WEIL DESCENT ATTACKS

F. HESS

ABSTRACT. This article is to appear as a chapter in *Advances in Elliptic Curve Cryptography*, edited by I. Blake, G. Seroussi and N. Smart, Cambridge University Press, 2004. It summarises the main aspects of the existing literature on Weil descent attacks and contains some new material on the GHS attack in even characteristic.

CONTENTS

Date: 2. April 2004. Updates: 14. November 2005.

1. Introduction — the Weil Descent Methodology

Weil descent attacks provide means of attacking the DLP for elliptic curves or for more general algebraic curves such as hyperelliptic curves, when they are used over finite extension fields, i.e. non-prime fields.

The application of the original basic idea, the Weil restriction of scalars for elliptic curves, to cryptography and the ECDLP was first suggested in [13]. An important step forward was made in [20] using explicit covering techniques, relating the ECDLP to a potentially easier HCDLP. Since then, variations, generalisations and ramifications of the employed methodology have been investigated in some detail.

The aim of this chapter is to explain the basic ideas, to summarise the main results about Weil descent attacks for elliptic curves and to discuss the relevance to ECC. Throughout this exposition we let K/k denote an extension of finite fields of degree n. The characteristic and cardinality of k are p and $q = p^r$ respectively.

1.1. **Curves in the Weil Restriction.**

Let $\mathcal{E}$ be an elliptic curve over K. The initial motivation for the Weil descent attacks came from the consideration of the Weil restriction $\mathrm{Res}_{K/k}(\mathcal{E})$ of $\mathcal{E}$ with respect to K/k, suggested by Frey [13].

The Weil restriction $\mathrm{Res}_{K/k}(\mathcal{E})$ is an abelian variety of dimension n defined over k, as opposed to $\mathcal{E}$ which is an abelian variety of dimension one over K. The group $\mathrm{Res}_{K/k}(\mathcal{E})(k)$ of k-rational points of $\mathrm{Res}_{K/k}(\mathcal{E})$ is isomorphic to the group $\mathcal{E}(K)$ of K-rational points of $\mathcal{E}$ and thus contains an equivalent version of any DLP in $\mathcal{E}(K)$. Given $\mathcal{E}$ and K/k and the defining equations, the group law of $\mathrm{Res}_{K/k}(\mathcal{E})$ and the isomorphism of the point groups can be computed without much difficulty. We do not need the details here and refer to [13], [19], [20] instead.

The main idea now is the following. An algebraic curve $\mathcal{C}^0$ and a map $\mathcal{C}^0 \to \mathrm{Res}_{K/k}(\mathcal{E})$ defined over k lead to a map $\phi : \mathrm{Jac}(\mathcal{C}^0) \to \mathrm{Res}_{K/k}(\mathcal{E})$, due to the functorial property of $\mathrm{Jac}(\mathcal{C}^0)$. If we take such a curve $\mathcal{C}^0$ we may be able to lift a given DLP from $\mathrm{Res}_{K/k}(\mathcal{E})(k)$ to $\mathrm{Jac}(\mathcal{C}^0)(k)$. The DLP in $\mathrm{Jac}(\mathcal{C}^0)(k)$ can then be attacked, possibly more efficiently by index calculus methods on $\mathcal{C}^0(k)$ than by the Pollard methods on $\mathcal{E}(K)$, the main point being that $\mathcal{C}^0$ is defined over the small field k.

In order to find $\mathcal{C}^0$ one can intersect $\mathrm{Res}_{K/k}(\mathcal{E})$ with suitable hyperplanes, and we remark that there is a fairly natural choice of such a hyperplane. It is then a priori not clear whether the DLP can be lifted to $\mathrm{Jac}(\mathcal{C}^0)(k)$, however some evidence is given by the fact that $\mathrm{Res}_{K/k}(\mathcal{E})$ is simple in many interesting cases [10]. Another quite difficult problem is how to actually lift the DLP to $\mathrm{Jac}(\mathcal{C}^0)(k)$, using explicit equations. We refer to [19] for a more detailed discussion.

1.2. **Covering Techniques.**

Covering techniques boil down to a reformulation of the method of the previous section at the level of curves, their function fields and Galois theory. Curves are basically one-dimensional objects as opposed to the above Weil restriction and Jacobians, and their function fields can furthermore be viewed as "equationless" substitutes. This leads to a much easier and algorithmically accessible treatment of the previous section, and was first applied by Gaudry, Hess and Smart in [20], an approach which is now referred to as the GHS attack.

We consider the following general situation. Let now E denote an elliptic function field over K and C a finite extension field of E such that there is a field automorphism σ which extends the Frobenius automorphism of K/k and has order n on C. We say that σ is a Frobenius automorphism of C with respect to K/k and denote the fixed field of σ by C^0. The extension C/C^0 has degree n and the exact constant field of C^0 is k. Choosing suitable defining equations we can regard E, C and C^0 as the function fields of curves $\mathcal{E}$, $\mathcal{C}$ and $\mathcal{C}^0$ respectively, where $\mathcal{E}$ is an elliptic curve, $\mathcal{E}$ and $\mathcal{C}$ are defined over K and $\mathcal{C}^0$ is defined over k. We denote the divisor class groups of E, C and C^0 by $\mathrm{Pic}^0_K(E)$, $\mathrm{Pic}^0_K(C)$ and $\mathrm{Pic}^0_k(C^0)$ so that $\mathcal{E}(K) \cong \mathrm{Pic}^0_K(E)$ and $\mathrm{Jac}(\mathcal{C}^0)(k) \cong \mathrm{Pic}^0_k(C^0)$. The conorm and norm maps of function field extensions yield homomorphisms $\mathrm{Con}_{C/E} : \mathrm{Pic}^0_K(E) \to \mathrm{Pic}^0_K(C)$ and $\mathrm{N}_{C/C^0} : \mathrm{Pic}^0_K(C) \to \mathrm{Pic}^0_k(C^0)$. Figure 1 contains a graphical presentation of the situation.

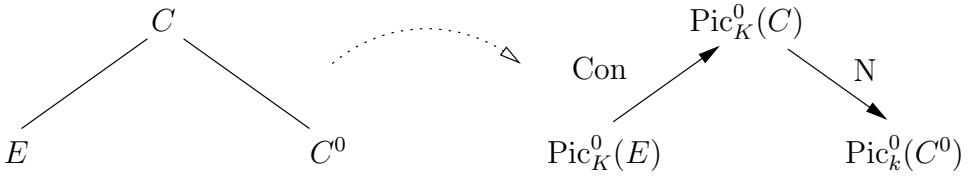

FIGURE 1. Diagram of function fields and divisor class groups

The composition of N_{C/C^0}, $\mathrm{Con}_{C/E}$ and the isomorphism between $\mathrm{Pic}^0_k(E)$ and $\mathcal{E}(K)$ is a homomorphism from $\mathcal{E}(K)$ to $\mathrm{Pic}^0_k(C^0)$ which we denote by ϕ. Using ϕ a discrete logarithm problem $Q = \lambda P$ in $\mathcal{E}(K)$ is mapped to the discrete logarithm problem $\phi(Q) = \lambda\phi(P)$ in $\mathrm{Pic}^0_k(C^0)$, where it can be attacked possibly more efficiently than in $\mathcal{E}(K)$, since it is defined over the small field k and index calculus methods can be applied. Of course, P and Q should not be in the kernel of ϕ. The index calculus methods depend exponentially or subexponentially on the genus g of C^0, see [2, chapter by P. Gaudry], [6], [12] and [21]. There are thus three main questions.

(1) How can such C and σ be constructed?
(2) Does ϕ preserve the DLP?
(3) Is the genus of C^0 small enough?

The construction of such a C and σ can be achieved quite generally using techniques from Galois theory. For example, one determines a suitable rational subfield $K(x)$ of E and defines C to be the splitting field of E over $k(x)$. A sufficient condition for the existence of a suitable σ is then that n is coprime to the index $[C : K(x)]$. For the sake of efficiency and explicitness Artin-Schreier and Kummer extensions are the most prominent constructions used.

The question whether ϕ preserves the DLP can be answered affirmatively in most cases of interest [8], [23].

Finally the genus can be explicitly determined or estimated for the employed Artin-Schreier and Kummer extensions, given E and n. As it turns out, the genus is in general exponential in n and it is smaller only in exceptional cases. This is the reason why the Weil descent methodology does not apply to general or randomly chosen elliptic curves when n is large.

These issues are discussed in detail in the following sections.

1.3. **Remarks.** The approaches of Subsection 1.1 and 1.2 are jointly carried out in [20]. For a further discussion of the equivalence of these two approaches see [7, Chapter 3] and the appendix of [8].

According to [9] the term "Weil descent" is actually used with a different meaning in mathematics than we do here and in cryptography. There a "Weil descent argument" refers to a special proof technique about the field of definition of a variety, introduced by A. Weil in [46], while here we loosely mean the transition of an elliptic curve to its Weil restriction and further considerations by which we hope to solve a DLP more quickly.

2. The GHS Attack

2.1. **The Reduction.** The most important case for practical applications are elliptic curves in characteristic two. In this section we describe the reduction of a DLP on such an elliptic curve over K to the divisor class group of a curve defined over k.

We start with an ordinary elliptic curve

$$\mathcal{E}_{a,b} : Y^2 + XY = X^3 + aX^2 + b \tag{1}$$

with $a, b \in K$, $b \neq 0$. Every isomorphism class of ordinary elliptic curves over K has a unique representative of the form (1) under the requirement that $a \in \{0, \omega\}$ where $\omega \in \mathbb{F}_{2^u}$ with $u = 2^{v_2(nr)}$ is a fixed element such that $\mathrm{Tr}_{\mathbb{F}_{2^u}/\mathbb{F}_2}(\omega) = 1$. In the following we only consider these unique elliptic curves with $a \in \{0, \omega\}$.

Applying the transformations $Y = y/\tilde{x} + b^{1/2}$, $X = 1/\tilde{x}$, multiplying by $\tilde{x}^2$, substituting $\tilde{x} = x/\gamma$ for some $\gamma \in K^\times$ and writing $\alpha = a$, $\beta = b^{1/2}/\gamma$ we obtain the Artin-Schreier equation

$$y^2 + y = \gamma/x + \alpha + \beta x. \tag{2}$$

On the other hand, reversing the transformations, we can return to equation (1) from equation (2) for any $\gamma, \beta \in K^\times$. This shows that the function field $E = K(\mathcal{E}_{a,b})$ of $\mathcal{E}_{a,b}$ contains and is in fact generated by two functions x, y satisfying the relation (2), that is $E = K(x, y)$. Note that the transformation backwards is described by the map $(\gamma, \beta) \mapsto b = (\gamma\beta)^2$ and $a = \alpha$.

The function field $E = K(x, y)$ is a Galois extension of the rational function field $K(x)$ of degree two. Furthermore, $K(x)$ is a Galois extension of $k(x)$ of degree n and the Galois group is generated by the Frobenius automorphism σ of $K(x)$ with respect to K/k satisfying $\sigma(x) = x$. We define the function field $C = C_{\gamma,\alpha,\beta}$ to be the splitting field of the extension $E/k(x)$.

Before we state the main theorem about $C_{\gamma,\alpha,\beta}$ we need some further notation. For $z \in K$ let $m_z(t) = \sum_{i=0}^{m} \lambda_i t^i \in \mathbb{F}_2[t]$ with $\lambda_m = 1$ be the unique polynomial of minimal degree such that $\sum_{i=0}^{m} \lambda_i \sigma^i(z) = 0$. We define $m_{\gamma,\beta} = \mathrm{lcm}\{m_\gamma, m_\beta\}$.

Recall that if we have a Frobenius automorphism on $C_{\gamma,\alpha,\beta}$ with respect to K/k we take $C^0 = C^0_{\gamma,\alpha,\beta}$ to be its fixed field.

Theorem 3. *The Frobenius automorphism σ of $K(x)$ with respect to K/k satisfying $\sigma(x) = x$ extends to a Frobenius automorphism of C with respect to K/k if and only if at least one of the conditions*

$$\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0,\ \mathrm{Tr}_{K/k}(\gamma) \neq 0 \text{ or } \mathrm{Tr}_{K/k}(\beta) \neq 0$$

holds. In this case, we have

(*i*) *If* $k(\gamma,\beta)=K$ *then*

$$\ker(\phi)\subseteq\mathcal{E}(K)[2^{\deg(m_{\gamma,\beta})-1}].$$

(*ii*) *The genus of* C^0 *satisfies*

$$g_{C^0}=2^{\deg(m_{\gamma,\beta})}-2^{\deg(m_{\gamma,\beta})-\deg(m_\gamma)}-2^{\deg(m_{\gamma,\beta})-\deg(m_\beta)}+1.$$

(*iii*) *There is a rational subfield of* C^0 *of index* $\min\{2^{\deg(m_\gamma)},2^{\deg(m_\beta)}\}$.

(*iv*) *If* $\gamma\in k$ *or* $\beta\in k$ *then* C^0 *is hyperelliptic.*

For the proof of Theorem 3 see [20], [23] and Section 2.6. The following corollary is an immediate consequence of Theorem 3 and the fact that m_β is not divisible by $t-1$ if and only if the given trace condition holds. A proof is given in [23].

Corollary 4. *If* $\gamma\in k$ *then*

$$g_{C^0}=\begin{cases}2^{\deg(m_{\gamma,\beta})-1}-1 & \text{if } \mathrm{Tr}_{K/\mathbb{F}_{q^u}}(\beta)=0 \text{ where } u=2^{v_2(n)},\\ 2^{\deg(m_{\gamma,\beta})-1} & \text{otherwise.}\end{cases}$$

Similarly with γ *and* β *exchanged.*

The construction of C^0 and the computation of images under ϕ can be made explicit using Artin-Schreier extensions and the operation of σ on C, see [20], [23] and [22]. This leads to algorithms which are at most polynomial in g_{C^0}. Various implementations of this construction are available in the computer algebra systems Kash and Magma [3], [27], [30].

If the condition of Theorem 3, (*i*) is satisfied we see that any large prime factor of $\mathcal{E}(K)$ and hence the DLP in $\mathcal{E}(K)$ is preserved under ϕ. Since there is some freedom in choosing γ and β this can also be achieved if $\mathcal{E}$ is actually defined over a subfield of K. We also remark that there is an explicit formula for the L-polynomial (or Zeta function) of C^0 in terms of the L-polynomials (or Zeta functions) of $\mathcal{E}$ and further related elliptic curves, see [22], [23] and Section 5.3.

The main points of interest are the possible degrees $m=\deg(m_{\gamma,\beta})$ and the relationship to γ and β. The efficiency or feasibility of the attack crucially depends on this m and it is therefore sometimes referred to as the "magic" number m. Its properties are discussed in Section 2.4.

We conclude this section with some examples.

Example 5. Let $k=\mathbb{F}_2$ and $K=\mathbb{F}_{2^{127}}=k[w]$ with $w^{127}+w+1=0$. Consider the elliptic curve

$$\mathcal{E}: Y^2+XY=X^3+w^2.$$

We can choose $\gamma=1$, $\alpha=0$ and $\beta=w$. Then $m_\gamma(t)=t+1$ and $m_\beta(t)=t^7+t+1$ since $\beta^{128}+\beta^2+\beta=0$. It follows that $m_{\gamma,\beta}(t)=t^8+t^7+t^2+1$. All conditions of Theorem 3 are fulfilled. We conclude that C^0 is a hyperelliptic function field over k of genus 127. Using the programs mentioned above we compute a representing curve

$$\mathcal{C}^0: y^2+(x^{127}+x^{64}+1)y=x^{255}+x^{192}+x^{128}.$$

A different model is given by $\mathcal{C}^0: y^2+(x^{128}+x^{64}+x)y=(x^{128}+x^{64}+x)$.

Example 6. Let $k = \mathbb{F}_{2^5} = \mathbb{F}_2[u]$ and $K = \mathbb{F}_{2^{155}} = \mathbb{F}_2[w]$ with $u^5 + u^2 + 1 = 0$ and $w^{155} + w^{62} + 1 = 0$. Consider the elliptic curve

$$\mathcal{E} : Y^2 + XY = X^3 + \delta$$

with

$$\delta = \begin{array}{l} w^{140} + w^{134} + w^{133} + w^{132} + w^{130} + w^{129} + w^{128} + w^{127} + w^{117} + \\ w^{113} + w^{111} + w^{110} + w^{102} + w^{97} + w^{96} + w^{78} + w^{74} + w^{72} + \\ w^{70} + w^{63} + w^{49} + w^{48} + w^{47} + w^{41} + w^{39} + w^{36} + w^{35} + w^{34} + \\ w^{32} + w^{24} + w^{17} + w^{10} + w^9 + w^8 + w^5 \end{array}.$$

Similarly to the previous example we can choose $\gamma = 1$, $\alpha = 0$ and $\beta = \delta^{1/2}$. Then $m_\gamma(t) = t + 1$ and $m_\beta(t) = t^{15} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^5 + t^3 + t^2 + t + 1$. It follows that $m_{\gamma,\beta}(t) = m_\gamma(t)m_\beta(t)$. All conditions of Theorem 3 are fulfilled and we conclude that C^0 is a hyperelliptic function field over k of genus 32767.

Example 7. In Example 6 we can also choose

$$\gamma = \begin{array}{l} w^{140} + w^{132} + w^{128} + w^{125} + w^{101} + w^{94} + \\ w^{78} + w^{70} + w^{64} + w^{63} + w^{47} + w^{39} + w^{35}, \end{array}$$

$\alpha = 0$ and $\beta = \delta^{1/2}/\gamma$. Then $m_{\gamma,\beta}(t) = m_\gamma(t) = m_\beta(t) = t^5 + t^2 + 1$. All conditions of Theorem 3 are fulfilled and we conclude that C^0 is a function field over k of genus 31. Using the programs mentioned above we compute a representing curve

$$\mathcal{C}^0 : \begin{array}{l} y^{32} + u^{22}y^{16} + u^3y^8 + u^9y^4 + u^{13}y^2 + u^{24}y + (u^{24}x^{24} + u^9x^{16} \\ +u^{25}x^{12} + u^{30}x^{10} + u^3x^9 + u^{26}x^7 + u^{23}x^6 + u^{15}x^4 + u^{30})/x^8 \end{array} = 0.$$

The last two examples show that the choice of γ and β can make a very significant difference for the size of the resulting genus.

2.2. **The Asymptotic Attack.** Let us assume that $\gamma \in k$. According to Theorem 3, (iv) and Corollary 4 the resulting function field C^0 is hyperelliptic and has genus bounded by $2^{n-1}-1$ or 2^{n-1} since $m_{\gamma,\beta}(t)$ divides t^n-1, and this holds independently of q. Combining this with the theorem of Gaudry, see [2, chapter by P. Gaudry], and the improvements of Harley for very small genera we obtain the following, slightly improved main result of [20].

Theorem 8. *Let $\mathcal{E} : Y^2+XY = X^3+\alpha X^2+\beta$ denote an elliptic curve over $K = \mathbb{F}_{q^n}$ such that*

$$n \text{ is odd or } \mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0 \text{ or } \mathrm{Tr}_{K/k}(\beta) \neq 0.$$

Let $\#\mathcal{E}(K) = \ell h$, where ℓ is a large prime. One can solve the discrete logarithm problem in the ℓ-cyclic subgroup of $\mathcal{E}(K)$ in time $O(q^2)$ where the complexity estimate holds for a fixed value of $n \geq 4$ as q tends to infinity.

The complexity estimate is in fact always slightly better than $O(q^2)$. This time has to be compared with the running time of the Pollard methods on $\mathcal{E}(K)$ which are $O(q^{n/2})$. It follows that the DLP can be solved (much) faster using the GHS attack when $n \geq 4$ is fixed and q tends to infinity. By the recent results of Thériault [44] improving index calculus for hyperelliptic curves further we find that the DLP on C^0 can be solved in time $O(q^{10/7})$ and $O(q^{14/9})$ if the genus is 3 or 4 respectively. Since

$10/7 < 3/2 < 14/9$ this means that the DLP on $\mathcal{E}$ can also be solved asymptotically faster using the GHS attack when $n = 3$ and $\mathrm{Tr}_{K/k}(\beta) = 0$, using Corollary 4.

It is now a natural question to ask at what sizes of q the cross over point lies. A computer experiment comparing the Pollard times against index calculus times for $n = 4$ has been carried out in [20]. The index calculus method proves to be faster by a factor of about 0.7 for an 84-bit elliptic curve. Since the cross over point is already reached for such small field sizes it can be concluded that for $n = 4$ the DLP is solved faster using the GHS attack also in practical instances and not only asymptotically. The cross over point for larger values of n however will be much higher (see for example [40]).

2.3. **Special Attacks.** The previous section applies uniformly to all elliptic curves when n is small and q large enough, so that g_{C^0} is relatively small. But it could also apply for cases where n is large and $\deg(m_{\gamma,\beta})$ happens to be sufficiently small. More generally, we could allow arbitrary $\gamma \in K$, resulting in non-hyperelliptic curves C^0, and consider only those cases where g_{C^0} is sufficiently small. Moreover, the running time of the algorithm behind Theorem 8 depends exponentially on g_{C^0}, since low genus index calculus methods are used. But there are also high genus index calculus methods available, [6], [12], [21], whose asymptotic running time depends subexponentially on g_{C^0} and is roughly of the form $q^{{g_{C^0}}^{1/2+o(1)}}$. In Example 5 we have $g_{C^0} = n$, and for such cases with large n the high genus index calculus attack would be much more efficient than the Pollard methods on the original elliptic curve.

In the following sections we investigate for which special values of n and which special families of elliptic curves an index calculus attack can be mounted which is (possibly) faster than the Pollard methods. A summary of the results of practical interest using also the methods of Section 3 is given in Section 4.

2.4. **Analysis of Possible Genera and Number of Curves.** Possible genera of C^0 and the number of corresponding elliptic curves have been investigated in detail in [31], [33] for the case $\gamma \in k$. We give here a more general and simplified discussion allowing for arbitrary $\gamma \in K$.

We first analyse the various possibilities for $m_\beta(t)$ and β in more detail. It is helpful to introduce the following standard technique from linear algebra (see also [17] and [33]). We define a multiplication of polynomials $h(t) = \sum_{i=0}^{d} \lambda_i t^i \in k[t]$ and finite field elements $z \in K$ by $h(t)z = \sum_{i=0}^{d} \lambda_i \sigma^i(z)$. This makes the additive group of K into a so-called $k[t]$-module. The polynomials $m_\beta(t)$ are then by definition polynomials in $\mathbb{F}_2[t]$ of smallest degree such that $m_\beta(t)\beta = 0$.

Let $w \in K$ be a normal basis element for K/k. The theorem of the normal basis is equivalent to the statement that K is a cyclic (or "one-dimensional") $k[t]$-module with annihilator $t^n - 1$, that is $K = \{h(t)w : h(t) \in k[t] \text{ and } \deg(h(t)) < n\} \cong k[t]/(t^n - 1)$ is generated by one element. We define $B_{m(t)} = \{\gamma \in K : m_\gamma(t) = m(t)\}$ for $m(t) \in k[t]$ and let $\Phi(m(t))$ be the number of polynomials of degree less than n in $k[t]$ coprime to $m(t)$. These observations and definitions give the following theorem.

Theorem 9. *For every $\beta \in K$ it holds that $m_\beta(t)$ is a divisor of $t^n - 1$ in $\mathbb{F}_2[t]$. Conversely, let $m(t)$ be a divisor of $t^n - 1$ in $\mathbb{F}_2[t]$. Then*

$$B_{m(t)} = \{h(t)\gamma_0 : h \in k[t], \deg(h) < \deg(m) \text{ and } \gcd\{h, m\} = 1\}$$

with $\gamma_0 = ((t^n - 1)/m(t))w$ and

$$\#B_{m(t)} = \Phi(m(t)) = \prod_{i=0}^{s} (q^{j_i d_i} - q^{(j_i - 1)d_i})$$

where $m(t) = \prod_{i=0}^{s} f_i^{j_i}$ is the factorisation of $m(t)$ into irreducible polynomials $f_i \in \mathbb{F}_2[t]$ with $\deg(f_i) = d_i$.

We remark that the situation is completely analogous to the possibly more familiar case of finite cyclic groups. Consider an additive cyclic group G with generator g of order M. Replace K by G, w by g, $k[t]$ by $\mathbb{Z}$, $t^n - 1$ by M and $k[t]/(t^n - 1)$ by $\mathbb{Z}/(M)$ and let m be a divisor of M. The analogous version of Theorem 9 then tells us, for example, that the elements $\gamma \in G$ of precise order $m_\gamma = m$ are given in the form $h\gamma_0$ with $0 \leq h < m$, $\gcd\{h, m\} = 1$ and $\gamma_0 = (M/m)g$.

Using Theorem 9 all possible $m_\beta(t)$, the corresponding β and their cardinalities can be easily computed. Combining the various possibilities for $m_\gamma(t)$ and $m_\beta(t)$ yields all possible $m_{\gamma,\beta}(t)$ and genera g_{C^0}. But we also require that $k(\gamma, \beta) = K$, so not all combinations do actually occur. We can obtain sharp lower bounds for g_{C^0} as follows. Let $n_1 = [k(\gamma) : k]$ and $n_2 = [k(\beta) : k]$. Then $n = \operatorname{lcm}\{n_1, n_2\}$. Furthermore, $m_\gamma(t)$ divides $t^{n_1} - 1$ but does not divide $t^s - 1$ for any proper divisor s of n_1, and analogously for $m_\beta(t)$. Enumerating the smallest possibilities for $m_\gamma(t)$ and $m_\beta(t)$ for all n_1, n_2 then yields sharp lower bounds.

The following theorem contains some statistics about the possible genera.

Theorem 10. *Assume that the trace condition of Theorem 3 and $k(\gamma, \beta) = K$ holds. Then $n \leq g_{C^0} \leq 2^n - 1$ and $g_{C^0} \geq 65535$ for all primes $100 \leq n \leq 1000$ except $g_{C^0} = 127$ for $n = 127$ and $g_{C^0} = 32767$ for $n = 151$. The lower bound is attained if and only if*

$$n \in \{1, 2, 3, 4, 7, 15, 21, 31, 63, 93, 105, 127, 217, 255, 381, 465, 511, 889\}.$$

Among these the values $n \in \{1, 2, 3, 4, 7, 15, 31, 63, 127, 255, 511\}$ yield an (elliptic or) hyperelliptic function field C^0.

The proof of Theorem 10 follows the above observations and requires explicit calculations using a computer. We remark that $n \leq g_{C^0} \leq 2n$ for 43 odd and even values of $n \in \{1, \ldots, 1000\}$.

Theorem 10 basically means that the GHS attack in even characteristic fails for large prime values of n since it does not appear that the DLP can be solved more easily in a curve of genus ≥ 65535, albeit defined over k instead of K. On the other hand, composite values of n and in particular the special values given in the list appear susceptible. Note that the extension degree 155 of Example 7 is not shown in Theorem 10, however $n = 31$ is a factor of 155 which was indeed used to construct a curve of genus 31.

Let us now look at the proportion of elliptic curves which yield a small g_{C^0} when n is large. In view of the running time for high genus index calculus a rough estimation of possibly interesting genera is $g_{C^0} \leq n^2$. The following lemma contains a crude upper bound for the proportion of possibly susceptible elliptic curves.

Lemma 11. *Let $\rho \geq 1$. The probability that a C^0 associated to a random elliptic curve $\mathcal{E}_{a,b}$ has a genus at most n^ρ is bounded by approximately $2^{2\rho\log_2(n)+2}q^{2\rho\log_2(n)}/q^n$.*

Proof. It is not difficult to see that $2^{m-d_1}+2^{m-d_2} \leq 2^{m-1}+2$ under the side conditions $1 \leq d_1, d_2 \leq m$, $d_1+d_2 \geq m$. Thus with $d_1 = \deg(m_\gamma)$, $d_2 = \deg(m_\beta)$ and Theorem 3, (ii) it follows that $n^2 \geq g_{C^0} \geq 2^{m-1}-1$ and $m \leq \log_2(n^\rho+1)+1$. Now there are at most 2^{m+1} polynomials over $\mathbb{F}_2$ of degree $\leq m$, so there are at most 2^{2m+2} pairs (m_γ, m_β) such that $m_{\gamma,\beta} = \operatorname{lcm}\{m_\gamma, m_\beta\}$ has degree $\leq m$. Consequently there are at most $2^{2m+2}q^{2m}$ pairs (γ, β) and thus elements $b = (\gamma\beta)^2$. The total number of b is q^n, so the result follows with $m \approx \rho\log_2(n)$. □

As a result we see that the probability of obtaining a relatively small genus for a random elliptic curve quickly becomes negligible as n increases.

The following results are additions to Theorem 9 and can be found in [33].

Lemma 12. *Let n be an odd prime. The polynomial t^n-1 factors over $\mathbb{F}_2$ as $t^n-1 = (t-1)\psi_n(t) = (t-1)h_1(t)\cdots h_s(t)$ where $\psi_n(t)$ denotes the n-th cyclotomic polynomial and the $h_i(t)$'s are distinct polynomials of a degree d. Furthermore, d is the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^\times$ and $d \geq \log_2(n+1)$.*

Corollary 13. *Let $\delta \in \{0,1\}$. For any $\beta \in K$ the degree of $m_\beta(t)$ is of the form $\deg(m_\beta(t)) = id+\delta$, and there are $\binom{s}{i}(q^d-1)^i(q-1)^\delta$ different $\beta \in K$ such that $\deg(m_\beta(t)) = id+\delta$.*

The corollary follows immediately from Theorem 9 and Lemma 12.

2.5. **Further Analysis and the Decompositions $b = \gamma\beta$.** In the following let $m_1(t), m_2(t) \in \mathbb{F}_2[t]$ denote divisors of t^n-1 such that if t^s-1 is divisible by $m_1(t)$ and by $m_2(t)$, then s is divisible by n. In other words, we require $K = k(\gamma,\beta)$ for every $\gamma \in B_{m_1(t)}$ and $\beta \in B_{m_2(t)}$. We abbreviate this condition on m_1 and m_2 by the predicate $P(m_1, m_2)$ and define

$$B_{m_1(t),m_2(t)} = \{\gamma\beta : \gamma \in B_{m_1(t)}, \beta \in B_{m_2(t)}\}.$$

We remark that $B_{m_1(t),m_2(t)}$ is invariant under the 2-power Frobenius automorphism. To distinguish cases we define the predicate

$$T(m_1(t), m_2(t)) = (v_{t-1}(m_1(t)) = 2^{v_2(n)} \text{ or } v_{t-1}(m_2(t)) = 2^{v_2(n)}).$$

Then, let

$$S_{m_1(t),m_2(t)} = \begin{cases} \{\mathcal{E}_{a,b} : a \in \{0,\omega\}, b \in B_{m_1(t),m_2(t)}\} & \text{if } T(m_1(t), m_2(t)), \\ \{\mathcal{E}_{0,b} : b \in B_{m_1(t),m_2(t)}\} & \text{otherwise.} \end{cases}$$

Observe that $T(m_1(t), m_2(t))$ holds true precisely when $\operatorname{Tr}_{K/k}(\gamma) \neq 0$ or $\operatorname{Tr}_{K/k}(\beta) \neq 0$. Thus by Theorem 3 and since $P(m_1, m_2)$ is assumed to hold true, the set $S_{m_1(t),m_2(t)}$

contains elliptic curves for which the GHS reduction applies when using the corresponding γ, α, β. Letting $m_{\gamma,\beta}(t) = \mathrm{lcm}\{m_1(t), m_2(t)\}$ and $m = \deg(m_{\gamma,\beta}(t))$ the resulting genus satisfies $g_{C^0} = 2^m - 2^{m-\deg(m_1(t))} - 2^{m-\deg(m_2(t))} + 1$.

We say that an elliptic curve $\mathcal{E}_{a,b}$ is susceptible to the GHS attack if $\mathcal{E}_{a,b} \in S_{m_1(t),m_2(t)}$ for some "suitable" choices of $m_1(t), m_2(t)$. Here suitable means that $m_1(t), m_2(t)$ are such that we expect that the DLP can be solved more easily in $\mathrm{Pic}_k(C^0)$ than by the Pollard methods in $\mathcal{E}_{a,b}(K)$. With regard to Section 2.3 the main questions then are how to find such suitable choices of $m_1(t), m_2(t)$, how to determine the cardinality of $S_{m_1(t),m_2(t)}$ and how to develop an efficient algorithm which checks whether $\mathcal{E}_{a,b} \in S_{m_1(t),m_2(t)}$ and computes the corresponding decomposition $b = \gamma\beta$ for $\gamma, \beta \in K$ with $m_\gamma = m_1$ and $m_\beta = m_2$. The following lemma gives an answer to these questions in the case of a composite n.

Lemma 14. *Let $n = n_1 n_2$, $K_1 = \mathbb{F}_{q^{n_1}}$ and $b \in K$. Let $f_1 = t^{n_1} - 1$ and $f_2 = (t-1)(t^n - 1)/(t^{n_1} - 1)$.*

(i) The following conditions are equivalent.
1. $\mathrm{Tr}_{K/K_1}(b) \neq 0$,
2. *There exist $\gamma_1, \gamma_2 \in K^\times$ with*
$$\gamma_1\gamma_2 = b,\ \gamma_1 \in K_1 \text{ and } \mathrm{Tr}_{K/K_1}(\gamma_2) \in k^\times$$
3. *There exist $\gamma_1, \gamma_2 \in K^\times$ with*
$\gamma_1\gamma_2 = b$, *m_{γ_1} dividing f_1, m_{γ_2} dividing f_2 and $v_{t-1}(m_{\gamma_2}) = v_{t-1}(f_2)$.*

(ii) If $\mathrm{Tr}_{K/K_1}(b) \neq 0$ then $\gamma_1 = \mathrm{Tr}_{K/K_1}(b)$ and $\gamma_2 = b/\gamma_1$ satisfy the conditions 2 and 3 of (i). For any two decompositions $b = \gamma_1\gamma_2 = \tilde{\gamma}_1\tilde{\gamma}_2$ as in (i) it holds that $\gamma_1/\tilde{\gamma}_1 \in k^\times$.

(iii) Let m_1 divide f_1 and m_2 divide f_2 such that $v_{t-1}(m_2) = v_{t-1}(f_2)$. Then
$$\#B_{m_1,m_2} = \Phi(m_1)\Phi(m_2)/(q-1).$$

(iv) (GHS conditions). In the case of (ii):
1. $k(b) = k(\gamma_1, \gamma_2)$,
2. $\mathrm{Tr}_{K/k}(\gamma_2) \neq 0$ *if and only if n_1 is odd,*
3. $\mathrm{Tr}_{K/k}(\gamma_1) \neq 0$ *if and only if $v_{t-1}(m_b) = 2^{v_2(n)}$ and n/n_1 is odd.*

Proof.

(i)

$1 \Rightarrow 2$. Define $\gamma_1 = \mathrm{Tr}_{K/K_1}(b)$ and $\gamma_2 = b/\gamma_1$, observing $\gamma_1 \neq 0$ by assumption. Then $\mathrm{Tr}_{K/K_1}(\gamma_2) = \mathrm{Tr}_{K/K_1}(b)/\gamma_1 = 1$ which proves the first implication.

$2 \Rightarrow 3$. If $\gamma_1 \in K_1$ then $(t^{n_1} - 1)\gamma_1 = 0$ and hence m_{γ_1} divides f_1. Also, $\mathrm{Tr}_{K/K_1}(\gamma_2) = ((t^n - 1)/(t^{n_1} - 1))\gamma_2 \neq 0$ and $(t-1)\mathrm{Tr}_{K/K_1}(\gamma_2) = 0$ since $\mathrm{Tr}_{K/K_1}(\gamma_2) \in k^\times$. This implies $v_{t-1}(m_{\gamma_2}) = v_{t-1}(f_2)$ and m_{γ_2} divides f_2, and the second implication follows.

$3 \Rightarrow 1$. Since m_{γ_1} divides f_1 we have $\gamma_1 \in K_1$. The conditions $v_{t-1}(m_{\gamma_2}) = v_{t-1}(f_2)$ and m_2 divides f_2 imply that
$$\mathrm{Tr}_{K/K_1}(\gamma_2) = ((t^n - 1)/(t^{n_1} - 1))\gamma_2 \neq 0.$$
Also $\gamma_1 \neq 0$ by assumption, so that $\mathrm{Tr}_{K/K_1}(b) = \gamma_1 \mathrm{Tr}_{K/K_1}(\gamma_2) \neq 0$. This proves the third implication.

(*ii*) The first part follows from the proof of (*i*). Let $b = \gamma_1\beta_1 = \gamma_2\beta_2$ be the two decompositions where $\gamma_i \in K_1$ and $\mu_i = \mathrm{Tr}_{K/K_1}(\beta_i) \in k^\times$ by (*i*). Then $\gamma_1\mu_1 = \mathrm{Tr}_{K/K_1}(b) = \gamma_2\mu_2 \neq 0$. Thus $\gamma_1/\gamma_2 \in k^\times$.

(*iii*) Using Theorem 9 and observing $\gamma_1\gamma_2 = (\lambda\gamma_1)(\lambda^{-1}\gamma_2)$ for $\lambda \in k^\times$ it follows that $\#B_{m_1,m_2} \leq \Phi(m_1)\Phi(m_2)/(q-1)$. Because of (*ii*) this is in fact an equality.

(*iv*)

(1) $k(b) \subseteq k(\gamma_1, \gamma_2)$ is clear since $b = \gamma_1\gamma_2$. On the other hand, $\gamma_2 = \mathrm{Tr}_{K/K_1}(b) \in k(b)$, hence $\gamma_1 = b/\gamma_2 \in k(b)$ and $k(\gamma_1, \gamma_2) \subseteq k(b)$ follows.

(2) Writing $\lambda = \mathrm{Tr}_{K/K_1}(\gamma_2)$ we have $\mathrm{Tr}_{K/k}(\gamma_2) = \mathrm{Tr}_{K_1/k}(\lambda) = n_1\lambda$ since $\lambda \in k^\times$.

(3) We have that $\mathrm{Tr}_{K/k}(\gamma_1) \neq 0$ is equivalent to $v_{t-1}(m_{\gamma_1}) = 2^{v_2(n)}$. Also, we have m_{γ_1} divides m_b since $\gamma_1 = ((t^n-1)/(t^{n_1}-1))b$ and $v_{t-1}(m_{\gamma_1}) = v_{t-1}(m_b)$ if and only if n/n_1 is odd. This implies the statement.

□

Corollary 15. *Assume that n_1 is odd. Then*

$$\left\{ \mathcal{E}_{a,b} : \begin{array}{l} a \in \{0,\omega\}, \\ \mathrm{Tr}_{K/K_1}(b) \neq 0, \\ k(b) = K \end{array} \right\} = \bigcup \left\{ S_{m_1,m_2} : \begin{array}{l} m_1 \text{ divides } f_1, \\ m_2 \text{ divides } f_2, \\ v_{t-1}(m_2) = 2^{v_2(n)}, \\ P(m_1,m_2) \end{array} \right\},$$

where the union is disjoint.

Example 16. Consider $n = 6$, $n_1 = 3$ and $n_2 = 2$. Using Corollary 15 wee see that every elliptic curve over $\mathbb{F}_{q^6}$ with $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(b) \neq 0$ leads to a genus $g_{C^0} \in \{8, 9, 11, 12, 14\}$.

We now focus on the case where n is an odd prime. We can then use Lemma 12 and Corollary 13. Over $\mathbb{F}_2$ we have the factorization into irreducible polynomials $t^n + 1 = (t-1)h_1 \cdots h_s$ and $\deg(h_i) = d$ such that $n = sd + 1$. In this situation the first non-trivial $m = \deg(m_{\gamma,\beta})$ satisfies $d \leq m \leq d+1$ corresponding to $m_{\gamma,\beta} = h_i$ or $m_{\gamma,\beta} = (t-1)h_i$ by Theorem 9 and equation (22), observing that $(t-1) \nmid h_i$. After that we already have $m \geq 2d$ which is too big in most instances. The case $m = d$ is (only) obtained when $\gamma, \beta \in B_{h_i(t)}$ and $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$. The conditions of Theorem 3 are fulfilled so the GHS reduction does work and the resulting genus is $g_{C^0} = 2^d - 1$. The case $m = d+1$ leads to the smallest genera when $\gamma \in B_{t-1}$ and $\beta \in B_{h_i(t)} \cup B_{(t-1)h_i(t)}$ which is a disjoint union. Since $\mathrm{Tr}_{K/k}(\gamma) = n\gamma \neq 0$ the conditions of Theorem 3 are fulfilled for every $\alpha \in \{0, \omega\}$ and the genus g_{C^0} is $2^d - 1$ if $\beta \in B_{h_i(t)}$ and 2^d if $\beta \in B_{(t-1)h_i(t)}$.

The transformation between (2) and (1) is described by $b = (\gamma\beta)^2$ and $a = \alpha$. The map $(\gamma, \beta) \mapsto (\gamma\beta)^2$ is not injective, so several tuples (γ, β) will lead to the same elliptic curve. It is $(q-1)$-1 when restricted to $B_{t-1} \times B_{h_i}$ or $B_{t-1} \times B_{(t-1)h_i}$, and at least $2(q-1)$-1 when restricted to $B_{h_i} \times B_{h_i}$. Namely, the tuples $(\lambda\gamma, \lambda^{-1}\beta)$ for $\lambda \in k^\times$ and also (β, γ) in the latter case are mapped to the same b as (γ, β). Heuristically we expect that the fibres are not much bigger than $2(q-1)$ in this case if $\#(B_{h_i} \times B_{h_i})$ is small in comparison with $\#K$. Now clearly $B_{t-1,h_i} = B_{h_i}$ and

m_γ	m_β	α	g_{C^0}	$\approx \#S_{m_\gamma,m_\beta}$
h_i	h_i	0	2^d-1	$\min\{q^n, sq^{2d-1}/2\}^\dagger$
$t-1$	h_i	$0,\omega$	2^d-1	$2sq^d$
$t-1$	$(t-1)h_i$	$0,\omega$	2^d	$2sq^{d+1}$

TABLE 1. Cardinalities of S_{m_γ,m_β} for n odd prime

$B_{t-1,(t-1)h_i} = B_{(t-1)h_i}$, so these sets are disjoint for all i and we obtain $\#\cup_i B_{t-1,h_i} = s(q^d-1)$ and $\#\cup_i B_{t-1,(t-1)h_i} = s(q-1)(q^d-1)$. Furthermore we expect that $\#B_{h_i,h_i} \approx \min\{q^n, (q^d-1)^2/(2(q-1))\}$ and that $\#\cup_i B_{h_i,h_i} \approx \min\{q^n, s(q^d-1)^2/(2(q-1))\}$.

A summary is given in Table 1. Note that the elliptic curves from S_{m_γ,m_β} of the last two rows lead to hyperelliptic function fields C^0 and that the cardinality † is only heuristically expected (Lemma 17 provides proven bounds in special cases).

If h_i is of a trinomial form we have the following precise statement.

Lemma 17. *Assume $h = t^{r_1} + t^{r_2} + 1$ with $r_1 > r_2 > 0$, $\gcd\{r_2, n\} = 1$ and $m_b \nmid h$. Then there are no or precisely $2(q-1)$ pairs $(\gamma,\beta) \in K^2$ such that $b = \gamma\beta$ and $m_\gamma = m_\beta = h$.*

Proof. Assume that $b = \gamma\beta$ and $m_\gamma = m_\beta = h$. Then $\gamma \neq 0$ and $\beta \neq 0$ since $b \neq 0$, and consequently

$$\gamma^{q^{r_1}-1} + \gamma^{q^{r_2}-1} + 1 = 0,$$
$$b^{q^{r_1}-1} + b^{q^{r_2}-1}\gamma^{q^{r_1}-q^{r_2}} + \gamma^{q^{r_1}-1} = 0.$$

Define $\rho = \gamma^{q^{r_2}-1}$. The first equation implies

$$\gamma^{q^{r_1}-1} = \rho + 1, \tag{18}$$
$$\gamma^{q^{r_1}-q^{r_2}} = (\rho+1)/\rho.$$

Substituting this into the second equation yields $b^{q^{r_1}-1} + b^{q^{r_2}-1}(\rho+1)/\rho + \rho + 1 = 0$ and then

$$\rho^2 + (b^{q^{r_1}-1} + b^{q^{r_2}-1} + 1)\rho + b^{q^{r_2}-1} = 0. \tag{19}$$

On the other hand, any further solution ρ, γ, β to (19), (18), $\gamma^{q^{r_2}-1} = \rho$ and $\beta = b/\gamma$ satisfies $m_\gamma = m_\beta = h$ because $b \neq 0$.

Since $m_b \nmid h$ we have that $\gamma/\beta \notin k$. There are thus at least $2(q-1)$ pairwise distinct solutions of the form $(\lambda\gamma, \lambda^{-1}\beta)$ and $(\lambda\beta, \lambda^{-1}\gamma)$ with $\lambda \in k^\times$. On the other hand there are at most two possibilities for ρ and at most $q-1$ possibilities for γ for each ρ, resulting in at most $2(q-1)$ solutions. Namely, for any two solutions γ_1, γ_2 with $\gamma_i^{q^{r_2}-1} = \rho$ we have that $(\gamma_1/\gamma_2)^{q^{r_2}-1} = 1$ and hence $\gamma_1/\gamma_2 \in \mathbb{F}_{q^{r_2}} \cap \mathbb{F}_{q^n}^\times = \mathbb{F}_q^\times$ since r_2 and n are coprime. □

Given b and h as in the Lemma, γ and β can be computed efficiently as follows, using Langrange's resolvent [29, p. 289].

1. Solve for ρ such that $\rho^2 + (b^{q^{r_1}-1} + b^{q^{r_2}-1} + 1)\rho + b^{q^{r_2}-1} = 0$.
2. Compute θ such that

$$\gamma = \theta + \rho^{-1}\theta^{q_2} + \rho^{-1-q_2}\theta^{q_2^2} + \cdots + \rho^{-1-q_2-\cdots-q_2^{n-2}}\theta^{q_2^{n-1}} \neq 0,$$

where $q_2 = q^{r_2}$. This can be achieved by linear algebra over k.
3. Compute $\beta = b/\gamma$.

If $\mathrm{N}_{K/k}(\rho) \neq 1$ in step 1 or if γ does not satisfy (18) in step 2 then there are no solutions γ, β with $m_\gamma = m_\beta = h$.

Example 20. Consider $n = 7$. Then $t^n - 1 = (t-1)(t^3+t+1)(t^3+t^2+1)$, $d = 3$ and $s = 2$. Using the first row of Table 1 we see that a proportion of about q^{-2} of all elliptic curves over $\mathbb{F}_{q^7}$ with $\alpha = 0$ leads to $g_{C^0} = 7$.

In Lemmas 14 and 17 we have discussed the decomposition $b = \gamma\beta$ and how to check $\mathcal{E}_{a,b} \in S_{m_1,m_2}$ in some special cases. A simple and the currently only known method to do this in full generality is to take all $\gamma \in B_{m_1}$ and to test whether $m_{b/\gamma} = m_2$. Of course, for any γ we do not need to check $\lambda\gamma$ with $\lambda \in k^\times$.

2.6. **Further Details.** In this section we present some details on the Artin-Schreier construction of Theorem 3 and provide the parts of the proof of Theorem 3 which have not occurred in the literature.

We let p denote an arbitrary prime for the moment, abbreviate $F = K(x)$ and let $f \in F$ be a rational function. A simple Artin-Schreier extension denoted by E_f, is given by adjoining to F a root of the polynomial $y^p - y - f \in F[y]$. Examples of such extensions are the function fields of elliptic curves in characteristic two and three.

The Artin-Schreier operator is denoted by $\wp(y) = y^p - y$. We then also write $F(\wp^{-1}(f))$ for E_f and $\wp(F) = \{\, f^p - f : f \in F \,\}$. More generally Theorem 3 uses the following construction and theorem which is a special version of [35, p. 279, Theorem 3.3]:

Theorem 21. *Let $\bar{F}$ be a fixed separable closure of F. For every additive subgroup $\Delta \leq F$ with $\wp(F) \subseteq \Delta \subseteq F$ there is a field $C = F\big(\wp^{-1}(\Delta)\big)$ with $F \subseteq C \subseteq \bar{F}$ obtained by adjoining all roots of all polynomials $y^p - y - d$ for $d \in \Delta$ in $\bar{F}$ to F. Given this, the map*

$$\Delta \mapsto C = F\big(\wp^{-1}(\Delta)\big)$$

defines a 1-1 correspondence between such additive subgroups Δ and abelian extensions C/F in $\bar{F}$ of exponent p.

For our purposes this construction is only applied for very special Δ, introduced in a moment. As in Section 1.2, by a Frobenius automorphism with respect to K/k of a function field over K we mean an automorphism of order $n = [K : k]$ of that function field which extends the Frobenius automorphism of K/k. Raising the coefficients of a rational function in $F = K(x)$ to the q-th power yields for example a Frobenius automorphism of F with respect to K/k, which we denote by σ.

For $f \in F$ we define $\Delta_f := \{\, d^p - d + \sum_{i=0}^{n-1} \lambda_i \sigma^i(f) : d \in F \text{ and } \lambda_i \in \mathbb{F}_p \,\}$. This is the subgroup of the additive group of F which is generated by f and contains $\wp(F)$. Also, let $m_f = \sum_{i=0}^{m} \lambda_i t^i$ with $\lambda_m = 1$ be the unique polynomial of smallest

degree in $\mathbb{F}_p[t]$ such that $\sum_{i=0}^m \lambda_i \sigma^i(f) = d^p - d$ for some $d \in F$. Similar as in Section 2.4 we can define a multiplication of polynomials $h(t) = \sum_{i=0}^d \lambda_i t^i \in k[t]$ and rational functions $z \in F$ by $h(t)z = \sum_{i=0}^d \lambda_i \sigma^i(z)$. This makes the additive group of F into a $k[t]$-module. The polynomials $m_f(t)$ are then by definition polynomials in $\mathbb{F}_p[t]$ of smallest degree such that $m_f(t)f \in \wp(F)$. The field $F\big(\wp^{-1}(\Delta_f)\big)$ exists by Theorem 21 and has degree $p^{\deg(m_f)}$ over F. Further statements on the existence of a Frobenius automorphism of this field with respect to K/k and it genus can be found in [23].

We let now $p = 2$ and $f = \gamma/x + \alpha + \beta x$. The field $F\big(\wp^{-1}(\Delta_f)\big)$ is then equal to the field C of Theorem 3 defined in Section 2.1. Let us exhibit an explicit model for C. We have

$$m_f = \begin{cases} \operatorname{lcm}\{m_\gamma, m_\beta\} & \text{if } \operatorname{Tr}_{K/\mathbb{F}_2}(\alpha) = 0, \\ \operatorname{lcm}\{m_\gamma, m_\beta, t+1\} & \text{otherwise.} \end{cases} \tag{22}$$

Let $m = \deg(m_f)$. The classes of $\sigma^i(f)$ for $0 \le i \le m-1$ form a $\mathbb{F}_2$-basis of $\Delta_f/\wp(F)$. From Theorem 21 it follows that C is obtained by adjoining one root of every $y^2 - y - \sigma^i(f)$ to F. In other words, $C = F[y_0, \dots, y_{m-1}]/I$ where I is the ideal of the polynomial ring $F[y_0, \dots, y_{m-1}]$ generated by the polynomials $y_i^2 - y_i - \sigma^i(f)$ for $0 \le i \le m-1$. We write $\bar{y}_i$ for the images of the y_i in C and abbreviate $\bar{y} = \bar{y}_0$.

Using this notation we are able to prove Theorem 3, (*iii*) and (*iv*). Assume without loss of generality that $\deg(m_\gamma) \le \deg(m_\beta)$. Let $h \in \mathbb{F}_2[t]$. The field C then contains the roots of $y^2 - y - h(t)f$ and is generated by these roots for all h of degree less than m. Using polynomial division write $h = sm_\gamma + r$ with $s, r \in \mathbb{F}_2[t]$ and $\deg(r) < \deg(m_\gamma)$. Thus $h(t)f = s(t)(m_\gamma(t)f) + r(t)f$. The rational function $m_\gamma(t)f$ is of the form $\rho + \delta x$ with $\rho, \delta \in K$. As a result, $h(t)f$ is a $\mathbb{F}_2$-linear combination of the conjugates $\sigma^i(f)$ for $0 \le i \le \deg(m_\gamma) - 1$ and $\sigma^j(m_\gamma(t)f)$ for $0 \le j \le m - \deg(m_\gamma) - 1$. We write $\bar{w}_j$ for a root of the polynomials $w_j^2 - w_j - \sigma^j(m_\gamma(t)f)$ in C. Then $C = F[\bar{y}_0, \dots, \bar{y}_{\deg(m_\gamma)-1}, \bar{w}_0, \dots, \bar{w}_{m-\deg(m_\gamma)-1}]$. By [20, Lemma 7] the field $L = F[\bar{w}_0, \dots, \bar{w}_{m-\deg(m_\gamma)-1}]$ is a rational function field and the extension L/F has degree $2^{m-\deg(m_\gamma)}$. Since C/F has degree 2^m we see that L has index $2^{\deg(m_\gamma)}$ in C. Furthermore, L is equal to $F(\wp^{-1}(\Delta_{m_\gamma(t)f}))$. Since $\sigma(\Delta_{m_\gamma(t)f}) = \Delta_{m_\gamma(t)f}$ we have that the Frobenius automorphism σ on C restricts to a Frobenius automorphism on L. It thus follows that the fixed field L^0 of σ in L is a rational function field over k and has index $2^{\deg(m_\gamma)}$ in C^0. This proves Theorem 3, (*iii*).

The hyperellipticity in Theorem 3, (*iv*) is proven in [20] and can be seen as follows. If $\gamma \in k$ then $m_\gamma = t - 1$. Consequently, by (*iii*) we see that C^0 contains a rational subfield of index 2, which yields the statement.

3. Extending the GHS Attack using Isogenies

3.1. **The Basic Idea.** The GHS attack can be extended to a much larger class of curves by using isogenies. Consider two elliptic curves $\mathcal{E}$ and $\mathcal{E}'$ defined over K. An isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ defined over K homomorphically maps points in $\mathcal{E}(K)$ to points in $\mathcal{E}'(K)$. The coordinates of an image point are defined by algebraic expressions involving the coordinates of the input point and elements of K, in a similar way

to the addition formulae. In particular, a discrete logarithm problem $P = \lambda Q$ is mapped to the discrete logarithm problem $\phi(P) = \lambda\phi(Q)$. The basic idea is that $\mathcal{E}'$ might be susceptible to the GHS attack while $\mathcal{E}$ is not. In this case we would transfer the discrete logarithm problem on $\mathcal{E}$ to $\mathcal{E}'$ using ϕ and attempt to solve it there.

For every isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ defined over K there is a dual isogeny $\hat{\phi} : \mathcal{E}' \to \mathcal{E}$ defined over K and $\mathcal{E}$ is said to be isogenous to $\mathcal{E}'$. This yields an equivalence relation so that elliptic curves defined over K can be partitioned into isogeny classes. Also, the isogeny class of an elliptic curve defined over K is uniquely determined by $\#\mathcal{E}(K) = q^n + 1 - t$ and its cardinality is roughly, and on average, of the order $(4q^n - t^2)^{1/2}$ where t satisfies $|t| \leq 2q^{n/2}$ (more precisely the cardinality is equal to the Kronecker-Hurwitz class number $H(t^2 - 4q^n)$, see [18], [37]).

If an isogeny class contains an elliptic curve which is susceptible to the GHS attack the whole isogeny class can be considered susceptible using the above idea. Of course this raises the following two questions: Can it be efficiently determined whether an isogeny class contains a susceptible curve and if so, can the isogeny be efficiently computed? There are two main strategies:

Isogeny Strategy 1. For all $\mathcal{E}'$ which are susceptible to the GHS attack check whether $\#\mathcal{E}'(K) = \#\mathcal{E}(K)$. If so, compute the isogeny between $\mathcal{E}$ and $\mathcal{E}'$.

Isogeny Strategy 2. Compute random (all) $\mathcal{E}'$ in the isogeny class of $\mathcal{E}$ and the corresponding isogenies from $\mathcal{E}$ to $\mathcal{E}'$. Check whether one of the $\mathcal{E}'$ is susceptible to the GHS attack.

Again, we only consider elliptic curves in the unique form (1) so that we are effectively dealing here and in the following with isomorphism classes of elliptic curves.

Assuming that the cardinality of the isogeny class of $\mathcal{E}$ is roughly $q^{n/2}$ and that isogeny class membership and being susceptible to the GHS attack are basically independent properties we expect that Strategy 1 is more efficient in terms of checks than Strategy 2 if the number of the susceptible $\mathcal{E}'$ is less than $q^{n/2}$, and that Strategy 2 is more efficient otherwise.

3.2. **Isogeny Probabilities.** Let $S'_{m_1(t),m_2(t)}$ denote a system of conjugacy class representatives of the operation of the 2-power Frobenius on $S_{m_1(t),m_2(t)}$. In order to obtain some quantitative statements about the above strategies we assume that $S'_{m_1(t),m_2(t)}$ behaves like any randomly and uniformly chosen set of ordinary elliptic curves defined over K of the same cardinality. We want to estimate the probability that a randomly and uniformly chosen elliptic curve $\mathcal{E}$ is isogenous to a fixed subset of N elliptic curves $\mathcal{E}_i$ from $S'_{m_1(t),m_2(t)}$.

Lemma 23. *Let $\mathcal{E}, \mathcal{E}_1, \ldots, \mathcal{E}_N$ be randomly, uniformly and independently chosen ordinary elliptic curves. Then*

$$\Pr(\mathcal{E} \sim \mathcal{E}_1 \text{ or } \ldots \text{ or } \mathcal{E} \sim \mathcal{E}_N) \geq 1 - \left(1 - \frac{1}{(1-1/p)4q^{n/2} + 2}\right)^N.$$

Proof. Abbreviate $A_N = \Pr(\mathcal{E} \sim \mathcal{E}_1 \text{ or } \ldots \text{ or } \mathcal{E} \sim \mathcal{E}_N)$ and let $\mathcal{E}'$ denote a further randomly, uniformly and independently chosen ordinary elliptic curve. Using the

complementary event it is straightforward to prove that

$$A_N = 1 - (1 - \Pr(\mathcal{E} \sim \mathcal{E}'))^N. \tag{24}$$

If a_i are M non-negative numbers such that $\sum_{i=1}^M a_i = 1$ then $\sum_{i=1}^M a_i^2 \geq 1/M$. This is easily seen by writing $a_i = 1/M + \varepsilon_i$ with $\sum_i \varepsilon_i = 0$ and expanding this in $\sum_{i=1}^M a_i^2$.

The following sums are over all ordinary isogeny classes I and the symbol $\#\{I\}$ denotes the number of such classes. Using the above observation with $a_i = \Pr(\mathcal{E} \in I)$ and $M = \#\{I\}$ we see

$$\begin{aligned} \Pr(\mathcal{E} \sim \mathcal{E}') &= \sum_I \Pr(\mathcal{E} \in I \text{ and } \mathcal{E}' \in I) = \sum_I \Pr(\mathcal{E} \in I) \Pr(\mathcal{E}' \in I) \\ &= \sum_I \Pr(\mathcal{E} \in I)^2 \geq 1/\#\{I\}. \end{aligned} \tag{25}$$

The number of ordinary isogeny classes satisfies

$$\#\{I\} \leq (1 - 1/p)4q^{n/2} + 2. \tag{26}$$

This is because every integer $q^n + 1 - t$ with $t^2 \leq 4q^n$ and $p \not| t$ occurs as the number of points of an ordinary elliptic curve over K (see [45]).

Combining (26), (25) and (24) yields the lemma. □

According to Lemma 23 it is reasonable to expect that a randomly and uniformly chosen elliptic curve $\mathcal{E}$ will be isogenous to at least one of the $\mathcal{E}_i$ from S'_{m_1,m_2} with probability approximately at least $N/(2q^{n/2})$, if N is much less than $q^{n/2}$, and with probability approximately one, if N is much larger than $q^{n/2}$. The first probability can in fact be improved slightly when one restricts for example to elliptic curves (1) with $a = 0$. Recall that if $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$ then the group order $\#E(K)$ of the elliptic curve is congruent to 0 modulo 4 and if $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 1$ then it is congruent to 2 modulo 4 (see [1, p. 38]). Thus elliptic curves with $a = 0$ represent only about half of all isogeny classes. It follows that the first of the above probabilities improves by a factor of two. Another property in this line is $\#E(K) = 0 \bmod 8$ if and only if $\mathrm{Tr}_{K/\mathbb{F}_2}(b) = 0$ for $a = 0$ and $nr \geq 3$ ([34]).

By our assumption on S'_{m_1,m_2} and in view of Isogeny Strategy 2 we expect that membership in S'_{m_1,m_2} and being isogenous to a randomly and uniformly chosen elliptic curve $\mathcal{E}$ are approximately independent events if $\#S'_{m_1,m_2}$ is much larger than $q^{n/2}$. More precisely we expect $\#(S'_{m_1,m_2} \cap I) \approx \#S'_{m_1,m_2}\#I/(2q^n)$ since the curves from S'_{m_1,m_2} should distribute over the isogeny classes relative to their sizes.

3.3. **Computing Isogenies.** Isogeny Strategy 1 and 2 require the computation of isogenies. In Isogeny Strategy 1 we have to construct the isogeny between $\mathcal{E}$ and $\mathcal{E}'$ given only that $\#\mathcal{E}(K) = \#\mathcal{E}'(K)$. In Isogeny Strategy 2 we start with $\mathcal{E}$ and have to construct the isogeny to a randomly and uniformly chosen $\mathcal{E}'$ of the unique form (1) in the isogeny class of $\mathcal{E}$.

We recall some additional basic facts about isogenies and endomorphism rings for *ordinary* elliptic curves. Useful references for the required theory and algorithmic aspects are [32, 39, 37, 14, 17, 28].

Endomorphisms of $\mathcal{E}$ are isogenies of $\mathcal{E}$ to itself. Addition and composition of maps makes the set of endomorphisms into a ring $\mathrm{End}(\mathcal{E})$. For elliptic curves defined over K all endomorphismus are defined over K as well. The q^n-th power Frobenius endomorphism $\pi : (x, y) \mapsto (x^{q^n}, y^{q^n})$ satisfies $\pi^2 - t\pi + q^n = 0$ with $t = q^n + 1 - \#\mathcal{E}(K)$, $t^2 \leq 4q^n$ and $t \not\equiv 0 \bmod p$, so $\mathbb{Q}(\pi)$ is an imaginary qadratic number field. The ring $\mathrm{End}(\mathcal{E})$ is an order in $\mathbb{Q}(\pi)$ with $\mathbb{Z}[\pi] \subseteq \mathrm{End}(\mathcal{E}) \subseteq \mathcal{O}_{\max}$, where $\mathcal{O}_{\max}$ is the maximal order or ring of algebraic integers of $\mathbb{Q}(\pi)$. Conversely, if $\pi^2 - t\pi + q^n = 0$, $t^2 \leq 4q^n$ and $t \not\equiv 0 \bmod p$ for some algebraic integer π then every order $\mathcal{O}$ with $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_{\max}$ occurs as the endomorphism ring of an elliptic curve $\mathcal{E}$ defined over K with $\#\mathcal{E}(K) = q+1-t$, such that π corresponds to the q^n-th power Frobenius endomorphism. There is a bijection of positive integers d and suborders $\mathcal{O}_d$ of $\mathcal{O}_{\max}$ of index d, given by $d \mapsto \mathcal{O}_d = \mathbb{Z} + d\mathcal{O}_{\max}$. The integer d is called conductor of $\mathcal{O}_d$.

The degree of an isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ defined over K is equal to the degree of the function field extension $K(\mathcal{E})/K(\mathcal{E}')$ defined by ϕ and coincides roughly with the degrees of its defining algebraic expressions. The degree of isogenies is multiplicative with respect to composition. Every isogeny defined over K can be decomposed into a chain of isogenies of prime degree defined over K. The cardinality of the kernel of ϕ as a homomorphism from $\mathcal{E}(K)$ to $\mathcal{E}'(K)$ is bounded by the degree of ϕ (and equal to the degree if ϕ is separable and K is algebraically closed). An isomorphism is an isogeny of degree one. For every $\mathcal{E}$ defined over K there is an $\mathcal{E}'$ defined over K (a quadratic twist of $\mathcal{E}$) such that for the j-invariants $j(\mathcal{E}) = j(\mathcal{E}')$, $\mathcal{E}$ and $\mathcal{E}'$ are isomorphic over a quadratic extension of K, and every $\mathcal{E}_2$ defined over K with $j(\mathcal{E}_2) = j(\mathcal{E})$ is isomorphic over K to $\mathcal{E}$ or $\mathcal{E}'$. Furthermore $\#\mathcal{E}(K) + \#\mathcal{E}'(K) = 2q^n + 2$. If ϕ is of degree r then $\phi_r(j(\mathcal{E}), j(\mathcal{E}')) = 0$ where ϕ_r is the r-th modular polynomial. Conversely, if $\phi_r(j(\mathcal{E}), x) = 0$ for $x \in K$ then there is an $\mathcal{E}'$ defined over K with $j(\mathcal{E}') = x$ and an isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ defined over K of degree r.

If $\mathcal{E}$ and $\mathcal{E}'$ are isogenous then $\mathrm{End}(\mathcal{E})$ and $\mathrm{End}(\mathcal{E}')$ are (isomorphic to) orders within the same imaginary quadratic number field. More specificially it holds that $\mathrm{End}(\mathcal{E}) = \mathrm{End}(\mathcal{E}')$, $\mathrm{End}(\mathcal{E}) \subseteq \mathrm{End}(\mathcal{E}')$ with $(\mathrm{End}(\mathcal{E}') : \mathrm{End}(\mathcal{E})) = \ell$ or $\mathrm{End}(\mathcal{E}') \subseteq \mathrm{End}(\mathcal{E})$ with $(\mathrm{End}(\mathcal{E}) : \mathrm{End}(\mathcal{E}')) = \ell$, if there is an isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ of prime degree ℓ. The cases where the index changes can be (partly) read off the number of zeros of $\phi_\ell(j(\mathcal{E}), x)$. An isogeny $\phi : \mathcal{E} \to \mathcal{E}'$ of elliptic curves with $\mathcal{O} = \mathrm{End}(\mathcal{E}) = \mathrm{End}(\mathcal{E}')$ defines a uniquely determined invertible (and integral) ideal I of $\mathcal{O}$ with $\mathrm{N}(I) = \deg(\phi)$, and any such I is obtained this way. Isomorphisms ϕ correspond to $I = \mathcal{O}$. Composition of isogenies corresponds to ideal multiplication. If $\phi_1 : \mathcal{E} \to \mathcal{E}_1$ and $\phi_2 : \mathcal{E} \to \mathcal{E}_2$ are isogenies with the ideals I_1 and I_2 then $\mathcal{E}_1$ is isomorphic to $\mathcal{E}_2$ if and only if I_1/I_2 is principal. As a result, the isogeny structure between the isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}$ is equivalent to the group structure of $\mathrm{Pic}(\mathcal{O})$, the group of classes of invertible ideals of $\mathcal{O}$ modulo principal ideals.

The basic technique in Isogeny Strategy 1 and 2 is as follows. For $\mathcal{O} = \mathrm{End}(\mathcal{E})$ we can use the group structure of $\mathrm{Pic}(\mathcal{O})$ for random walks along chains of isogenies of prime degree starting at $\mathcal{E}$. This way we can generate random elliptic curves $\mathcal{E}'$ with $\mathrm{End}(\mathcal{E}') = \mathcal{O}$ and known isogenies $\mathcal{E} \to \mathcal{E}'$ for Isogeny Strategy 2. For Isogeny Strategy 1 we use a second random walk starting at the second elliptic curve $\mathcal{E}'$,

assuming $\mathrm{End}(\mathcal{E}') = \mathcal{O}$ for the moment. If these walks meet we can connect the two parts using dual isogenies to obtain a chain of isogenies from $\mathcal{E}$ to $\mathcal{E}'$. Since we consider only elliptic curves of the unique form (1) we are effectively working with isomorphism classes.

A single step in the random walk from a curve $\mathcal{E}_i$ to a curve $\mathcal{E}_{i+1}$ to be determined proceeds as follows. We assume that $\mathcal{O} = \mathrm{End}(\mathcal{E})$ is known and $\mathrm{End}(\mathcal{E}_i) = \mathcal{O}$ holds, where $\mathcal{O}$ can be computed by the algorithm of Kohel [28]. A prime number ℓ is chosen which does not divide the conductor of $\mathcal{O} = \mathrm{End}(\mathcal{E}_i)$ and is split or ramified in $\mathcal{O}$. The j-invariants of the curves $\mathcal{E}_{i+1}$ related to $\mathcal{E}_i$ by an isogeny of degree ℓ are the roots x of $\phi_\ell(j(\mathcal{E}_i), x)$ in K. If (and only if) ℓ divides the index of $\mathbb{Z}[\pi]$ in $\mathcal{O}$ then not all of these roots result in an $\mathcal{E}_{i+1}$ with $\mathrm{End}(\mathcal{E}_{i+1}) = \mathrm{End}(\mathcal{E}_i)$, the case $(\mathrm{End}(\mathcal{E}_i) : \mathrm{End}(\mathcal{E}_{i+1})) = \ell$ is also possible. Using the techniques of [28, p. 46] we determine those x for which $\mathcal{E}_{i+1}$ isogenous to $\mathcal{E}_i$ has the same endomorphism ring. According to whether ℓ is ramified or split there are one or two such values. We choose a value and compute $\mathcal{E}_{i+1}$ of the unique form (1) and the isogeny from it. Checking the action of the Frobenius or another suitable endomorphism on the kernel of the isogeny (i.e. on an eigenvalue of the Frobenius) allows to determine the prime ideal of norm ℓ above ℓ which corresponds to the isogeny [1, 38].

For the whole random walk we note that any class in $\mathrm{Pic}(\mathcal{O})$ can be represented by an ideal of $\mathcal{O}$ of (small) norm $O(|d(\mathcal{O})|^{1/2})$, where $d(\mathcal{O})$ denotes the discriminant of $\mathcal{O}$ and is $O(q^{n/2})$. Furthermore, $\#\mathrm{Pic}(\mathcal{O}) \approx O(|d(\mathcal{O})|^{1/2})$ and $\mathrm{Pic}(\mathcal{O})$ is generated by split prime ideals of (very small) norm $O(\log(|d(\mathcal{O})|)^2)$ under the GRH (generalised Riemann hypothesis). We let B denote a set of split or ramified prime ideals of very small norm which generate $\mathrm{Pic}(\mathcal{O})$, and let B_0 the corresponding prime numbers. The prime numbers ℓ in every single step are chosen from B_0 such that the walk extends over the whole of $\mathrm{Pic}(\mathcal{O})$. Furthermore, the i-th step of the random walk starting at $\mathcal{E}$ can be represented by a single ideal I_i of small norm, corresponding to an isogeny $\mathcal{E} \to \mathcal{E}_i$. The ideal I_i is defined inductively as follows. First, $I_0 = \mathcal{O}$. For the $i+1$-th step the curve $\mathcal{E}_{i+1}$, an isogeny and a prime ideal P are computed as above. Then I_{i+1} is defined to be a representative of small norm of the class of $I_i P$ and corresponds to an isogeny $\mathcal{E} \to \mathcal{E}_{i+1}$.

Assume the random walk stops at $\mathcal{E}_r$, and the isogeny $\mathcal{E} \to \mathcal{E}_r$ is described by I_r or a chain of isogenies of prime degree. The factorisation of I_r is likely to contain prime ideals which have too large norm for our purpose. Also, the chain may have length exponential in $n\log(q)$. We can obtain a much reduced chain as follows. Using techniques from index calculus in imaginary quadratic orders we compute a representation of I_r in $\mathrm{Pic}(\mathcal{O})$ in terms of powers of the elements of B or an enlargement of B in the form $I_r = (\gamma)\prod_{i=1}^{m} P_i^{d_i}$ where m and the d_i are (expected to be) polynomial in $n\log(q)$ if B is sufficiently large. Again using techniques from point counting we determine a chain of explicitly given isogenies from $\mathcal{E}$ to $\mathcal{E}_r$, such that every step corresponds to a P_i. This concludes the description of the random walks on (isomorphism classes of) elliptic curves with endomorphism ring $\mathcal{O}$.

In Isogeny Strategy 2 we do not want to restrict the possible endomorphism rings to a given $\mathcal{O}$. In a precomputation we compute all intermediate orders $\mathcal{O}_\nu$ with $\mathbb{Z}[\pi] \subseteq \mathcal{O}_\nu \subseteq \mathcal{O}_{\max}$ and isogenies $\mathcal{E} \to \mathcal{E}_\nu$ to curves $\mathcal{E}_\nu$ with $\mathcal{O}_\nu = \mathrm{End}(\mathcal{E}_\nu)$, using

[28]. We start random walks in every $\mathcal{E}_\nu$. In every step we choose ν with probability about $\sum_{\mu\neq\nu}\#\mathrm{Pic}(\mathcal{O}_\mu)/\sum_\mu \#\mathrm{Pic}(\mathcal{O}_\mu)$ and extend the walk from say $\mathcal{E}_{\nu,i}$ to some $\mathcal{E}_{\nu,i+1}$. The curve $\mathcal{E}_{\nu,i+1}$ is returned.

In Isogeny Strategy 1 the curves $\mathcal{E}$ and $\mathcal{E}'$ may have different endomorphism rings. In a precomputation we compute isogenies $\mathcal{E}\to\mathcal{E}_0$ and $\mathcal{E}'\to\mathcal{E}'_0$ such that $\mathrm{End}(\mathcal{E}_0)$ and $\mathrm{End}(\mathcal{E}'_0)$ are equal to $\mathcal{O}=\mathcal{O}_{\max}$. Following the Pollard methods we start a random walk at $\mathcal{E}_0$ of length $t=O(\#\mathrm{Pic}(\mathcal{O})^{1/2})=O(q^{n/4})$. Here ℓ, $x=j(\mathcal{E}_{i+1})$ and hence the prime ideal P are chosen in a way that depends deterministically on $j(\mathcal{E}_i)$ and gives a pseudo random distribution close to uniform. Then we proceed analogously with a random walk starting at $\mathcal{E}'_0$. After an expected t steps we find s such that $j(\mathcal{E}_t)=j(\mathcal{E}'_s)$. Since $\#\mathcal{E}(K)=\#\mathcal{E}'(K)$ the curves $\mathcal{E}_t$ and $\mathcal{E}'_s$ must be isomorphic, so $I=I_t/I'_s$ corresponds to an isogeny between $\mathcal{E}_0$ and $\mathcal{E}'_0$, where I_i and I'_i are the ideals describing the random walks as above. Applying the index calculus trick for the reduction of random walks to I and combining this with the isogenies from the precomputation (and their duals) finally yields a short chain of isogenies $\mathcal{E}\to\mathcal{E}'$.

In many cases $\mathbb{Z}[\pi]=\mathcal{O}_{\max}$ holds so that the complications with intermediate orders in Isogeny Strategy 1 and Isogeny Strategy 2 do not occur.

Theorem 27. *Let $\mathcal{E}$ and $\mathcal{E}'$ be two ordinary isogenous elliptic curves such that $\#\mathcal{E}(K)=\#\mathcal{E}'(K)=q^n+1-t$, and let l be the largest prime or one with l^2 dividing $(4q^n-t^2)$. Under the GRH and further reasonable assumptions there is a probabilistic algorithm which computes $O(n\log(q))$ isogenies $\phi_i:\mathcal{E}_i\to\mathcal{E}_{i+1}$ of degree $O(\max\{(n\log(q))^2,l\})$ such that $\phi=\prod_i\phi_i$ is an isogeny between $\mathcal{E}$ and $\mathcal{E}'$. The expected running time is $O(\max\{q^{n/4+\varepsilon},l^{3+\varepsilon}\})$.*

The theorem follows from [14], [17] along the lines explained above. The algorithm involves some not rigorously proven steps from index calculus in imaginary quadratic orders which accounts for the GRH and further "reasonable" assumptions. In most cases l will be fairly small so that the running time of the algorithm is essentially $O(q^{n/4+\varepsilon})$. A worse running time can only occur when l is large since potentially some isogenies ϕ_i of degree l could be required. If $\mathrm{End}(\mathcal{E})$ and $\mathrm{End}(\mathcal{E}')$ are equal then using isogenies of degree l can be circumvent, but if the mutual index contains a large prime l, isogenies of degree l cannot be avoided. The algorithm is particularly efficient if $4q^n-t^2$ is small or if $\mathcal{O}_{\max}$ has small class number $\#\mathrm{Pic}(\mathcal{O}_{\max})$ and smooth index $(\mathcal{O}_{\max}:\mathbb{Z}[\pi])$.

If $\mathcal{E}$ is our target curve and $\mathcal{E}'\in S_{m_1(t),m_2(t)}$ is isogenous to $\mathcal{E}$ we can hence compute the isogeny ϕ between $\mathcal{E}$ and $\mathcal{E}'$ in (much) less time than the Pollard methods require for solving the DLP on $\mathcal{E}$, assuming that $4q^n-t^2$ is only divisible by squares of primes $l=O(q^{n/6-\varepsilon})$ or that $\mathrm{End}(\mathcal{E})=\mathrm{End}(\mathcal{E}')$. Then ϕ is given in the product form $\phi=\prod_i\phi_i$ and images $\phi(P)$ are computed in time about $O(\max\{(n\log(q))^7,(n\log(q))l^3\})$. Furthermore, also due to the degree bounds for the ϕ_i, the order of the kernel of ϕ cannot be divisible by the large prime factor of $\#\mathcal{E}(K)$ and hence the DLP is preserved under ϕ.

3.4. **Implications for n Odd Prime.** We now combine the previous observations with the results of Sections 2.3–2.5 and Table 1 for n an odd prime. Since the 2-power Frobenius has order nr on K the cardinalities of the representative sets S'_{h_i,h_i}, S'_{t-1,h_i} and $S'_{t-1,(t-1)h_i}$ are at least $1/(nr)$ times the cardinalities of the sets S_{h_i,h_i}, S_{t-1,h_i} and $S_{t-1,(t-1)h_i}$. If we take N pairwise distinct elliptic curves $\mathcal{E}_i$ from these representative sets with $N \lll q^{n/2}$ we expect by Lemma 23 and the discussion thereafter that a randomly and uniformly chosen elliptic curve $\mathcal{E}$ will be isogenous to one of the $\mathcal{E}_i$ with probability at least $\min\{1, N/(2q^{n/2})\}$ or $\min\{1, N/q^{n/2}\}$ if the considered elliptic curves have $a = 0$.

Following Isogeny Strategy 1 we need to actually compute the $\mathcal{E}_i$. Some details on how this can be achieved are given in the appendix of [17]. For each curve $\mathcal{E}_i$ we check $\#\mathcal{E}(K) \cdot P = \mathcal{O}$ for some random points $P \in \mathcal{E}_i(K)$. If the check fails, $\mathcal{E}_i$ is not isogenous to $\mathcal{E}$. Otherwise it is quite likely that it is and we check $\#\mathcal{E}_i(K) = \#\mathcal{E}(K)$ using fast point counting techniques. If we find $\mathcal{E}_i$ such that $\#\mathcal{E}_i(K) = \#\mathcal{E}(K)$ we are left to apply the algorithm from Theorem 27. This strategy requires a time linear in N, plus a time of about $O(q^{n/4})$ for the isogeny computation.

Following Isogeny Strategy 2 we need to sample random and uniformly distributed elliptic curves $\mathcal{E}'$ from the isogeny class of $\mathcal{E}$ as described in Section 3.3. We expect to compute approximately $q^n/\#S_{h_i,h_i}$, $2q^n/\#S_{t-1,h_i}$ and $2q^n/\#S_{t-1,(t-1)h_i}$ curves $\mathcal{E}'$ and isogenies $\mathcal{E} \to \mathcal{E}'$ until $\mathcal{E}'$ is isomorphic to one of the curves in S_{h_i,h_i}, S_{t-1,h_i} and $S_{t-1,(t-1)h_i}$ respectively. Table 2 contains a summary.

m_γ	m_β	$\Pr(\mathcal{E} \sim \mathcal{E}' \in S_{m_\gamma,m_\beta})$	Strat 1	Strat 2
h_i	h_i	$\min\{1, sq^{2d-1-n/2}/(2nr)\}$	$sq^{2d-1}/(2nr)$	$2q^{n-2d+1}/s$
$t-1$	h_i	$\min\{1, sq^{d-n/2}/(nr)\}$	$2sq^d/(nr)$	q^{n-d}/s
$t-1$	$(t-1)h_i$	$\min\{1, s(q-1)q^{d-n/2}/(nr)\}$	$2sq^{d+1}/(nr)$	q^{n-d-1}/s

TABLE 2. Expected probabilities that a random $\mathcal{E}$ is isogenous to a curve $\mathcal{E}'$ in S_{m_γ,m_β} and runtimes for Isogeny Strategy 1 (excluding the $O(q^{n/4})$ contribution) and Isogeny Strategy 2, for n odd prime

Example 28. Consider $n = 7$. By Example 20 a proportion of about q^{-2} of all elliptic curves over $\mathbb{F}_{q^7}$ with $\alpha = 0$ leads to an efficiently computable, not necessarily hyperelliptic C^0 of genus 7. Using Isogeny Strategy 2 and the first row of Table 2 we thus expect that sampling of the order of q^2 many random elliptic curves from the isogeny class of the target curve $\mathcal{E}$ yields such a C^0.

Example 29. Consider $n = 31$. The factorisation of $t^{31} - 1$ modulo 2 consists of $t - 1$ and $s = 6$ irreducible polynomials $h_i(t)$ of degree $d = 5$, two of which are of the trinomial form of Lemma 17. Using Table 1 there are hence about $3q^9$, $12q^5$ and $12q^6$ elliptic curves which lead to non-hyperelliptic and hyperelliptic curves C^0 of genus 31, 31 and 32 respectively. Using Table 2 the probability that a random elliptic curve lies in the isogeny class of one of these curves is $3q^{-13/2}/(31r)$, $6q^{-21/2}/(31r)$ and

$6q^{-19/2}/(31r)$ respectively. Since the above cardinalities are much smaller than $q^{31/2}$ Isogeny Strategy 1 is more efficient and requires a runtime of $3q^9/(31r)$, $12q^5/(31r)$ and $12q^6/(31r)$ respectively, plus $O(q^{31/4})$ for the (possible) isogeny computation.

4. Summary of Practical Implications

We now describe practical implications of the techniques of the previous sections for some values of n and fields of cryptographical sizes. We say that the GHS attack leads to a security reduction of a special family of elliptic curves or general elliptic curves if it is more efficient than the appropriate Pollard methods for these curves. As a rule of the thumb the effectiveness of the GHS attack depends chiefly on n, q and the "specialness" of the considered elliptic curves (namely the genus of the resulting curve). With increasing n the effectiveness drops, and with increasing q or increasing "specialness" the effectiveness increases. This means for example that for sufficiently large n the set of elliptic curves for which the GHS attack is effective is in general negligibly small. Also by Theorem 8 and the discussion thereafter there is always a (significant) security reduction due to the GHS attack for $n \geq 4$ and partly for $n \geq 3$ if the field size is large enough. The general method of Theorem 8 may however not readily apply to fields of cryptographical size.

Practical implications for elliptic curves in characteristic two have been investigated in [5], [17], [23], [26], [31], [33], [34], [40].

For $n = 1$ or $n = 2$ there are no elliptic curves over $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$ respectively for which the GHS attack would lead to a security reduction. The case $n = 1$ is clear as $E = C^0$ and there is nothing new to consider. The case $n = 2$ yields C^0 of genus at least two. Since the Pollard methods on E are more efficient than index calculus on curves of genus at least two there is no security reduction due to the GHS attack [5].

The case $n = 3$ has not been discussed in the literature. From the results for $n = 4$ it appears however reasonable to expect no or only a minor security reduction due to the GHS attack for any elliptic curve over $\mathbb{F}_{q^3}$.

The cases $n = 4$ and $n = 5$ are discussed in detail in [40] considering low genus index calculus methods and in [31], [34] considering high genus index calculus methods. The conclusion for $n = 4$ is that there is (only) a minor security reduction due to the GHS attack, applicable to any elliptic curve over $\mathbb{F}_{q^4}$, and a slightly more significant security reduction for a proportion of around $1/q$ of these elliptic curves. The case $n = 5$ is particularly interesting since there is an IETF standard [25] using the fields $\mathbb{F}_{155}$ and $\mathbb{F}_{185}$. In [40] it is concluded that an arbitrary elliptic curve over $\mathbb{F}_{155}$ is subject to only a minor security reduction. In [31] it is argued that an arbitrary elliptic curve over $\mathbb{F}_{185}$ is subject to a security reduction by a factor of 2^{16}, resulting in a security of 2^{76} instead of 2^{92}. In [34] timing estimates are given for further fields, the security reduction becomes larger as the field size grows. For $\mathbb{F}_{q^{600}}$ the factor is for example already 2^{69}, applicable to every elliptic curve over that field.

The case $n = 6$ is partly discussed in [34], focusing on the field $\mathbb{F}_{2^{210}}$. The conclusion is that about one quarter of all elliptic curves over $\mathbb{F}_{2^{210}}$, namely those with $\mathrm{Tr}_{\mathbb{F}_{2^{210}}}(a) = \mathrm{Tr}_{\mathbb{F}_{2^{210}}}(b) = 0$ or equivalently $\#E(\mathbb{F}_{2^{210}}) \equiv 0 \bmod 8$, are subject to a security reduction by a factor of 2^{20}. The attack uses isogenies and maps the DLP to hyperelliptic curves of genus 15 or 16. Alternatively we can make use of the more

general Example 16, which yields smaller genera up to 14. Note that the resulting function field C^0 is in general not hyperelliptic, so solving the DLP for C^0 will be more expensive. Precise experiments have not been carried out, but we can still expect a significant security reduction for essentially all elliptic curves over $\mathbb{F}_{q^6}$.

The case $n = 7$ has been considered in [17] using the GHS reduction with $\gamma = 1$ and it was concluded that there should be a significant security reduction for every elliptic curve over $\mathbb{F}_{q^7}$ if only C^0 could be found efficiently enough. In [34] the field $\mathbb{F}_{2^{161}}$ is briefly discussed, for which the GHS attack would yield a feasible HCDLP for genus 7 or 8 over $\mathbb{F}_{2^{23}}$. By Example 28 we expect that sampling of the order of q^2 many random elliptic curves from the isogeny class of a target elliptic curve $\mathcal{E}_{a,b}$ over $\mathbb{F}_{q^7}$ with $a = 0$ yields a not necessarily hyperelliptic C^0 over $\mathbb{F}_q$ of genus 7. Comparing against the cost of $q^{7/2}$ for the Pollard methods finding C^0 thus takes negligible time. We can hence expect a particularly significant security reduction of up to a factor of $q^{3/2}$ for all elliptic curves over $\mathbb{F}_{q^7}$. A precise analysis and whether the DLP for elliptic curves over $\mathbb{F}_{2^{161}}$ is feasible using these techniques has not been carried out yet.

The case $n = 8$ has been discussed in [31]. There is a class of approximately q^5 elliptic curves $\mathcal{E}_{a,b}$ with $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$ and $m_b(t) = (t-1)^5$ whose security is significantly reduced by the GHS attack. In [31] it is argued that using Isogeny Strategy 1 would not present a feasible method of finding such a susceptible elliptic curve isogenous to a given arbitrary target curve. Applying Isogeny Strategy 2 however would seem to require sampling approximately q^3 random curves in the isogeny class of the target curve before a susceptible curve is found. As a result the security of any elliptic curve with $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$ and $n = 8$ could be reduced by a factor of approximately q. The case $n = 8$ is of particular interest since the ANSI X.962 standard [47] lists in Appendix H.4 specific elliptic curves over fields of characteristic two and extension degrees 16ℓ where $\ell \in \{11, 13, 17, 19, 23\}$. We remark that the curves are defined over $\mathbb{F}_{16}$.

The case $n = 15$ is illustrated in [31]. A striking example is $\mathbb{F}_{2^{600}}$ where the GHS attack applies to 2^{202} curves and requires about 2^{79} steps, which is much less than the 2^{299} steps for the Pollard methods.

The case $n = 31$ has been discussed in [23],[26],[31]. The existing methods do not yield a security reduction for random elliptic curves over $\mathbb{F}_{q^{31}}$, but do yield a very significant security reduction for special curves. Some of these special curves are given as challenge curves in [31]. For example, over $\mathbb{F}_{2^{155}}$ and $\mathbb{F}_{2^{186}}$ the Pollard methods have a runtime of about 2^{77} compared to 2^{37} and 2^{92} compared to 2^{42} for the GHS attack and a hyperelliptic C^0 respectively. Example 29 shows some attack possibilities. For $\mathbb{F}_{2^{155}}$ we expect to transfer the DLP on an elliptic curve with $a = 0$ to a non-hyperelliptic curve of genus 31 with approximate probability $3q^{-13/2}/(31r) \approx 2^{-37}$ and a runtime of about $3q^9/(31r) + q^{31/4} \approx 2^{40}$.

Further extension degrees and field sizes are investigated in [31]. The above discussion shows that elliptic curves over composite extension fields $\mathbb{F}_{q^n}$ with $n \in \{5, 6, 7, 8\}$ (are likely to) offer less security due to the GHS attack than expected. On the other hand, if n is a prime $\neq 127$ in the interval 100 to 600 then the GHS attack is infeasible

and does not lead to a security reduction for any elliptic curve over $\mathbb{F}_{q^n}$, see [33] and Theorem 10.

5. Further Topics

In this section we briefly discuss the Weil descent methodology and generalisations of the GHS attack in odd characteristic and for more general curves. We also include some further applications.

The basic ideas of Section 1 and Section 2.1 can be generalised to odd characteristic and to more general curves quite verbatim and are made explicit by using Kummer and Artin-Schreier constructions. Some indications for the Artin-Schreier case can already be found in Section 2.6.

5.1. **Kummer Constructions.** The main reference here is [8] which considers the case of elliptic and hyperelliptic curves in odd characteristic with a particular emphasis on odd prime degree extension fields. Since the 2-nd roots of unity $1, -1$ are always contained in the base field, an elliptic or hyperelliptic curve $\mathcal{H} : Y^2 = f(X)$ defines a Kummer extension $H/K(X)$ of degree two where $H = K(\mathcal{H})$ is an elliptic or hyperelliptic function field. The following statements are given and proved in [8].

Theorem 30. *Let K/k be an extension of finite fields of odd characteristic and odd degree $n = \prod_p p^{n_p}$. Let H be an elliptic or hyperelliptic function field of genus g and regular over K suitable for cryptographic applications. Choose some element $x \in H$ such that $H/K(x)$ is of degree two, given by an equation of the form $y^2 = cf(x)$ where f is monic and $c \in K^\times$.*

Then, via the GHS attack, one obtains a function field C^0 regular over k or its unique quadratic extension, an extension C/H of degree 2^{m-1} for some $m \leq n$ with $C = KC^0$, and a homomorphism from $\mathrm{Pic}^0_K(H)$ to $\mathrm{Pic}^0_k(C^0)$ with the following properties:

- *(i) If $c = 1$, C^0/k is regular.*
- *(ii) $g_{C^0} \leq 2^{n-1}((g+1)n - 2) + 1$.*
- *(iii) If there exists some field L with $k \subseteq L \subseteq K$ such that $H/L(x)$ is Galois, the large subgroup of prime order is not preserved under the homomorphism.*
- *(iv) If there does not exist such an L the kernel of the homomorphism contains only elements of 2-power order and*

$$g_{C^0} \;\geq\; 2^{\lceil (\sum_p p^{n_p})/(2g+2) \rceil - 2} \Big(\sum_p p^{n_p} - 4 \Big) + 1.$$

- *(v) If n is prime then additionally*

$$g_{C^0} \;\geq\; 2^{\phi_2(n)-2}(n-4) + 1,$$

  where $\phi_2(n)$ denotes the multiplicative order of 2 modulo n.
- *(vi) If $[\bar{K}C : \bar{K}(x)] \geq 2^4$, then $C/K(x)$ does not contain an intermediate field which is rational and of index 2 in C.*

Let σ be the extension of the Frobenius automorphism of K/k to $K(x)$ via $\sigma(x) = x$. Let U be the (multiplicative) $\mathbb{F}_2$-subspace of $K(x)^\times/K(x)^{\times 2}$ generated by the conjugates $\sigma^i(f)$, and $\bar{U}$ the $\mathbb{F}_2$-subspace of $\bar{K}(x)^\times/\bar{K}(x)^{\times 2}$ generated by U. Then

$C = KC^0$ is obtained by adjoining all square roots of class representatives of U to $K(x)$. Furthermore, $[C : K(x)] = 2^m$ and $[\bar{K}C : \bar{K}(x)] = 2^{\bar{m}}$ where $m = \dim U$ and $\bar{m} = \dim \bar{U}$. Also, $\bar{m} = m$ if and only if C/K is regular, and $\bar{m} = m - 1$ otherwise.

For $n = 5$ and $n = 7$ there are families of elliptic curves over any extension field of degree n for which g_{C^0} assumes the lower bounds 5 and 7 respectively given by (v). There is for example an elliptic curve over $\mathbb{F}_{10000019^7}$ whose group order is four times a prime and which yields $g_{C^0} = 7$. Moreover, a defining polynomial for C^0 can be given in these cases. For $n = 11, 13, 17, 19, 23$ and elliptic curves we have $g_{C^0} \geq 1793, 9217, 833, 983041, 9729$. The attack is not feasible for prime $n \geq 11$.

A further study of Kummer techniques is carried out in [43] and leads to examples of attackable (or reduced security) classes of elliptic and hyperelliptic curves for $n = 2$ and $n = 3$. We summarise the examples of [8, 43, 11] in Table 5.1. A nice table of smallest possible genera depending on small values of n and $g = g_H$ is given in [11]. We remark that [43] also deals with a class of superelliptic curves.

n	H	g	C^0	g_{C^0}
2	$Y^2 = (X-a)h(X)$	$\lfloor \deg(h)/2 \rfloor$	hyperell.	$2g$
3	$Y^2 = (X-a)h(X)$	$\lfloor \deg(h)/2 \rfloor$	hyperell.	$4g+1$
3	$Y^2 = (X-a)(X-\sigma(a))h(X)$	$\lfloor (\deg(h)-1)/2 \rfloor$	hyperell.	$4g-1$
3	$Y^2 = \prod_{i=1}^{g+1}(X-a_i)(X-\sigma(a_i))$	g	–	$3g$
5	$Y^2 = \prod_{i\in\{0,1,2,3\}}(X-\sigma^i(a))$	1	–	5
7	$Y^2 = \prod_{i\in\{0,1,2,4\}}(X-\sigma^i(a))$	1	–	7

TABLE 3. Examples of [8, 43, 11] for $a, a_i \in K\backslash k$ and $h \in k[X]$ (no multiple factors allowed on the right hand sides of $=$).

5.2. **Artin-Schreier Constructions.** An elliptic or hyperelliptic curve $\mathcal{H} : Y^2 + h(X)Y = f(X)$ in characteristic two defines (after a transformation similar to the one from (1) to (2)) an Artin-Schreier extension $H/K(X)$ of degree two where $H = K(\mathcal{H})$ is an elliptic or hyperelliptic function field.

A generalisation of the Artin-Schreier construction for elliptic curves as in [20] to hyperelliptic curves in characteristic two was first considered in [16]. There conditions for the hyperelliptic curves are derived such that the construction of [20] carries through in an analogous way. Some examples of the resulting curves are

$$Y^2 + XY = X^{2g+1} + \cdots + c_3X^3 + c_2X^2 + c_1X + \theta$$
$$Y^2 + XY = X^{2g+1} + \cdots + c_3X^3 + c_2X^2 + \theta X + c_1$$
$$Y^2 + XY = X^{2g+1} + \cdots + \theta X^3 + c_3X^2 + c_2X + c_1$$
$$Y^2 + XY = X^{2g+1} + \cdots + \theta' X^3 + c_1X^2 + \theta X + \theta^2$$

where $c_i \in k$, $\theta, \theta' \in K$ and θ, θ' have n distinct conjugates. A bound $g_{C^0} \leq g2^{m-1}$ for the genus of the corresponding C^0 holds, where m is defined similarly as in Section 2.6.

Another family of curves is given in [42], of the form $Y^2 + h(X)Y = f(X)h(X) + (\alpha X + \beta)h(X)^2$ with $f, h \in k[X]$, $\alpha, \beta \in K$ and some further conditions. Here the genus g_{C^0} is proven to be equal to $g2^{m-1} - 1$ or $g2^{m-1}$.

A discussion of general Artin-Schreier extensions is carried out in [23]. The main consequences for elliptic curves are presented 3. One result for general Artin-Schreier extensions is that g_{C^0} grows exponentially in m whence the attack can only apply to very special families of curves or if n is small. A similar statement holds true for Kummer extensions.

We remark that [42] and [23] also include Artin-Schreier extensions in characteristic $p > 2$.

5.3. **Kernel of Norm-Conorm Maps and Genera.** We consider a generalisation of the situation in Section 1.2. Let E be a function field of transcendence degree one over the finite exact constant field K, C/E a finite extension and U a finite subgroup of $\mathrm{Aut}(C)$. The fixed field of U in C is denoted by C^0. As in Section 1.2, we obtain a homomorphism of the divisor class groups $\phi : \mathrm{Pic}^0_K(E) \to \mathrm{Pic}^0_k(C^0)$ by $\mathrm{N}_{C/C^0} \circ \mathrm{Con}_{C/E}$, the conorm from E to C followed by the norm from C to C^0. This situation is quite general, for example we do not require U to be abelian.

Theorem 31. *The kernel of ϕ satisfies*

(*i*) $\ker(\mathrm{N}_{E/E^V}) \subseteq \ker(\phi)$, *where V is any subgroup of U with $VE \subseteq E$, so V restricts to a subgroup of $\mathrm{Aut}(E)$, and E^V is the fixed field of V in E.*

(*ii*) *If the intersection $E \cap \sigma E$ is a function field and E, σE are linearly disjoint over $E \cap \sigma E$ for every $\sigma \in U$ then*

$$[C : E] \cdot \ker \phi \ \subseteq \sum_{\sigma \in U \setminus \{1\}} \mathrm{Con}_{E/E\cap\sigma E}\big(\mathrm{Pic}^0_K(E \cap \sigma E)\big).$$

For example, E and σE are linear disjoint over $E \cap \sigma E$ if at least one is Galois over $E \cap \sigma E$.

The theorem applies in particular to the Kummer and Artin-Schreier constructions discussed so far. Condition (*i*) basically means that for subfield curves, $\ker(\phi)$ contains the large prime factor subgroup of $\mathrm{Pic}^0_K(E)$. In condition (*ii*) we have that the $\mathrm{Pic}^0_K(E \cap \sigma E)$ do not contain the large prime factor subgroup since $E \cap \sigma E = K(x)$, and $[C : E]$ is also not divisible by the large prime factor. As a result, $\ker(\phi)$ does not contain the large prime factor subgroup either.

A proof of a more general version of Theorem 31 is given in [23]. The case of hyperelliptic curves has been independently dealt with in [8].

The genus of C^0 can be computed in a number of ways. A general way, which also determines the L-polynomial of C^0, is as follows. Let G be a finite subgroup of $\mathrm{Aut}(C)$ and let H and U be subgroups of G such that H is normal in G, $H \cap U = \{1\}$ and $G = HU$. The subgroup U operates on H by conjugation. Assume further that H is elementary abelian of prime exponent l and let $\{ H_\nu \mid \nu \in I \}$ be a system of representatives under the operation of U on the subgroups of H of index l for some index set I. Let U_ν be the largest subgroup of U which leaves H_ν invariant. If A is any subgroup of G then the fixed field of A in C is denoted by C^A and the degree of the exact constant field of C^A over that of C^G by d_{C^A}.

Theorem 32. *Under the above assumptions the L-polynomials satisfy*

$$L_{C^U}(t^{d_{C^U}}) \,/\, L_{C^G}(t) \;=\; \prod_{\nu\in I} L_{C^{H_\nu U_\nu}}(t^{d_{C^{H_\nu U_\nu}}}) \,/\, L_{C^{HU_\nu}}(t^{d_{C^{HU_\nu}}}).$$

Corollary 33. *The genera satisfy the equation*

$$d_{C^U}\, g_{C^U} - g_{C^G} \;=\; \sum_{\nu\in I} \big(d_{C^{H_\nu U_\nu}}\, g_{C^{H_\nu U_\nu}} - d_{C^{HU_\nu}}\, g_{C^{HU_\nu}}\big).$$

Theorem 32 and Corollary 33 are proved in [23]. They can be applied to the Artin-Schreier and prime degree Kummer constructions quite straightforwardly by analysing the defining groups Δ (and U as in Section 5.1).

5.4. **Construction of Models.** The construction of explicit defining equations for C^0 obtained by the Kummer or Artin-Schreier constructions and the computation of images under ϕ by means of computer algebra systems is quite technical but does not pose principal algorithmic problems. We refer to [20, 23, 16, 8, 43, 42] for details.

5.5. **Trap Door Systems.** The GHS attack with isogenies from Section 3 can also be used constructively for a trap door system [41]. The basic idea is as follows. A user creates a secret elliptic curve $\mathcal{E}_s$ which is susceptible to the GHS attack. The user then computes a public elliptic curve $\mathcal{E}_p$ by means of a secret, sufficiently long and random isogeny chain starting at $\mathcal{E}_s$. The curve $\mathcal{E}_s$ and the isogeny chain are submitted to a trusted authority for key escrow, while $\mathcal{E}_p$ is used as usual in elliptic curve cryptosystems. The parameters are chosen such that the Pollard methods are the most efficient way to solve the DLP on $\mathcal{E}_p$, while solving the DLP on $\mathcal{E}_s$ is much easier but still sufficiently hard. The trusted authority thus has to invest considerable computing power to decrypt which makes widespread wire tapping infeasible. For further details and parameter choices see [41].

5.6. **Other Approaches.** Covering techniques can also be applied when the target function field E comes from a true subfield curve. The methods described so far do not readily apply because $\sigma E = E$, in view of Theorem 31. One strategy to overcome this problem is to perform a suitable change of variable such that there are n different conjugate fields $\sigma^i(E)$, so basically one considers a different σ. Accordingly, another strategy is to twist σ by an automorphism τ of order n such that there are n different conjugate fields $(\sigma\tau)^i(E)$. If E_0 is the target field defined over k, such that $E = E_0K$, then this strategy leads to the construction of suitable extensions C_0/E_0 and $\tau_0 \in \mathrm{Aut}(C_0)$ with $\tau_0(E_0) \neq E_0$, and departs from the Kummer and Artin-Schreier paradigms. We refer to [7, 11] for details. As a consequence, with respect to an extension K/k of degree 3 and $\mathrm{char}(k) \neq 2, 3$, the DLP (in the trace zero group) of a genus 2 curve can always be transformed into a DLP of a genus 6 curve defined over k. For a non-negligible percentage even genus 5 is possible which leads to a more efficient attack via index calculus than by the Pollard methods.

A further approach described in [11] uses special classes of hyperelliptic curves defined over k which admit maps to elliptic curves defined over K. The genus of these hyperelliptic curves is equal to $n = [K : k]$, so these attacks would be very

efficient. However, the maps between the curves are not (yet) known explicitly and upper bounds for their degrees are very large.

We close with two more remarks. In [4] the GHS construction is used to construct elliptic curves over $\bar{\mathbb{F}}_2(x)$ of high rank with constant j-invariant. In [36] a covering technique is used to construct genus 2 curves defined over k with Jacobian isogenous to the Weil restriction of a large class of elliptic curves defined over K with respect to a quadratic extension K/k of finite fields in odd characteristic. This allows for SEA point counting while avoiding patents in ECC (see also [24, 15]).

References

[1] I.F. Blake, G. Seroussi, and N.P. Smart. *Elliptic Curves in Cryptography*. Cambridge University Press, 1999.

[2] I.F. Blake, G. Seroussi, and N.P. Smart. *Advances in Elliptic Curve Cryptography*. Cambridge University Press, 2004. to appear.

[3] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symbolic Comp.*, 24, 3/4:235–265, 1997.

[4] I. Bouw, C. Diem, and J. Scholten. Ordinary elliptic curves of high rank over $\bar{\mathbb{F}}_p(x)$ with constant j-invariant. Submitted, 2003.

[5] M. Ciet, J.-J. Quisquater, and F. Sica. A secure family of composite finite fields suitable for fast implementation of elliptic curve cryptography. In C. Pandu Rangan and C. Ding, editors, *Progress in Cryptology – INDOCRYPT 2001*, volume 2247 of *LNCS*, pages 108–116. Springer-Verlag, 2001.

[6] J.-M. Couveignes. Algebraic groups and discrete logarithms. In *Public Key Cryptography and Computational Number Theory*, pages 17–27, Warsaw (2000), 2001. Walter de Gruyter.

[7] C. Diem. *A study on theoretical and practical aspects of Weil-restrictions of varieties*. PhD thesis, Universtität-Gesamthochschule Essen, 2001.

[8] C. Diem. The GHS-attack in odd characteristic. *J. Ramanujan Math. Soc.*, 18(1):1–32, 2002.

[9] C. Diem. Private communication, 2003.

[10] C. Diem and N. Naumann. On the structure of Weil restrictions of abelian varieties. *J. Ramanujan Math. Soc.*, 18, 2003.

[11] C. Diem and J. Scholten. Cover attacks – a report for the arehcc project. Submitted, 2003.

[12] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arith.*, 102:83–103, 2002.

[13] G. Frey. How to disguise an elliptic curve. Talk at ECC' 98, Waterloo, 1998.

[14] S. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999.

[15] S. Galbraith. Limitations of constructive Weil descent. In K. Alster et al., editor, *Public-Key Cryptography and Computational Number Theory*, pages 59–70, Warsaw, 2001. Walter de Gruyter.

[16] S. Galbraith. Weil descent of Jacobians. In D. Augot and C. Carlet, editors, *WCC2001 International workshop on coding and cryptography*, Electron. Notes Discrete Math. 6, Paris, 2001. Elsevier, Amsterdam.

[17] S. Galbraith, F. Hess, and N.P. Smart. Extending the GHS Weil descent attack. In L. Knudsen, editor, *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 29–44. Springer-Verlag, 2002.

[18] S. Galbraith and J. McKee. The probability that the number of points on an elliptic curve over a finite field is prime. *J. London Math. Soc.*, 62:671–684, 2000.

[19] S. Galbraith and N.P. Smart. A cryptographic application of Weil descent. In M. Walker, editor, *Cryptography and Coding*, volume 1746 of *LNCS*, pages 191–200. Springer-Verlag, 1999.

[20] P. Gaudry, F. Hess, and N.P. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Crypt.*, 15:19–46, 2002.

[21] F. Hess. Computing relations in divisor class groups of algebraic curves over finite fields. Submitted, 2003.

[22] F. Hess. The GHS attack revisited. In E. Biham, editor, *Advances in Cryptology – EUROCRYPT 2003*, volume 2656 of *LNCS*, pages 374–387. Springer-Verlag, 2003.

[23] F. Hess. Generalising the GHS attack. *LMS Journal of Computation and Mathematics*, To appear.

[24] F. Hess, N. P. Smart, and G. Seroussi. Two topics in hyperelliptic cryptography. In S. Vaudenay and Amr M. Youssef, editors, *Proceedings of SAC 2001*, volume 2259 of *LNCS*, pages 181–189, Toronto, Canada, 2001. Springer-Verlag.

[25] IETF. *The Oakley Key Determination Protocol*, 1998.

[26] M. Jacobson, A. Menezes, and A. Stein. Solving elliptic curve discrete logarithm problems using Weil descent. *J. Ramanujan Math. Soc.*, 16:231–260, 2001.
[27] Kant group. *Kash*. `http://www.math.tu-berlin.de/~kant`, 2003.
[28] D. R. Kohel. *Endomorphism rings of elliptic curves over finite fields*. Phd thesis, University of California, Berkeley, 1996.
[29] S. Lang. *Algebra*. Addison-Wesley, 3rd edition, 1993.
[30] Magma Comp. algebra group. *Magma*. Available from `http://www.maths.usyd.edu.au:8000/u/magma/`, 2003.
[31] 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*, 5:127–174, 2002.
[32] A. Menezes. *Elliptic curve public key cryptosystems*. Kluwer Academic Publishers, Boston, 1993.
[33] A. Menezes and M. Qu. Analysis of the Weil descent attack of Gaudry, Hess and Smart. In D. Naccache, editor, *Topics in Cryptology – CT-RSA 2001*, volume 2020 of *LNCS*, pages 308–318. Springer-Verlag, 2001.
[34] A. Menezes, E. Teske, and A. Weng. Weak fields for ECC. In T. Okamoto, editor, *Topics in Cryptology – CT-RSA 2004*, LNCS. Springer-Verlag, To appear.
[35] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag, 1999.
[36] J. Scholten. Weil restriction of an elliptic curve over a quadratic extension. Submitted, 2004.
[37] R. Schoof. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A*, 46:183–211, 1987.
[38] R. Schoof. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux*, 1995.
[39] J.H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *GTM*. Springer-Verlag, 1986.
[40] N.P. Smart. How secure are elliptic curves over composite extension fields? In B. Pfitzmann, editor, *Advances in Cryptology – EUROCRYPT 2001*, volume 2045 of *LNCS*, pages 30–39. Springer-Verlag, 2001.
[41] E. Teske. An elliptic curve trapdoor system. To appear in J. Crypto., 2003.
[42] N. Thériault. Weil descent attack for artin-schreier curves. Submitted.
[43] N. Thériault. Weil descent attack for kummer extensions. Submitted.
[44] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In C.S. Laih, editor, *Advances in Cryptology – ASIACRYPT 2003*, volume 2894 of *LNCS*, pages 75–92. Springer-Verlag, 2003.
[45] E. Waterhouse. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup.*, 2:521–560, 1969.
[46] A. Weil. The field of definition of a variety. *Am. J. Math.*, 78:509–524, 1956.
[47] ANSI X9.62. *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*. American National Standards Institute, 1999.

Technische Universität Berlin, Fakultät II - Institut für Mathematik - MA8-1, Strasse des 17. Juni 136, 10623 Berlin, Germany