb{F}_q^*$. Let $\lambda \in \mathbb{F}_{q^7} \setminus \mathbb{F}_q$ such that $\delta_1 = \lambda\gamma_1$. For a given γ_1, there are $q^3 - q$ values $\lambda' \in \mathbb{F}_{q^7} \setminus \mathbb{F}_q$ such that $\lambda'\gamma_1 \in A$. But then for the particular λ, it is highly unlikely that $\lambda^{-1}\gamma_2$ is also in A, given that the proportion q^3/q^7 is extremely small. Thus, heuristically, the only repeated representations of $\beta = \gamma_1\gamma_2$ for $(\gamma_1, \gamma_2) \in A \times A$ are of the form $\beta = (\lambda\gamma_1)(\lambda^{-1}\gamma_2)$ or $\beta = \gamma_2\gamma_1$.

To estimate the effect on $\#B$ caused by symmetries, we call two pairs (γ_1, γ_2), $(\delta_1, \delta_2) \in A \times A$ equivalent if there exists $\lambda \in \mathbb{F}_q^*$ such that $\gamma_1 = \lambda\delta_1$ and $\gamma_2 = \lambda^{-1}\delta_2$. This is an equivalence relation, and there are $T^2/(q-1)$ equivalence classes. Let G be such an equivalence class. Now, if $(\gamma, \gamma) \in G$ for some $\gamma \in A$, then for any $(\gamma_1, \gamma_2) \in G$ we have $(\gamma_1, \gamma_2) \sim (\gamma_2, \gamma_1)$. There are T such classes, which altogether make up T distinct values $b \in B$. On the other hand, if G does not contain a pair (γ, γ), then, if $(\gamma_1, \gamma_2) \in G$ necessarily $(\gamma_2, \gamma_1) \in G' \neq G$. This is because $\#G = q - 1$, which is odd. Furthermore, if $(\delta_1, \delta_2) \sim (\gamma_1, \gamma_2) \in G$ then $(\delta_2, \delta_1) \sim (\gamma_2, \gamma_1) \in G'$. Consequently, the $T^2/(q-1) - T$ equivalence classes that do not contain a pair (γ, γ) account for $(T^2/(q-1) - T)/2$ distinct values $\beta \in B$.

Along with the heuristic explanation above, this yields $\#B = T + (T^2/(q-1) - T)/2 = (q^3-1)(q^2+q+2)/2$. (This has been confirmed experimentally for $N = 7, 14, 21$.)

The same holds for the case $\mathrm{Ord}_\gamma = X^3 + X^2 + 1$. However, there may or may not be a significant overlap for the two corresponding sets B. We therefore simply estimate $\#\mathcal{W}_0 \approx q^5/2$.

Consequently, under Assumption C, expected $2q^2$ random walk steps in the endomorphism class of an elliptic curve $E' \in \mathcal{X}$ need to be executed until a curve $E'' \in \mathcal{W}_0$ is found.

5.1.3. *Analysis.* For selected values of N, Table 1 compares the expected running time R_ρ (see equation (6)) for solving the ECDLP in an elliptic curve in $\mathcal{X}$ with the running times R_{RG}, R_{LA}, R_{W} (see equations (7), (8), (9)) of the dominant stages of the generalized GHS attack. The values R_{RG}, R_{LA} are for hyperelliptic curves, so Assumptions A and B are under effect. The value for R_{W} relies on Assumption C. Since $R_{\mathrm{W}} \ll R_\rho$, we conclude

N	l	$\log_2 R_\rho$	$\log_2 R_{\mathrm{RG}}$	$\log_2 R_{\mathrm{LA}}$	$\log_2 R_{\mathrm{W}}$
161	23	83	43	47	69
210	30	108	51	61	84
301	43	153	64	87	110
399	57	202	79	115	139
497	71	251	93	143	167
595	85	300	107	171	195

TABLE 1. Time estimates for the generalized GHS attack with $n = 7$ (under Assumptions A, B and C). An ECDLP instance in $E_{a,b}(\mathbb{F}_{2^{7l}})$ where $\mathrm{Tr}(a) = 0$ is reduced to a DLP instance in $J_C(\mathbb{F}_{2^l})$ where C is a genus 7 curve.

that the fields $\mathbb{F}_{2^{7l}}$ are potentially partially weak. Note that $R_{\mathrm{RG}} \ll R_{\mathrm{W}}$, so the veracity of our conclusion remains unchanged even if DLP algorithms for the non-hyperelliptic curve C are significantly slower than their hyperelliptic curve counterparts.

5.2. **Elliptic curves over $\mathbb{F}_{2^{7l}}$ with $\mathrm{Tr}(a) = 1$.** Let $\mathcal{W}_1$ be the set of elliptic curves $E_{a,b} \in \mathcal{E}_1$ with $b = (\gamma_1\gamma_2)^2$, where either[2] $\mathrm{Ord}_{\gamma_1} = X^3 + X + 1$ and $\mathrm{Ord}_{\gamma_2} = (X^3 + X + 1)(X + 1)$, or $\mathrm{Ord}_{\gamma_1} = X^3 + X^2 + 1$ and $\mathrm{Ord}_{\gamma_2} = (X^3 + X^2 + 1)(X + 1)$. Thus $\mathrm{Tr}_{K/k}(\gamma_2) \neq 0$. For each $E \in \mathcal{W}_1$ we have $s_1 = 3$, $s_2 = 4$, $t = 4$, and hence the generalized GHS reduction with $n = 7$ yields a curve C of genus $g = 14$ over $\mathbb{F}_{2^l}$. Under assumptions A and B, the DLP in $J_C(\mathbb{F}_{2^l})$ can be solved significantly faster than Pollard's rho method.

[2]We cannot take $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X + 1$ or $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^3 + X^2 + 1$ as in the case of $E_{a,b} \in \mathcal{E}_0$ because then $\mathrm{Tr}_{K/k}(\gamma_1) = \mathrm{Tr}_{K/k}(\gamma_2) = 0$, in violation of condition (3).

Now, we expect that $\#\mathcal{W}_1 \approx q^6$. Hence to attack a given non-subfield elliptic curve in $\mathcal{E}_1$, one expects to perform about q random walk steps in an isogeny class before a curve in $\mathcal{W}_1$ is encountered. Unfortunately, we were unable to devise an efficient algorithm for deciding whether an element $b \in \mathbb{F}_{2^{7l}}$ admits a decomposition $b = (\gamma_1\gamma_2)^2$ with γ_1, γ_2 satisfying the above conditions (and to find such a decomposition if it exists). The running time of such an algorithm would have to be significantly less than $q^{2.5}$, otherwise the random walk would be slower than Pollard's rho method for solving the original ECDLP instance.

Thus we do not have any arguments to support the weakness of all elliptic curves in $\mathcal{E}_1$ under the generalized GHS attack with $n = 7$.

6. The case $n = 6$

Suppose now that $n = 6$, $N = 6l$, $K = \mathbb{F}_{2^{6l}}$, $K_1 = \mathbb{F}_{2^{3l}}$, $q = 2^l$, and $k = \mathbb{F}_q$. We give two arguments for the potential weakness of the fields $\mathbb{F}_{2^{6l}}$.

The factorization of $X^6 + 1$ over $\mathbb{F}_2$ is:

$$X^6 + 1 = (X + 1)^2(X^2 + X + 1)^2.$$

Let $\mathcal{W}$ be the set of elliptic curves $E_{a,b} \in \mathcal{E}$ over $\mathbb{F}_{q^6}$ with $b = (\gamma_1\gamma_2)^2$, where $\mathrm{Ord}_{\gamma_1} = X^3 + 1$ and $\mathrm{Ord}_{\gamma_2} = (X + 1)(X^3 + 1)$. For each $E \in \mathcal{W}$ we have $s_1 = 3$ and $s_2 = t = 4$, and so the generalized GHS reduction with $n = 6$ yields a curve C of genus 14 over $\mathbb{F}_q$. Note also that $\mathrm{Tr}_{K/K_1}(b) \neq 0$. This is because $\gamma_1 \in \mathbb{F}^*_{q^3}$, so $\mathrm{Tr}_{K/K_1}(b) = (\mathrm{Tr}_{K/K_1}(\gamma_1\gamma_2))^2 = (\gamma_1\mathrm{Tr}_{K/K_1}(\gamma_2))^2$. If $\mathrm{Tr}_{K/K_1}(b) = 0$, then $\mathrm{Tr}_{K/K_1}(\gamma_2) = 0$, and hence $\mathrm{Ord}_{\gamma_2} | (X^3 + 1)$ which is not possible.

Theorem 11. *Let $E = E_{a,b} \in \mathcal{E}$ with $\mathrm{Tr}_{K/K_1}(b) \neq 0$. Let $\beta = b^{1/2}$, $\gamma_1 = \mathrm{Tr}_{K/K_1}(\beta)$, and $\gamma_2 = \beta/\gamma_1$. We have $E \in \mathcal{W}$ if and only if $\mathrm{Ord}_{\gamma_1} = X^3 + 1$ and $\mathrm{Ord}_{\gamma_2} \neq X^2 + 1$. Moreover $\#\mathcal{W} = 2q(q - 1)(q^2 - 1)^2 \approx 2q^6$.*

Proof. Let

$$\begin{aligned} A_1 &= \{\delta_1 \in \mathbb{F}_{q^6} \,:\, \mathrm{Ord}_{\delta_1} = X^3 + 1\}\,, \\ A_2 &= \{\delta_2 \in \mathbb{F}_{q^6} \,:\, \mathrm{Ord}_{\delta_2} = (X + 1)(X^3 + 1)\}\,, \\ B &= \{\delta_1\delta_2 \,:\, \delta_1 \in A_1, \delta_2 \in A_2\}\,. \end{aligned}$$

Note that $E_{a,b} \in \mathcal{W}$ if and only if $b^{1/2} \in B$. Also, $\#A_1 = (q - 1)(q^2 - 1)$ and $\#A_2 = (q^2 - q)(q^2 - 1)$. It follows from Theorem 1(iv) with $n_1 = 3$ that $\#\mathcal{W} = 2\#B = (\#A_1)(\#A_2)/(q - 1) = 2q(q - 1)(q^2 - 1)^2$.

By Theorem 1(ii) with $n_1 = 3$, we have $\mathrm{Ord}_{\gamma_1} | X^3 + 1$ and $\mathrm{Ord}_{\gamma_2} | (X + 1)(X^3 + 1)$. Suppose first that $E \in \mathcal{W}$. Then we can write $\beta = \delta_1\delta_2$ with $\mathrm{Ord}_{\delta_1} = X^3 + 1$ and $\mathrm{Ord}_{\delta_2} = (X + 1)(X^3 + 1)$. Let $\lambda \in \mathbb{F}^*_{q^3}$ with $\delta_1 = \lambda\gamma_1$,

whence $\delta_2 = \lambda^{-1}\gamma_2$. Then

$$\begin{aligned} 0 &= \mathrm{Tr}_{K/K_1}(\gamma_2 + \gamma_2^q) \\ &= \mathrm{Tr}_{K/K_1}(\lambda\delta_2 + \lambda^q\delta_2^q) + 2\mathrm{Tr}_{K/K_1}(\lambda\delta_2^q) \\ &= \lambda\mathrm{Tr}_{K/K_1}(\delta_2 + \delta_2^q) + (\lambda + \lambda^q)\mathrm{Tr}_{K/K_1}(\delta_2^q) \\ &= (\lambda + \lambda^q)\mathrm{Tr}_{K/K_1}(\delta_2^q). \end{aligned}$$

But $\mathrm{Tr}_{K/K_1}(\delta_2) \neq 0$ since $\mathrm{Ord}_{\delta_2} \nmid (X^3+1)$. Hence $\lambda \in \mathbb{F}_q^*$. If follows that $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\delta_1} = (X^3+1)$ and $\mathrm{Ord}_{\gamma_2} = \mathrm{Ord}_{\delta_2} = (X+1)(X^3+1) \neq X^2+1$.

Suppose now that $\mathrm{Ord}_{\gamma_1} = X^3+1$ and $\mathrm{Ord}_{\gamma_2} \neq X^2+1$. Then $\mathrm{Tr}_{K/K_1}(\gamma_2) = \mathrm{Tr}_{K/K_1}(\beta/\gamma_1) = \mathrm{Tr}_{K/K_1}(\beta)/\gamma_1 = 1$. Hence $\mathrm{Ord}_{\gamma_2} \nmid (X^3+1)$. And, $(\sigma+1)(\sigma^3+1)(\gamma_2) = (\sigma+1)(\gamma_2^{q^3} + \gamma_2) = (\sigma+1)(1) = 0$. Hence $\mathrm{Ord}_{\gamma_2} | (X+1)(X^3+1)$. Since $\mathrm{Ord}_{\gamma_2} \neq X^2+1$, it follows that $\mathrm{Ord}_{\gamma_2} = (X+1)(X^3+1)$ and so $E \in \mathcal{W}$. □

Given a non-subfield curve $E \in \mathcal{E}$, Theorem 11 can be used to efficiently decide whether $E \in \mathcal{W}$ in which case the generalized GHS reduction can be applied. In the rare event that $E \notin \mathcal{W}$, proceeding just as outlined in §5.1 yields an isogenous curve $E'' \in \mathcal{W}$ in just a few random walk steps. Table 2 gives the time estimates for solving the DLP in $J_C(\mathbb{F}_{2^l})$ under Assumptions A and B, leading to our conclusion that the fields $\mathbb{F}_{2^{6l}}$ are potentially weak.

N	l	$\log_2 R_\rho$	$\log_2 R_{\mathrm{RG}}$	$\log_2 R_{\mathrm{LA}}$
162	27	84	74	56
210	35	108	82	72
300	50	153	98	102
402	67	204	115	136
498	83	252	131	168
600	100	303	149	202

TABLE 2. Time estimates for the generalized GHS attack with $n = 6$ (under Assumptions A and B). An ECDLP instance in $E_{a,b}(\mathbb{F}_{2^{6l}})$ is reduced to a DLP instance in $J_C(\mathbb{F}_{2^l})$ where C is a genus 14 curve.

Now let $\mathcal{W}$ be the set of elliptic curves $E_{a,b} \in \mathcal{E}$ for which b can be written as $b = (\gamma_1\gamma_2)^2$ with $\mathrm{Ord}_{\gamma_1} = X^2+X+1$ and $\mathrm{Ord}_{\gamma_2} = (X+1)^2(X^2+X+1)$. Then $b \notin \mathbb{F}_{q^3}$ and $\mathrm{Tr}_{K/K_1}(b) \neq 0$. Since there exist q^2-1 such values γ_1 and $(q^2-q)(q^2-1)$ such values γ_2, Theorem 1(iv) gives $\#\mathcal{W} = 2q(q^2-1)^2 \approx 2q^5$. For $E \in \mathcal{W}$, a corresponding decomposition of b can be easily obtained by putting $\beta = b^{1/2}$, $\gamma_1 = \beta^{q^3} + \beta$, and $\gamma_2 = \beta/\gamma_1$. Then, by Theorem 1(ii) with $n_1 = 3$ we have $\mathrm{Ord}_{\gamma_1} | (X^3+1)$ and $\mathrm{Ord}_{\gamma_2} | (X+1)^2(X^2+X+1)$. Since $b \notin \mathbb{F}_{q^3}$, $\mathrm{Ord}_{\gamma_2} \nmid (X^3+1)$ and thus $\mathrm{Ord}_{\gamma_2} = (X+1)^2(X^2+X+1)$. Further, it is easily verified that $\mathrm{Ord}_\beta | (X^5+X^4+X^3+X^2+X+1)$. Thus, $\mathrm{Ord}_{\gamma_1} | (X^2+X+1)$, and hence $\mathrm{Ord}_{\gamma_1} = X^2+X+1$.

On the other hand, $\mathrm{Ord}_\beta|(X^5+X^4+X^3+X^2+X+1)$ implies that $\mathrm{Tr}_{K/k}(b)=0$ and thus $\mathrm{Tr}_{K/\mathbb{F}_2}(b)=0$. By Lemma 7 of [18], this implies that $\#E(\mathbb{F}_{q^6})\equiv 0 \pmod 8$ if $\mathrm{Tr}(a)=0$. So let $\mathcal{X}$ be the set of all non-subfield elliptic curves $E\in\mathcal{E}$ over $\mathbb{F}_{q^6}$ with $\#E(\mathbb{F}_{q^6})\equiv 0$ or $2 \pmod 8$. Then $\#\mathcal{X}\approx q^6$.

Using the above decomposition, for $E\in\mathcal{W}$ we have $s_1=2$, $s_2=t=4$, so that the generalized GHS reduction with $n=6$ yields a curve C of genus 12. Combined with random walks in isogeny classes (under Assumption C, with $\#\mathcal{W}/\#\mathcal{X}\approx 2^{-(l-1)}$), we obtain that the curves in $\mathcal{X}$ are particularly (potentially) vulnerable to the generalized GHS attack, which further supports the conclusion that the fields $\mathbb{F}_{2^{6l}}$ are potentially weak (cf. Table 3).

N	l	$\log_2 R_\rho$	$\log_2 R_{\mathrm{RG}}$	$\log_2 R_{\mathrm{LA}}$	$\log_2 R_{\mathrm{W}}$
162	27	84	66	56	48
210	35	108	72	72	57
300	50	153	90	102	72
402	67	204	107	136	90
498	83	252	123	168	106
600	100	303	141	202	123

TABLE 3. Time estimates for the generalized GHS attack with $n=6$ (under Assumptions A, B and C). An ECDLP instance in $E(\mathbb{F}_{2^{6l}})$ is reduced to a DLP instance in $J_C(\mathbb{F}_{2^l})$ where C is a genus 12 curve.

7. The case $n=3$

Suppose now that $n=3$, $N=3l$, $K=\mathbb{F}_{2^{3l}}$, $q=2^l$, and $k=\mathbb{F}_q$. We show that the fields $\mathbb{F}_{2^{3l}}$ are partially weak.

We have $X^3+1=(X+1)(X^2+X+1)$. Let $\mathcal{W}$ be the set of elliptic curves $E_{a,b}\in\mathcal{E}$ over $\mathbb{F}_{2^{3l}}$ with $b=(\gamma_1\gamma_2)^2$, where $\mathrm{Ord}_{\gamma_1}=X+1$ and $\mathrm{Ord}_{\gamma_2}=X^2+X+1$. For each $E\in\mathcal{W}$ we have $s_1=1$, $s_2=2$ and $t=3$, so that the generalized GHS reduction with $n=3$ produces a curve C of genus $g=3$ over $\mathbb{F}_q$. In fact, in this case the generalized GHS reduction and the GHS reduction coincide: Among the $q-1$ representations $b=(\gamma_1\gamma_2)^2$ with $\mathrm{Ord}_{\gamma_1}=X+1$ and $\mathrm{Ord}_{\gamma_2}=X^2+X+1$, one particular choice is $\gamma_1=1$ and $\gamma_2=b^{1/2}$. Thus, $E_{a,b}\in\mathcal{W}$ if and only if $\mathrm{Ord}_b=X^2+X+1$, there are q^2-1 such $b\in\mathbb{F}_{q^3}$, and thus $\approx 2(q^2-1)$ such $E_{a,b}\in\mathcal{W}$, and the resulting curve of genus 3 over $\mathbb{F}_q$ is hyperelliptic.

However, for $E=E_{a,b}\in\mathcal{W}$ we have $\mathrm{Tr}_{K/k}(b)=0$ and thus $\mathrm{Tr}_{K/\mathbb{F}_2}(b)=0$. Hence, by Lemma 7 of [18] $\#E(\mathbb{F}_{q^3})\equiv 0 \pmod 8$ if $\mathrm{Tr}(a)=0$. Let $\mathcal{X}$ be the set of all non-subfield elliptic curves $E\in\mathcal{E}$ over $\mathbb{F}_{q^3}$ with $\#E(\mathbb{F}_{q^3})\equiv 0 \pmod 8$ or $2 \pmod 8$. Then $\#\mathcal{X}\approx q^3$.

Now, given an instance of the ECDLP on a given curve $E_{a,b} \in \mathcal{X}$, we proceed just as outlined in §5.1, where the algorithm for deciding whether an elliptic curve is in $\mathcal{W}$ is replaced by the check for $b^{q^2} + b^q + b = 0$.

Under Assumption C, for a given curve $E \in \mathcal{X} \setminus \mathcal{W}$ it takes expected $q/2$ random walk steps in the isogeny class of E to find a curve in $\mathcal{W}$.

Gaudry and Thomé's [10] double-large prime variant of the index-calculus algorithm for computing the logarithms in a genus 3 hyperelliptic curve C over $\mathbb{F}_q$ has running time $O(q^{4/3+\epsilon})$. Their experiments confirm that the algorithm is indeed faster in practice than Pollard's rho method (which has a running time of $O(q^{1.5})$) even for rather small jacobian sizes (about 2^{81}). Thus, finite fields $\mathbb{F}_{2^{3l}}$ should be considered partially weak.

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

The field $K = \mathbb{F}_{2^{210}}$ is interesting for ECC implementations because its arithmetic can be efficiently implemented by successive extensions, e.g., $\mathbb{F}_{2^2} \subseteq \mathbb{F}_{2^6} \subseteq \mathbb{F}_{2^{30}} \subseteq \mathbb{F}_{2^{210}}$. In [18], the following evidence was given for the weakness of $\mathbb{F}_{2^{210}}$ for ECC. For this field, we have $R_\rho \approx 2^{108}$.

(1) For (essentially) all elliptic curves over $\mathbb{F}_{2^{210}}$, the GHS reduction with $n = 5$ yields a hyperelliptic curve of genus 15 or 16 over $\mathbb{F}_{2^{42}}$. This gives $R_{\mathrm{RG}} \approx 2^{98}$ and $R_{\mathrm{LA}} \approx 2^{86}$.
(2) For about 2^{175} isomorphism classes of elliptic curves over $\mathbb{F}_{2^{210}}$, the GHS reduction with $n = 6$ yields a hyperelliptic curve of genus 15 or 16 over $\mathbb{F}_{2^{35}}$ for which $R_{\mathrm{RG}} \approx 2^{90}$ and $R_{\mathrm{LA}} \approx 2^{75}$. Random walks in isogeny classes [6] can then be used to solve the ECDLP in a quarter of all elliptic curves $E_{a,b}$ over $\mathbb{F}_{2^{210}}$, namely those satisfying $\mathrm{Tr}(a) = \mathrm{Tr}(b) = 0$, in the same time ($R_{\mathrm{RG}} \approx 2^{90}$, $R_{\mathrm{LA}} \approx 2^{72}$).

The results of §§5.1, 6 and 7 provide further evidence for the weakness of $\mathbb{F}_{2^{210}}$.

(3) For about 2^{149} curves in $\mathcal{E}_0$, the generalized GHS reduction with $n = 7$ gives a genus 7 (non-hyperelliptic) curve C over $\mathbb{F}_{2^{30}}$. Under Assumptions A and B, we have $R_{\mathrm{RG}} \approx 2^{53}$ and $R_{\mathrm{LA}} \approx 2^{61}$. Random walks in isogeny classes can then be used so solve the ECDLP in all non-subfield elliptic curves in $\mathcal{E}_0$ in approximately 2^{84} operations in $\mathbb{F}_{2^{210}}$.
(4) For almost all curves in $\mathcal{E}$, the generalized GHS reduction with $n = 6$ gives a genus 14 (non-hyperelliptic) curve C over $\mathbb{F}_{2^{35}}$. Under Assumptions A and B, we have $R_{\mathrm{RG}} \approx 2^{82}$ and $R_{\mathrm{LA}} \approx 2^{72}$. With a few random walk steps in the appropriate isogeny class the ECDLP in any non-subfield elliptic curve in $\mathcal{E}$ can be solved in the same time ($R_{\mathrm{RG}} \approx 2^{82}$, $R_{\mathrm{LA}} \approx 2^{72}$).
(5) For about 2^{176} curves in $\mathcal{E}$, the generalized GHS reduction with $n = 6$ gives a genus 12 (non-hyperelliptic) curve C over $\mathbb{F}_{2^{35}}$. Under Assumptions A and B, we have $R_{\mathrm{RG}} \approx 2^{72}$ and $R_{\mathrm{LA}} \approx 2^{72}$. Random walks in isogeny classes can then be used so solve the ECDLP in all

non-subfield elliptic curves in $\mathcal{E}$ with $\#E(\mathbb{F}_{2^{210}}) \equiv 0$ or $2 \pmod 8$ in the same time ($R_{\mathrm{RG}} \approx 2^{72}$, $R_{\mathrm{LA}} \approx 2^{72}$).

(6) For about 2^{140} of all curves in $\mathcal{E}$, the GHS reduction with $n = 3$ produces a genus 3 hyperelliptic curve C over $\mathbb{F}_{2^{70}}$. Random walks in isogeny classes can then be used to reduce the ECDLP in all elliptic curves $E \in \mathcal{E}$ with $\#E(\mathbb{F}_{2^{210}}) \equiv 0$ or $2 \pmod 8$ to the DLP in a genus 3 hyperelliptic curve. The Gaudry-Thomé index-calculus algorithm can solve the latter problem in time significantly less than R_ρ.

9. The case $n \neq 3, 6, 7$

In this section we examine the weakness of fields $\mathbb{F}_{q^n}$ with $n \neq 3, 6, 7$ under the generalized GHS attack.

First observe that just as with the GHS attack, for each field $\mathbb{F}_{q^n}$ the set of possible genera of the curves over $\mathbb{F}_q$ produced by the generalized GHS reduction is completely determined by the factorization of the polynomial $X^n + 1$ over $\mathbb{F}_2$. Consequently, for most fields $\mathbb{F}_{q^n}$ one would expect that the smallest (useful) genera that can be obtained by both attacks are approximately the same.

For each n, we search for a class $\mathcal{W}$ of vulnerable elliptic curves. Note $\#\mathcal{W}/\#\mathcal{E}$ cannot be negligibly small because otherwise the random walk in an isogeny class will be infeasible.

9.1. **The case N prime.** Let $N \in [160, 600]$ be prime. Then the factorization of $X^N + 1$ over $\mathbb{F}_2$ is $X^N + 1 = (X+1)f_1 f_2 \cdots f_s$ with $\deg f_i = d$, where d is the multiplicative order of 2 modulo N. For an elliptic curve $E = E_{a,b}$ over $\mathbb{F}_{2^N}$, the best possible choice for the decomposition of b is such that $\mathrm{Ord}_{\gamma_1} = f_i$ for some $1 \leq i \leq s$ and $\mathrm{Ord}_{\gamma_2} = X + 1$ (in which case $s_1 = d$, $s_2 = 1$ and $t = d + 1$), or $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = f_i$ for some $1 \leq i \leq s$ (in which case $s_1 = s_2 = t = d$ if $\mathrm{Tr}(a) = 0$). In either case, the generalized GHS reduction with $n = N$ produces a curve C over $\mathbb{F}_2$ of genus $g = 2^d - 1$. Since $d \geq 16$ for prime $N \in [160, 600]$, the DLP in $J_C(\mathbb{F}_2)$ will take longer than Pollard's rho method for $E(\mathbb{F}_{2^N})$ (even if the curve C were hyperelliptic). Thus the generalized GHS attack fails for *all* instances of the ECDLP for all elliptic curves over finite fields of prime extension degree.

9.2. **The case $n = 8$.** Now let $n = 8$, $N = 8l$, $K = \mathbb{F}_{2^{8l}}$, $K_1 = \mathbb{F}_{2^{4l}}$, $q = 2^l$, and $k = \mathbb{F}_q$. We argue that for sufficiently large N, the set $\mathcal{X}$ of all non-subfield elliptic curves E over $\mathbb{F}_{2^{8l}}$ with $\#E(\mathbb{F}_{2^{8l}}) \equiv 0 \pmod 8$ are vulnerable to the GHS attack and potentially vulnerable to the generalized GHS attack.

Over $\mathbb{F}_2$, we have $X^8 + 1 = (X + 1)^8$. Let $\mathcal{W}$ be the set of elliptic curves $E_{a,b} \in \mathcal{E}_0$ over $\mathbb{F}_{q^8}$ with $b = (\gamma_1\gamma_2)^2$, where $\mathrm{Ord}_{\gamma_1} = X^2 + 1$ and $\mathrm{Ord}_{\gamma_2} = (X+1)^5 = X^5 + X^4 + X + 1$. For each $E \in \mathcal{W}$ we have $s_1 = 2$ and

$s_2 = t = 5$, and the generalized GHS reduction with $n = 8$ yields a curve C of genus 24 over $\mathbb{F}_q$.

Theorem 12. *Let $E = E_{a,b} \in \mathcal{E}_0$. We have $E \in \mathcal{W}$ if and only if* $\mathrm{Ord}_b = (X+1)^6 = X^6 + X^4 + X^2 + 1$.

Proof. Let

$$\begin{aligned} A_1 &= \{\gamma_1 \in \mathbb{F}_{q^8} \,:\, \mathrm{Ord}_{\gamma_1} = X^2 + 1\} = \mathbb{F}_{q^2} \setminus \mathbb{F}_q \,, \\ A_2 &= \{\gamma_2 \in \mathbb{F}_{q^8} \,:\, \mathrm{Ord}_{\gamma_2} = (X+1)^5\} \,, \\ B &= \{\gamma_1\gamma_2 \,:\, \gamma_1 \in A_1, \gamma_2 \in A_2\} \,. \end{aligned}$$

Note that $E_{a,b} \in \mathcal{W}$ if and only if $b^{1/2} \in B$. Also, $\#A_1 = q^2 - q$ and $\#A_2 = q^5 - q^4$. By Theorem 1(iv) with $n_1 = 4$, we have $\#B = q^6 - q^5$.

Now assume that $\beta = b^{1/2} \in B$. Let $\gamma_1 \in A_1$ and $\gamma_2 \in A_2$ such that $\beta = \gamma_1\gamma_2$. An easy calculation shows that $(\gamma_1\gamma_2)^{q^6} + (\gamma_1\gamma_2)^{q^4} + (\gamma_1\gamma_2)^{q^2} + \gamma_1\gamma_2 = 0$. Thus $\mathrm{Ord}_b | (X+1)^6$. Now, if Ord_b divided $(X+1)^5$, then

$$\begin{aligned} 0 &= (\gamma_1\gamma_2)^{q^5} + (\gamma_1\gamma_2)^{q^4} + (\gamma_1\gamma_2)^q + \gamma_1\gamma_2 \\ &= \gamma_1^q(\gamma_2^{q^4} + \gamma_2^q + \gamma_2) + \gamma_1\gamma_2^{q^4} + \gamma_1^q\gamma_2^q + \gamma_1\gamma_2 \\ &= (\gamma_1^q + \gamma_1)(\gamma_2^{q^4} + \gamma_2). \end{aligned}$$

Since $\gamma_1 \notin \mathbb{F}_q$, we have $\gamma_2^{q^4} + \gamma_2 = 0$, so $\mathrm{Ord}_{\gamma_2} | (X+1)^4$ which is a contradiction. Therefore, $\mathrm{Ord}_b = (X+1)^6$.

To show the converse, simply observe that there are $q^6 - q^5$ elements $b \in \mathbb{F}_{q^8}$ with $\mathrm{Ord}_b = (X+1)^6$. Thus, any such b must be in B. □

For $E_{a,b} \in \mathcal{W}$ we thus have $\mathrm{Tr}_{K/k}(b) = 0$ and hence $\mathrm{Tr}(b) = 0$. By Lemma 7 of [18], this implies that $\#E(\mathbb{F}_{2^{8l}}) \equiv 0 \pmod 8$.

If $b \in \mathbb{F}_{q^8}^*$ with $\mathrm{Ord}_b = (X+1)^6$, a decomposition $b = (\gamma_1\gamma_2)^2$ with $\mathrm{Ord}_{\gamma_1} = X^2 + 1$ and $\mathrm{Ord}_{\gamma_2} = (X+1)^5$ can be obtained as follows. Let $\beta = b^{1/2}$, $\gamma_1 = \beta^{q^4} + \beta$, and $\gamma_2 = \beta/\gamma_1$. Then, by Theorem 1(ii) with $n_1 = 4$, we have $\mathrm{Ord}_{\gamma_1} | (X+1)^4$ and $\mathrm{Ord}_{\gamma_2} | (X+1)^5$. Since $\mathrm{Ord}_b = (X+1)^6$, we have that $\mathrm{Ord}_{\gamma_1} | (X^2+1)$ and $\mathrm{Ord}_{\gamma_1} \neq X+1$, and thus $\mathrm{Ord}_{\gamma_1} = X^2 + 1$. Further, $\gamma_2 \notin \mathbb{F}_{q^4}$ (since $b \notin \mathbb{F}_{q^4}$) and thus $\mathrm{Ord}_{\gamma_2} = (X+1)^5$.

Observe that for each curve in $\mathcal{W}$, the GHS reduction yields a hyperelliptic curve over $\mathbb{F}_q$ of genus 32.

Using random walks in isogeny classes, both the generalized GHS attack and the GHS attack can be extended from $\mathcal{W}$ to all elliptic curves $E_{a,b} \in \mathcal{X}$. For selected values of N, Table 4 compares the time estimates for R_ρ with the estimates for R_{RG}, R_{LA}, R_{W} for both cases[3]. For the genus 24 case, Assumptions A and B are under effect. In either case, the estimate for R_{W} relies on Assumption C (with $\#\mathcal{W}/\#\mathcal{X} \approx 2^{-(2l-1)}$).

[3]If $g = 24$ and $N \in \{160, 208\}$, and if $g = 32$ and $N \in \{160, 208, 304\}$, the running times R_{RG} and R_{LA} take into account that the Enge-Gaudry index calculus algorithm performs best if the factor base contains both degree one and degree two divisors.

N	l	$\log_2 R_\rho$	$\log_2 R_{\mathrm{RG}}$ ($g=24$)	$\log_2 R_{\mathrm{LA}}$ ($g=24$)	$\log_2 R_{\mathrm{RG}}$ ($g=32$)	$\log_2 R_{\mathrm{LA}}$ ($g=32$)	$\log_2 R_{\mathrm{W}}$
160	20	83	86	81	104	81	61
200	25	103	96	101	114	101	72
304	38	155	129	79	140	153	98
400	50	203	142	103	181	103	123
504	63	255	155	129	195	129	149
600	75	303	167	153	207	153	173

TABLE 4. Time estimates for the generalized GHS attack with $n = 8$ (under Assumptions A, B and C for $g = 24$, and under Assumption C for $g = 32$). An ECDLP instance in $E(\mathbb{F}_{2^{8l}})$ is reduced to a DLP instance in $J_C(\mathbb{F}_{2^l})$ where C is a genus 24 curve, or a genus 32 hyperelliptic curve.

9.3. **Other small n.**

9.3.1. $n = 2$. For non-subfield curves $E_{a,b}$ defined over $\mathbb{F}_{2^{2l}}$, the only possibility for applying the generalized GHS attack with $n = 2$ has $\mathrm{Ord}_{\gamma_1} = (X + 1)$ and $\mathrm{Ord}_{\gamma_2} = (X + 1)^2$. This yields a genus 2 curve over $\mathbb{F}_{2^l}$. Since no DLP solvers for the DLP in genus 2 curves are known that are faster than Pollard's rho method, the generalized GHS attack fails.

9.3.2. $n = 4$. In [18] it was shown that for a majority of elliptic curves over $\mathbb{F}_{2^{4l}}$, the GHS reduction yields a genus 8 hyperelliptic curve over $\mathbb{F}_{2^l}$. The DLP in the latter is slightly easier to solve than the original ECDLP, which led to the conclusion that fields $\mathbb{F}_{2^{4l}}$ are only slightly weak.

Let $b \in \mathbb{F}_{2^{4l}}$ with $\mathrm{Tr}_{\mathbb{F}_{2^{4l}}/\mathbb{F}_{2^l}}(b) \neq 0$, and let $\beta = b^{1/2}$. Let $\gamma_1 = \beta^{q^2} + \beta$ and $\gamma_2 = \beta/\gamma_1$. Then $b = (\gamma_1\gamma_2)^2$, $\mathrm{Ord}_{\gamma_1} = X^2 + 1$, $\mathrm{Ord}_{\gamma_2} = (X + 1)^3$, and the generalized GHS yields a curve C of genus 6 over $\mathbb{F}_{2^l}$. If C were hyperelliptic, then the Enge-Gaudry algorithm for solving the DLP in $J_C(\mathbb{F}_{2^l})$ would still only be slightly faster than Pollard's rho method for $E(\mathbb{F}_{2^{4l}})$. Since in fact C is not hyperelliptic, we conclude that fields $\mathbb{F}_{2^{4l}}$ are not further weakened by the generalized GHS attack with $n = 4$.

9.3.3. $n = 5$. We have $X^5 + 1 = (X + 1)(X^4 + X^3 + X^2 + X + 1)$. The best possible choice for the decomposition of b is such that $\mathrm{Ord}_{\gamma_1} = X^4 + X^3 + X^2 + X + 1$ and $\mathrm{Ord}_{\gamma_2} = X + 1$ (in which case $s_1 = 4$, $s_2 = 1$, $t = 5$), or $\mathrm{Ord}_{\gamma_1} = \mathrm{Ord}_{\gamma_2} = X^4 + X^3 + X^2 + X + 1$ (in which case $s_1 = s_2 = t = 4$ if $\mathrm{Tr}(a) = 0$). In either case, the generalized GHS reduction with $n = 5$ produces curves of genus $g = 15$. Thus the generalized GHS attack does not further weaken the fields $\mathbb{F}_{2^{5l}}$ over the GHS attack for which any non-subfield elliptic curve over $\mathbb{F}_{2^{5l}}$ can be reduced to a genus 15 or 16 hyperelliptic curve over $\mathbb{F}_{2^l}$ [18].

9.3.4. $n = 9$. For any non-subfield elliptic curve defined over $\mathbb{F}_{2^{9l}}$, the smallest possible genus obtained by the generalized GHS reduction with $n = 9$ is $g = 63$; this can be achieved by taking $\mathrm{Ord}_{\gamma_1} = X^6 + X^3 + 1$ and $\mathrm{Ord}_{\gamma_2} = X + 1$. The smallest genus obtained by the GHS reduction with $n = 9$ is also $g = 63$. In either case, this does not yield an ECDLP solver that is faster than Pollard's rho method.

9.3.5. $n = 10$. For any non-subfield elliptic curve defined over $\mathbb{F}_{2^{10l}}$, the smallest achievable genus for the generalized GHS reduction with $n = 10$ is $g = 32$ (by taking $\mathrm{Ord}_{\gamma_1} = (X^5 + 1)(X + 1)$ and $\mathrm{Ord}_{\gamma_2} = X + 1$). This is no improvement over the GHS reduction with $n = 10$.

9.3.6. $11 \leq n \leq 300$. Continuing in this way, we checked all remaining values upto $n = 300$. We found that for all fields $\mathbb{F}_{q^n}$ with $9 \leq n \leq 300$ only at most a small proportion of elliptic curves over $\mathbb{F}_{2^{nl}}$ succumb to the generalized GHS attack with descent degree n. For some n, these proportions are slightly larger than for the GHS attack, but they are still negligibly small (and also the curves are not hyperelliptic).

10. Conclusions

We examined the weakness of characteristic two finite fields under Hess' generalized GHS attack. The only new fields found to exhibit any weaknesses are the fields $\mathbb{F}_{2^{3l}}$ which are partially weak, the fields $\mathbb{F}_{2^{6l}}$ which are potentially weak, and the fields $\mathbb{F}_{2^{7l}}$ and $\mathbb{F}_{2^{8l}}$ which are potentially partially weak. These results strongly suggest that finite fields $\mathbb{F}_{2^N}$ where N is divisible by 3, 5, 6, 7 or 8, should not be used to implement elliptic curve cryptographic protocols.

An outstanding task is to characterize the curves produced by the generalized GHS reduction, and to exactly analyze their best DLP solvers. Another open problem is to determine whether the elliptic curves $E_{a,b}$ over $\mathbb{F}_{2^{7l}}$ with $\mathrm{Tr}(a) = 1$ are (potentially) weak.

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*, Lecture Notes in Computer Science, 877 (1994), 28-40.

[2] A. Enge and P. Gaudry, "A general framework for subexponential discrete logarithm algorithms", *Acta Arithmetica*, 102 (2002), 83-103.

[3] 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.

[4] 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.

[5] S. Galbraith, "Constructing isogenies between elliptic curves over finite fields", *LMS Journal of Computation and Mathematics*, 2 (1999), 118-138.

[6] 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.

[7] 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.

[8] P. Gaudry, "Index calculus for abelian varieties and the elliptic curve discrete logarithm problem", *Cryptology ePrint Archive: Report 2004/073*, 2004. Available from http://eprint.iacr.org/2004/073/

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

[10] P. Gaudry and E. Thomé, "A double large prime variation for small genus hyperelliptic index calculus", *Cryptology ePrint Archive: Report 2004/153*, 2004. Available from http://eprint.iacr.org/2004/153/

[11] F. Hess, "Computing Riemann-Roch spaces in algebraic function fields and related topics", *Journal of Symbolic Computation*, 33 (2002), 425-445.

[12] F. Hess, "Computing relations in divisor class groups of algebraic curves over finite fields", preprint, 2003.

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

[14] D. Kohel, *Endomorphism rings of elliptic curves over finite fields*, PhD thesis, University of California, Berkeley, 1996.

[15] 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.

[16] 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.

[17] A. Menezes and M. Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart", *Topics in Cryptology—CT-RSA 2001*, Lecture Notes in Computer Science, 2020 (2001), 308-318.

[18] 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.

[19] P. van Oorschot and M. Wiener, "Parallel collision search with cryptanalytic applications", *Journal of Cryptology*, 12 (1999), 1-28.

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

[21] 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.

[22] 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.

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

[24] E. Teske. "On random walks for Pollard's rho method", *Mathematics of Computation*, 70 (2001), 809-825.

Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: ajmeneze@uwaterloo.ca, eteske@uwaterloo.ca