Analysis of the GHS Weil Descent Attack on the ECDLP over Characteristic Two Finite Fields of Composite Degree

Markus Maurer, Alfred Menezes and Edlyn Teske
Dept. of Combinatorics and Optimization, University of Waterloo
ajmeneze@uwaterloo.ca, eteske@uwaterloo.ca

October 12, 2001

Abstract

In this paper, we analyze the Gaudry-Hess-Smart (GHS) Weil descent attack on the elliptic curve discrete logarithm problem (ECDLP) for elliptic curves defined over characteristic two finite fields of composite extension degree. For each such field $\mathbb{F}_{2^N}$, $N \in [100, 600]$, we identify elliptic curve parameters such that (i) there should exist a cryptographically interesting elliptic curve E over $\mathbb{F}_{2^N}$ with these parameters; and (ii) the GHS attack is more efficient for solving the ECDLP in $E(\mathbb{F}_{2^N})$ than for solving the ECDLP on any other cryptographically interesting elliptic curve over $\mathbb{F}_{2^N}$. We examine the feasibility of the GHS attack on the specific elliptic curves over $\mathbb{F}_{2^{176}}$, $\mathbb{F}_{2^{208}}$, $\mathbb{F}_{2^{272}}$, $\mathbb{F}_{2^{304}}$, and $\mathbb{F}_{2^{368}}$ that are provided as examples in the ANSI X9.62 standard for the elliptic curve signature scheme ECDSA. Finally, we provide several concrete instances of the ECDLP over $\mathbb{F}_{2^N}$, N composite, of increasing difficulty which resist all previously known attacks but which are within reach of the GHS attack.

Contents

1 Introduction

Let E be an elliptic curve defined over a finite field $K = \mathbb{F}_{2^N}$. The elliptic curve discrete logarithm problem (ECDLP) in $E(K)$ is the following: given E, $P \in E(K)$, $r = \mathrm{ord}(P)$ and $Q \in \langle P \rangle$, find the integer $\lambda \in [0, r-1]$ such that $Q = \lambda P$. We write $\lambda = \log_P Q$. The ECDLP is of interest because its apparent intractability forms the basis for the security of elliptic curve cryptographic schemes.

The elliptic curve parameters have to be carefully chosen in order to circumvent some known attacks on the ECDLP. We say that an elliptic curve E over $\mathbb{F}_{2^N}$ is *cryptographically interesting* if: (i) $\#E(\mathbb{F}_{2^N})$ is almost prime—that is, $\#E(\mathbb{F}_{2^N}) = rd$ where r is prime and $d \in \{2, 4\}$—in order to avoid the Pohlig-Hellman [29] and Pollard's rho [30, 27] attacks; and (ii) r does not divide $2^{Nj} - 1$ for each $j \in [1, J]$, where J is large enough so that it is computationally infeasible to find discrete logarithms in $\mathbb{F}_{2^{NJ}}$—in order to avoid the Weil pairing [24] and Tate pairing [11] attacks.

Frey [9, 10] first proposed using Weil descent as a means to reduce the ECDLP in elliptic curves over $\mathbb{F}_{2^N}$ to the discrete logarithm problem in an abelian variety over a proper subfield $\mathbb{F}_{2^l}$ of $\mathbb{F}_{2^N}$. Frey's method, which we refer to as the *Weil descent attack methodology*, was further elaborated by Galbraith and Smart [14]. In 2000, Gaudry, Hess and Smart (GHS) [17] showed how Frey's methodology could be used (in most cases) to reduce any instance of the ECDLP to an instance of the discrete logarithm problem in the Jacobian of a hyperelliptic curve over $\mathbb{F}_{2^l}$. Since subexponential-time algorithms for the hyperelliptic curve discrete logarithm problem (HCDLP) are known, this could have important implications to the security of elliptic curve cryptographic schemes.

The GHS attack was analyzed in [17, 26]. It was proven to fail for *all* cryptographically interesting elliptic curves over $\mathbb{F}_{2^N}$, where $N \in [160, 600]$ is prime. Namely, the hyperelliptic curves C produced either have genus too small (whence $J_C(\mathbb{F}_2)$ is too small to yield any non-trivial information about the ECDLP in $E(\mathbb{F}_{2^N})$), or have genus too large ($g \geq 2^{16} - 1$, whence the HCDLP in $J_C(\mathbb{F}_2)$ is infeasible). The purpose of this paper is to investigate the applicability of the GHS attack on the ECDLP for cryptographically interesting elliptic curves over $\mathbb{F}_{2^N}$ for composite $N \in [100, 600]$.

The remainder of this paper is organized as follows. §2 provides a brief introduction to the relevant theory of hyperelliptic curves. The GHS Weil descent attack is outlined in §3, and an overview of the best methods known for solving the ECDLP and HCDLP are given in §4. Our analysis of the applicability of the GHS attack on the ECDLP over characteristic two finite fields of composite extension degree is presented in §5. In §6, a detailed analysis is presented of the feasibility of the GHS attack on certain elliptic curves specified in the ANSI X9.62 standard. §7 lists some ECDLP "challenges" of increasing difficulty which should resist all previously known attacks but which are within reach of the GHS attack. Our conclusions are stated in §8.

2 Hyperelliptic Curves

We provide a brief overview of the theory of hyperelliptic curves that is relevant to this paper.

Hyperelliptic Curves. Let $k = \mathbb{F}_q$ denote the finite field of order q. The *algebraic closure* of $\mathbb{F}_q$ is

$\overline{k} = \bigcup_{n\geq 1} \mathbb{F}_{q^n}$. A *hyperelliptic curve C of genus g over k* is defined by a non-singular equation

$$v^2 + h(u)v = f(u), \tag{1}$$

where $h, f \in k[u]$, $\deg f = 2g+1$, and $\deg h \leq g$. Let L be an extension field of k. The set of *L-rational points* on C is $C(L) = \{(x,y) : x,y \in L,\ y^2 + h(x)y = f(x)\} \cup \{\infty\}$. The *opposite* of $P = (x,y) \in C(L)$ is $\widetilde{P} = (x, -y-h(x))$; we also define $\widetilde{\infty} = \infty$. Note that $\widetilde{P} \in C(L)$. Except for the case $g = 1$ (since a genus 1 hyperelliptic curve is precisely an elliptic curve), there is no natural group law on the set of points $C(L)$. Instead, one considers the Jacobian of C over k which is a finite group.

Jacobian of a Hyperelliptic Curve. The set D^0 of *degree zero divisors* of C is the set of formal sums $\sum_{P\in C(\overline{k})} m_P P$, where $m_P \in \mathbb{Z}$, $\sum m_P = 0$, and only a finite number of the m_P's are non-zero. D^0 is a group under the addition rule $\sum m_P P + \sum n_P P = \sum (m_P + n_P)P$. Let $\sigma : \overline{k} \to \overline{k}$ be the *Frobenius map* defined by $x \mapsto x^q$. The map σ extends to $C(\overline{k})$ by $(x,y) \mapsto (x^\sigma, y^\sigma)$ and $\infty^\sigma \mapsto \infty$, and to D^0 by $\sum m_P P \mapsto \sum m_P P^\sigma$. The set of zero divisors defined over k is $D^0_k = \{D \in D^0 : D^\sigma = D\}$. The *function field* of C over k, denoted $k(C)$, is the field of fractions of the integral domain of polynomial functions $k[u,v]/(v^2 + h(u)v - f(u))$. For $f \in k(C)$, the *divisor of f* is $\operatorname{div}(f) = \sum_{P\in C(\overline{k})} v_P(f)P$, where $v_P(f)$ denotes the multiplicity of P as a root of f. Now the set $\mathrm{Prin}_k = \{\operatorname{div}(f) : f \in k(C)\}$ is a subgroup of D^0_k. The *Jacobian* of C (over k) is the quotient group $J_C(k) = D^0_k/\mathrm{Prin}_k$.

Properties of the Jacobian. $J_C(k)$ is a finite group. A theorem of Weil's implies that

$$(\sqrt{q}-1)^{2g} \leq \#J_C(k) \leq (\sqrt{q}+1)^{2g}. \tag{2}$$

If D_1 and D_2 are in the same equivalence class of divisors in $J_C(k)$ we write $D_1 \sim D_2$. Each equivalence class has a unique divisor in *reduced form*, i.e., a divisor $\sum_{P\neq\infty} m_P P - (\sum_{P\neq\infty} m_P)\infty$ satisfying (i) $m_P \geq 0$ for all P; (ii) if $m_P \geq 1$ and $P \neq \widetilde{P}$, then $m_{\widetilde{P}} = 0$; (iii) $m_P = 0$ or 1 if $P = \widetilde{P}$; and (iv) $\sum m_P \leq g$. Such a *reduced divisor* D can be uniquely represented by a pair of polynomials $a, b \in k[u]$ where (i) $\deg b < \deg a \leq g$; (ii) a is monic; and (iii) $a | (b^2 + bh - f)$. We write $D = \operatorname{div}(a,b)$ to mean $D = \gcd(\operatorname{div}(a), \operatorname{div}(b-v))$ where the gcd of two divisors $\sum_{P\neq\infty} m_P P - (\sum_{P\neq\infty} m_P)\infty$ and $\sum_{P\neq\infty} n_P P - (\sum_{P\neq\infty} n_P)\infty$ is defined to be $\sum_{P\neq\infty} \min(m_P, n_P)P - (\sum_{P\neq\infty} \min(m_P,n_P))\infty$. The *degree* of D is $\deg a$. Cantor's algorithm [4] can be used to efficiently compute the sum of two reduced divisors, and express the sum in reduced form.

Artin's Bound. In the above, we only considered the *imaginary* form of a hyperelliptic curve, and not the *real* form for which $\deg(f) = 2g+2$ in the defining equation (1). Let C be a hyperelliptic curve (real or imaginary) of genus g over $k = \mathbb{F}_p$ with p an odd prime. Artin [3] showed that

$$\#J_C(k) = \begin{cases} \sum_{\nu=0}^{2g} \chi_\nu & \text{if } \deg f = 2g+1, \\ -\sum_{\nu=1}^{2g+1} \nu\chi_\nu & \text{if } \deg f = 2g+2. \end{cases} \tag{3}$$

Here, $\chi_\nu = \sum_{\deg F = \nu} \left[\frac{f}{F}\right]$, where the summation is over all degree-ν monic polynomials $F \in \mathbb{F}_p[u]$ coprime to f, and $\left[\frac{f}{F}\right]$ is the polynomial Legendre symbol. We trivially have that $|\chi_\nu| \leq p^\nu$, and Artin showed that $|\chi_\nu| \leq p^g$ $(0 \leq \nu \leq 2g)$ if $\deg f = 2g+1$, and $\chi_{2g+1} = -p^g$ and $|\chi_\nu| \leq 2p^g$ $(1 \leq \nu \leq 2g)$

if $\deg f = 2g+2$. These results can be extended to the case $k = \mathbb{F}_q$, where $q = p^l$ and p is prime, by replacing the Artin character by the general quadratic character. Then

$$\#J_C(k) \le \begin{cases} gq^g + \sum_{\nu=0}^{g} q^\nu & \text{if } \deg f = 2g+1, \\ ((2g+1)^2 - g(g+1))q^g + \sum_{\nu=1}^{g} \nu q^\nu & \text{if } \deg f = 2g+2. \end{cases}$$

Since over constant fields of characteristic 2 the real case is strictly more general than the imaginary case (cf. [28]), we work with

$$B_2 := ((2g+1)^2 - g(g+1))q^g + \sum_{\nu=1}^{g} \nu q^\nu \tag{4}$$

as an upper bound on the cardinality of the Jacobian. Notice that the larger q is, the larger is the smallest genus g for which the Artin bound B_2 is indeed smaller than the Hasse-Weil upper bound

$$B_1 := (\sqrt{q}+1)^{2g}. \tag{5}$$

3 Weil Descent Attack

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

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

Gaudry, Hess and Smart [17] showed how Weil descent can be used to reduce the ECDLP in $E(K)$ to a discrete logarithm problem in the Jacobian $J_C(k)$ of a hyperelliptic curve C defined over k. One first constructs the Weil restriction $W_{E/k}$ of scalars of E, which is an n-dimensional abelian variety over k. Then, $W_{E/k}$ is intersected with $n-1$ hyperplanes to obtain the hyperelliptic curve C. We call their reduction algorithm the *GHS attack* on the ECDLP. The following is proven in [17].

Theorem 1 (Gaudry, Hess and Smart [17]) Let $q = 2^l$ and let $E : y^2 + xy = x^3 + ax^2 + b$ be an elliptic curve defined over $K = \mathbb{F}_{q^n}$. Let $\sigma : K \to K$ be the Frobenius automorphism defined by $\alpha \mapsto \alpha^q$, and let $b_i = \sigma^i(b)$ for $0 \le i \le n-1$. Let the *magic number for E relative to n* be

$$m = m(b) = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, b_0^{1/2}), (1, b_1^{1/2}), \ldots, (1, b_{n-1}^{1/2})\}). \tag{6}$$

Assume that

$$n \text{ is odd}, \quad \text{or } m(b) = n, \quad \text{or } \mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0. \tag{7}$$

Then the GHS attack constructs an explicit group homomorphism

$$\phi : E(\mathbb{F}_{q^n}) \to J_C(\mathbb{F}_q), \tag{8}$$

where C is a hyperelliptic curve defined over $\mathbb{F}_q$ of genus $g = 2^{m-1}$ or $2^{m-1} - 1$.

Remark 2 (*solving ECDLP instances in $E(\mathbb{F}_{q^n})$*) Assume now that $\#E(\mathbb{F}_{q^n})$ is almost prime, i.e., $\#E(\mathbb{F}_{q^n}) = rd$ where r is prime and d is small. In [17] it is argued that it is highly unlikely that the kernel of ϕ will contain the subgroup of order r of $E(\mathbb{F}_{q^n})$ unless E is defined over a proper subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$. Thus, ϕ can be used to reduce instances of the ECDLP in $\langle P \rangle$, where P is a point of order r in $E(\mathbb{F}_{q^n})$, to instances of the HCDLP in $J_C(\mathbb{F}_q)$. Namely, given P and $Q \in \langle P \rangle$, then $\log_P Q = \log_{\phi(P)} \phi(Q)$.

Remark 3 (*efficiency of determining C and computing ϕ*) The running time complexity of the algorithm presented in [17] for finding the defining equation of C and for computing ϕ has not been determined. However, if ng is relatively small, say $ng \leq 1000$, our extensive experiments suggest that Hess's KASH implementation [18, 5] of the algorithm takes at most a few hours on a workstation.

Formula (6) was analyzed in [26] and Theorem 5 was obtained. We first need to define the *type* of an element of $\mathbb{F}_{q^n}$.

Definition 4 Let $n = 2^e n_1$ where n_1 is odd. Let $h = 2^e$ and $x^n - 1 = (f_0 f_1 \cdots f_s)^h$ where $f_0 = x - 1$ and the f_i's are distinct irreducible polynomials over $\mathbb{F}_2$ with $\deg(f_i) = d_i$ and $1 = d_0 < d_1 \leq d_2 \leq \cdots \leq d_s$. For $b \in \mathbb{F}_{q^n}$, let $\mathrm{Ord}_b(x)$ be the unique polynomial $f \in \mathbb{F}_2[x]$ of least degree such that $f(\sigma)b = 0$; we have $\mathrm{Ord}_b(x) | x^n - 1$. For each $i \in [0, s]$, let j_i be the largest power of f_i which divides $\mathrm{Ord}_b(x)$. The *type* of b is defined to be $(j_0, j_1, \ldots, j_s)$.

Theorem 5 ([26]) Let $b \in \mathbb{F}_{q^n}$ have type $(j_0, j_1, \ldots, j_s)$.

(i) Then $m(b) = \sum_{i=0}^{s} j_i d_i + c$, where $c = 1$ if $j_0 = 0$, and $c = 0$ if $j_0 \neq 0$.

(ii) The number of elements $b \in \mathbb{F}_{q^n}$ of type $(j_0, j_1, \ldots, j_s)$ is $\prod_{i=0, j_i \neq 0}^{s} (q^{j_i d_i} - q^{(j_i - 1) d_i})$.

Lemma 6 asserts that condition (7) of Theorem 1 can be weakened.

Lemma 6 Let $E/\mathbb{F}_{q^n}$ be an elliptic curve defined by the equation $y^2 + xy = x^3 + ax^2 + b$ where $b \in \mathbb{F}_{q^n}$ has type $(j_0, j_1, \ldots, j_s)$. In Theorem 1, condition (7) can be replaced by the following, weaker, condition:

$$n \text{ is odd}, \quad \text{or } 2^e = j_0, \quad \text{or } \mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0. \tag{9}$$

Proof: Observe first that if n is even and $m(b) = n$, then b must be of type $(2^e, \ldots, 2^e)$ so that $2^e = j_0$. Thus, (7) indeed implies (9).

Now, let $\overline{f} = (x-1)^c \prod_{i=0}^{s} f_i^{j_i d_i}$, where $c = 1$ if $j_0 = 0$, and $c = 0$ if $j_0 \neq 0$. (This function has to replace the function f incorrectly defined in the proof of Lemma 11 in [17].) Let $\overline{h} = (x^n - 1)/\overline{f}$. From the proof of Lemma 11 in [17] it follows that Theorem 1 is true if $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$ or $\mathrm{Tr}_{K/\mathbb{F}_2}(a) + \overline{h}(1) = 0$. Thus, if $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 1$, Theorem 1 is true if $\overline{h}(1) = 1$. Since $x^n - 1 = (x^{n_1} - 1)^{2^e} = (x-1)^{2^e} \cdot \widetilde{k}$ with $\widetilde{k}(1) = 1$, we have $\overline{h}(1) = 1$ if and only if $(x-1)^{2^e}$ divides $\overline{f}$. Since the latter is true if and only if n is odd or $2^e = j_0$, the lemma is established. $\square$

There are $2^{N+1} - 2$ isomorphism classes of elliptic curves over $\mathbb{F}_{2^N}$ with representatives $y^2 + xy = x^3 + b$, $y^2 + xy = x^3 + ax^2 + b$, where $b \in \mathbb{F}_{2^N}^*$ and $a \in \mathbb{F}_{2^N}$ is a fixed element with $\mathrm{Tr}_{\mathbb{F}_{2^N}/\mathbb{F}_2}(a) = 1$.

The number I of isomorphism classes of elliptic curves over $\mathbb{F}_{2^N}$ with a given magic number m relative to n and satisfying (9) can be efficiently computed using the following.

Lemma 7 Let n and $m \in [1, n]$ be fixed. Let $c_{i,j} = q^{jd_i} - q^{(j-1)d_i}$ for $0 \le i \le s$ and $1 \le j \le h$. Let

$$F_0(z) = \begin{cases} 2(z + \sum_{j=1}^{h} c_{0,j} z^j) & \text{if } n \text{ is odd,} \\ z + \sum_{j=1}^{h-1} c_{0,j} z^j + 2c_{0,h} z^h & \text{if } n \text{ is even,} \end{cases}$$

$F_i(z) = 1 + \sum_{j=1}^{h} c_{i,j} z^{jd_i}$ for $1 \le i \le s$, and $F(z) = F_0(z) \prod_{i=1}^{s} F_i(z)$. Then the number of isomorphism classes of elliptic curves over $\mathbb{F}_{2^N}$ with magic number m relative to n and satisfying (9) is $I = [z^m]F(z)$ where $[\,]$ denotes the coefficient operator.

Proof: Follows immediately from Lemma 6 and Theorem 5. $\square$

If n is an odd prime, we have the following.

Theorem 8 ([26]) Let n be an odd prime, let $\bar{t}$ be the multiplicative order of 2 modulo n, and let $s = (n-1)/\bar{t}$. Then

(i) $x^n - 1$ factors over $\mathbb{F}_2$ as $(x-1) f_1 f_2 \cdots f_s$, where the f_i's are distinct irreducible polynomials of degree $\bar{t}$.

(ii) The smallest admissible value of $m(b)$ greater than 1 is $m(b) = \bar{t} + 1$.

(iii) Let $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be the Frobenius map defined by $x \mapsto x^q$. Define $B = \{b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q : (\sigma - 1) f_i(\sigma)(b) = 0 \text{ for some } 1 \le i \le s\}$, and let $a \in \mathbb{F}_{q^n}$ be an element of trace 1. Then for all $b \in B$, the elliptic curves $y^2 + xy = x^3 + b$ and $y^2 + xy = x^3 + ax^2 + b$ have $m(b) = \bar{t} + 1$. Furthermore, no element $b \in \mathbb{F}_{q^n} \setminus B$ has $m(b) = \bar{t} + 1$.

(iv) The cardinality of the set B is $qs(q^{\bar{t}} - 1)$.

4 Algorithms for the ECDLP and HCDLP

4.1 ECDLP

Let $E/\mathbb{F}_{2^N}$ be a cryptographically interesting elliptic curve, and let r be the large prime divisor of $\#E(\mathbb{F}_{2^N})$. Then Pollard's rho algorithm [30, 15, 34] for solving the ECDLP in the subgroup of order r of $E(\mathbb{F}_{2^N})$ has an expected running time of $(\sqrt{\pi r})/2$ elliptic curve additions. Since E is cryptographically interesting, $r \approx 2^{N-1}$ (taking into account that there is always a cofactor at least 2). We henceforth use $(\sqrt{\pi 2^{N-1}})/2$ to express the running time of Pollard's rho algorithm. Note that the algorithm can be effectively parallelized (see [27]) so that its expected running time on a network of S processors is $(\sqrt{\pi 2^{N-1}})/(2S)$.

4.2 HCDLP

Let C be a genus g hyperelliptic curve over $k = \mathbb{F}_q$. The HCDLP is the following: given C, $D_1 \in J_C(k)$, $r = \mathrm{ord}(D_1)$, and $D_2 \in \langle D_1 \rangle$, find the integer $\lambda \in [0, r-1]$ such that $D_2 = \lambda D_1$. We shall assume that r is prime.

We describe the Enge-Gaudry (EG) index-calculus algorithm [16, 7] for the HCDLP.

A reduced divisor $D = \mathrm{div}(a, b) \in J_C(k)$ is called a *prime divisor* if a is irreducible over k. Each reduced divisor $D = \mathrm{div}(a, b) \in J_C(k)$ can be expressed as a sum of prime divisors as follows: if $a = a_1^{e_1} a_2^{e_2} \cdots a_L^{e_L}$ is the factorization of a into monic irreducibles over k, then $D = \sum_{i=1}^{L} e_i \mathrm{div}(a_i, b_i)$ where $b_i = b \bmod a_i$ for all $i \in [1, L]$. Such a D is said to be *t-smooth* if $\max\{\deg a_i\} \leq t$.

In the Enge-Gaudry algorithm, a *smoothness bound* t is first chosen. Next, the *factor base* $\{P_1, P_2, \ldots, P_w\}$ is constructed—for each prime divisor $D = \mathrm{div}(a, b)$ of degree $\leq t$, exactly one of D and $-D$ is included in the factor base. Then, a random walk (á la Teske [33]) is performed in the set of reduced divisors equivalent to divisors of the form $\alpha D_1 + \beta D_2$ and the t-smooth divisors encountered in this walk are stored—each t-smooth divisor yields a relation $\alpha_i D_1 + \beta_i D_2 \sim R_i = \sum_j e_{ij} P_j$. When $w+5$ different relations have been found, one can find by linear algebra modulo r a non-trivial linear combination $\sum_{i=1}^{w+5} \gamma_i(e_{i1}, e_{i2}, \ldots, e_{iw}) = (0, 0, \ldots, 0)$. Thus $\sum_{i=1}^{w+5} \gamma_i R_i = 0$, whence $\sum \gamma_i(\alpha_i D_1 + \beta_i D_2) = 0$ and $\log_{D_1} D_2 = -(\sum \gamma_i \alpha_i)/(\sum \gamma_i \beta_i) \bmod r$.

The EG algorithm has a subexponential-time running time of

$$O(\exp((\sqrt{2} + o(1))\sqrt{\log q^g \log\log q^g}))$$

bit operations for $g/\log q \to \infty$. The following non-asymptotic analysis of the running time for the relation gathering stage was given in [21]. A good approximation for the number A_l of prime divisors of degree l in the factor base is

$$A_l \approx \frac{1}{2}\left(\frac{1}{l}\sum_{d|l} \mu(l/d) q^d\right), \tag{10}$$

where μ is the Möbius function. The factor base size w is therefore well approximated by

$$F(t) = \sum_{l=1}^{t} A_l = \frac{1}{2}\sum_{l=1}^{t}\left(\frac{1}{l}\sum_{d|l} \mu(l/d) q^d\right). \tag{11}$$

By [21, Lemma 2], the number of t-smooth reduced divisors in $J_C(k)$ is

$$M(t) = \sum_{i=1}^{g}\left([x^i]\prod_{l=1}^{t}\left(\frac{1+x^l}{1-x^l}\right)^{A_l}\right), \tag{12}$$

where [ ] denotes the coefficient operator. Under the heuristic assumption that the proportion of t-smooth divisors in $\langle D_1 \rangle$ is the same as the proportion of t-smooth divisors in the full group $J_C(k)$, the expected number of random walk iterations before a t-smooth divisor is encountered is

$$E(t) = \#J_C(k)/M(t). \tag{13}$$

Finally, the expected number of random walk iterations before $F(t) + 5$ relations are generated is

$$T(t) = (F(t) + 5)E(t). \tag{14}$$

5 Analysis

For each composite $N \in [100, 600]$, we determine and compare the running times for solving the ECDLP in a (potentially) cryptographically interesting elliptic curve over $\mathbb{F}_{2^N}$ using the GHS attack and using Pollard's rho method. We express the running times for Pollard's rho method and the GHS attack in terms of elliptic curve operations and in terms of random walk iterations in the Jacobian, respectively, as outlined in §4. In particular, we do not consider the different bit complexities of operations for elliptic and hyperelliptic curves since these are expected to be roughly the same. Furthermore, we do not take into account the time spent on mapping the ECDLP instance to a HCDLP instance, and the time spent on the linear algebra stage of the Enge-Gaudry index-calculus algorithm.

For each composite $N \in [100, 600]$, Algorithm 10 determines the elliptic curve parameters (in terms of n, m and g) such that (i) there should (cf. Remark 20) exist a cryptographically interesting elliptic curve E over $\mathbb{F}_{2^N}$ with these parameters; and (ii) the GHS attack is more efficient for solving the ECDLP in $E(\mathbb{F}_{2^N})$ than for solving the ECDLP on any other cryptographically interesting elliptic curve over $\mathbb{F}_{2^N}$. For each such set of parameters (n, m, g), we list the number I of isomorphism classes of elliptic curves over $\mathbb{F}_{2^N}$ that have magic number m relative to n and satisfy (9), the optimal smoothness bound t for the Enge-Gaudry algorithm, and the resulting estimates for the factor base size $F(t)$ and the (minimized) running time $T(t)$ in terms of random walk iterations.

Remark 9 (*EG1 versus EG2*) In Algorithm 10, two variants of the Enge-Gaudry algorithm are considered. The first variant, denoted by EG1, only works with a factor base whose size is upper bounded by $10^7 \approx 2^{23}$, while the second variant, denoted by EG2, does not assume any upper bound on the factor base size. Note that a factor base of size 10^7 is on the edge of what is considered feasible today [22, 23]. If $A_1 = 2^{l-1} > 10^7$ for some hyperelliptic curve of genus g over $\mathbb{F}_{2^l}$, then, in order to achieve a factor base size $\leq 10^7$, the Enge-Gaudry algorithm can be modified by selecting the factor base to consist of only a proportion $\frac{1}{\epsilon}$ of all prime divisors of degree 1 [17]. However, the expected time to find a smooth divisor will be increased by a factor of ϵ^g. Therefore, we decided not to consider this modification in our analysis. If the factor base size for EG2 is significantly larger than 10^7, then the EG2 algorithm is not currently practical. Nevertheless, we feel that listing the optimum times for EG2 is important because they will become relevant should improvements be made in the future to algorithms for solving sparse linear systems.

Algorithm 10 (*Computing optimal* (n, m, g, t, F, T))
INPUT: N, "EG1" or "EG2".
OUTPUT: Parameters n, m, g for which there may exist a cryptographically interesting elliptic curve whose ECDLP is most easily solved with the GHS attack; optimal smoothness bound t; (estimated) factor base size F; and (estimated) expected running time T in terms of random walk iterations.

1. For all divisors $n \geq 2$ of N do the following:
   (a) Set $l \leftarrow N/n$ and $q \leftarrow 2^l$.
   (b) { For EG1: The 10^7 bound on the factor base size must be violated if $A_1 = 2^{l-1} > 10^7$. }
   Case EG1: If $l \geq 25$ then set $T_n \leftarrow \infty$ and go to step 1.
   (c) Write $n = n_1 h$ where $h = 2^e$ and n_1 is odd.
   (d) { Compute the degrees of the irreducible factors of $x^{n_1} - 1$ over $\mathbb{F}_2$. }
   Let the cyclotomic cosets of 2 modulo n_1 have sizes $1 = d_0 \leq d_1 \leq d_2 \leq \cdots \leq d_s$.
   (e) { Compute a lower bound m' on magic number m relative to n that yields a large enough Jacobian (cf. Remark 11). }
   For $m' = 2, 3, \ldots, n$ do the following:
      i. Set $g \leftarrow 2^{m'-1} - 1$. Compute B_1, B_2 as defined in (5),(4).
      ii. If $\min\{\log_2 B_1, \log_2 B_2\} \geq N - 3$ then go to step 1(f).
      iii. Set $g \leftarrow 2^{m'-1}$. Compute B_1, B_2 as defined in (5),(4).
      iv. If $\min\{\log_2 B_1, \log_2 B_2\} \geq N - 3$ then go to step 1(f).
   (f) { Find the smallest admissible magic number m relative to n (cf. Theorem 5). }
   For $m = m', m' + 1, \ldots, n$ do the following:
   If m can be written in the form $\sum_{i=0}^{s} d_i j_i$ with $0 \leq j_i \leq h$, $j_0 \geq 1$, then:
      { Check that the sufficient conditions of Corollary 14 (for every elliptic curve over $\mathbb{F}_{2^N}$ having magic number m relative to n to be defined over a proper subfield $\mathbb{F}_{2^\nu}$ of $\mathbb{F}_{2^N}$ for some $\nu \geq 3$) are violated. }
      If n is a power of 2, set $d \leftarrow \infty$; else set $d \leftarrow d_1$.
      If $[m > d$ or $m > 2^e]$ or $[d = \infty$ and $m > 2^{e-1}]$ then go to step 1(g).
   (g) If $m > m'$ then set $g \leftarrow 2^{m-1} - 1$.
   (h) { If the size of the Jacobian is not too large, i.e., if $gl \leq 4096$ (cf. Remark 15), then find the optimum smoothness bound t for the Enge-Gaudry algorithm using (11) to estimate the factor base size $F(t)$, (13) to estimate the expected running time $E(t)$ to find a smooth divisor with $\#J_C(\mathbb{F}_q) = 2^{gl}$, and (14) to estimate the expected running time $T(t)$. }
   If $gl \geq 4097$ then set $T_n \leftarrow \infty$.
   Else:
      i. Case EG1: Set $S \leftarrow \{1 \leq t \leq 120 \ : \ F(t) \leq 10^7\}$.
      Case EG2: Set $S \leftarrow \{1, 2, \ldots, 120\}$.
      ii. Let t be the index in S which minimizes $T(t)$.
      iii. Set $m_n \leftarrow m$, $g_n \leftarrow g$, $t_n \leftarrow t$, $F_n \leftarrow F(t_n)$, $T_n \leftarrow T(t_n)$.

2. If $T_n = \infty$ for all n, output "$gl \geq 4097$ for all n".
   Else, let n be the index for which T_n is a minimum and output "$(n, m_n, g_n, t_n, F_n, T_n)$".

Remark 11 (*explanation of the lower bound on* $\log_2 B_1$ *and* $\log_2 B_2$ *in step 1(e) of Algorithm 10*) If we restrict our attention to cryptographically interesting elliptic curves E over $\mathbb{F}_{2^N}$ with $\#E(\mathbb{F}_{2^N}) = dr$, where $d \in \{2, 4\}$ and r is prime, then

$$r \geq \#E(\mathbb{F}_{2^N})/4 \geq (2^{N/2} - 1)^2/4 > 2^{N-1}/4 = 2^{N-3} \text{ for } N \geq 4.$$

Thus, if the hyperelliptic curve C over $\mathbb{F}_q$ generated by the GHS reduction has genus g, then by (4) and (5) a necessary condition for $J_C(\mathbb{F}_q)$ to have a subgroup of order r is $\min(B_1, B_2) \geq \#J_C(\mathbb{F}_q) \geq 2^{N-3}$.

Remark 12 (*explanation of step 1(f) of Algorithm 10*) There are some (N, l, g) parameters for which elliptic curves over $\mathbb{F}_{2^N}$ with parameters (l, g) do exist, but none of which are cryptographically interesting. For example, if $N = 160$, the ECDLP is most easily solved with the GHS attack if $(n, l, m, g) = (8, 20, 4, 8)$. Then, for the attack to work (cf. condition (9) in Lemma 6), we need $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$, i.e., without loss of generality, $a = 0$. Now, consider an elliptic curve $E : y^2 + xy = x^3 + b$ over $\mathbb{F}_{2^{160}}$ that yields magic number $m = 4$ on performing the GHS attack with $n = 8$. We have $x^n - 1 = (x - 1)^8$, and hence $(\sigma - 1)^4 b = 0$ where $\sigma : \mathbb{F}_{2^{160}} \to \mathbb{F}_{2^{160}}$ is defined by $\alpha \mapsto \alpha^{2^{20}}$. That is, $b \in \mathbb{F}_{2^{80}}$, which implies that $\#E(\mathbb{F}_{2^{80}})$ divides $\#E(\mathbb{F}_{2^{160}})$. Hence E is not cryptographically interesting. The next easiest instance of an ECDLP over $\mathbb{F}_{2^{160}}$ for which a cryptographically interesting curve can exist is $(n, l, m, g) = (20, 8, 6, 31)$. Such a phenomenon always occurs when $(n, m) = (8, 4)$ are the GHS parameters for which the ECDLP is most easily solved, which is the case for $N = 176, 184, 192$ and many other N divisible by 8. But also for $N = 224$ where $(n, m) = (32, 6)$ would be best we find that $\#E(\mathbb{F}_{2^{56}})$ must divide $\#E(\mathbb{F}_{2^{224}})$ for any elliptic curve with these parameters. Another example is $N = 304$ where $(n, m) = (16, 5)$ would be optimal—here we find that $\#E(\mathbb{F}_{2^{304}})$ must be divisible by $\#E(\mathbb{F}_{2^{152}})$.

Lemma 13 generalizes the observations made in Remark 12.

Lemma 13 Let $E/\mathbb{F}_{q^n}$ be an elliptic curve defined by the equation $y^2 + xy = x^3 + ax^2 + b$, where $b \in \mathbb{F}_{q^n}$ has type $(j_0, j_1, \ldots, j_s)$. Suppose that (9) holds. Let $n = 2^e n_1$, where n_1 is odd. If n is a power of 2, then let $d = \infty$; otherwise, let $d = d_1 = \min\{d_i : 1 \leq i \leq s\}$. Let $m = m(b)$ be as in Theorem 1. Let $\mu = 2^{\lceil \log_2 m \rceil}$, i.e., the smallest power of 2 greater than or equal to m. If $m \leq d$ and $m \leq 2^e$, then E is isomorphic to an elliptic curve defined over $\mathbb{F}_{q^\mu}$ and hence $\#E(\mathbb{F}_{q^n})$ is divisible by $\#E(\mathbb{F}_{q^\mu})$.

Proof: Assume first that $m \leq d$ and $m < 2^e$. Then b must have type $(m, 0, \ldots, 0)$, and n is even and $2^e \neq j_0$. The former implies that $b \in B = \{b \in \mathbb{F}_{q^n} : (\sigma + 1)^m(b) = 0\} \setminus \{b \in \mathbb{F}_{q^n} : (\sigma + 1)^{m-1}(b) = 0\}$. Let $m_- = \mu/2$, i.e., the largest power of 2 strictly less than m. Then $B \subset \mathbb{F}_{q^\mu} \setminus \mathbb{F}_{q^{m_-}}$. Since n is even and $2^e \neq j_0$, we require $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$ for Lemma 6 to hold. Thus, without loss of generality, $a = 0$. Thus, E is defined over $\mathbb{F}_{q^\mu}$ but not over any proper subfield of $\mathbb{F}_{q^\mu}$.
Now assume that $m \leq d$ and $m = 2^e$. Then n/μ is odd. As before, $b \in \mathbb{F}_{q^\mu} \setminus \mathbb{F}_{q^{m_-}}$. Since $m = 2^e$, both $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0, 1$ are possible. Now, $\mathrm{Tr}_{K/\mathbb{F}_2}(c) = (n/\mu)\mathrm{Tr}_{\mathbb{F}_{q^\mu}/\mathbb{F}_2}(c)$ for all $c \in \mathbb{F}_{q^\mu}$. Since n/μ is odd, $\mathrm{Tr}_{K/\mathbb{F}_2}(c) = \mathrm{Tr}_{\mathbb{F}_{q^\mu}/\mathbb{F}_2}(c)$, so that there exists $c \in \mathbb{F}_{q^\mu}$ such that $\mathrm{Tr}_{K/\mathbb{F}_2}(c) = 1$. Therefore, both for $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$ and $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 1$ there exists a curve isomorphic to E that is defined over $\mathbb{F}_{q^\mu}$ but not over any proper subfield of $\mathbb{F}_{q^\mu}$. $\square$

N	EG1										EG2									
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
160	20	8	6	31	48	3	21	52	79	27	4	40	3	4	120	1	39	44	79	35
161	7	23	4	7	94	1	22	34	80	46	7	23	4	7	94	1	22	34	80	46
162	54	3	7	63	21	9	23	42	80	38	6	27	4	7	109	1	26	38	80	42
164	–	–	–	–	–	–	–	–	–	–	4	41	3	4	123	1	40	45	81	36
165	15	11	5	15	58	2	20	37	82	45	15	11	5	15	58	2	20	37	82	45
166	–	–	–	–	–	–	–	–	–	–	2	83	2	2	167	1	82	83	82	–
168	7	24	4	7	98	1	23	35	83	48	7	24	4	7	98	1	23	35	83	48
169	169	1	13	4095	14	28	23	1208	84	–	169	1	13	4095	14	120	113	307	84	–

Table 1: Sample output of Algorithm 10 (cf. Appendix A).

Corollary 14 If n is not a power of 2 and $m \leq \min(d, 2^e)$, then E is isomorphic to an elliptic curve defined over a proper subfield of $\mathbb{F}_{q^n}$. If n is a power of 2 and $m \leq n/2$, then E is isomorphic to an elliptic curve defined over $\#E(\mathbb{F}_{q^{n/2}})$.

Observe that if the conditions of Corollary 14 hold, then either $\#\mathbb{F}_{q^\mu} \geq 8$, or $m \in \{1, 2\}$ and $\#\mathbb{F}_q \in \{2, 4\}$ in which case the Jacobian $J_C(\mathbb{F}_q)$ is too small to have a subgroup of order r.

Remark 15 (*restriction on gl in step 1(h) of Algorithm 10*) For $g \geq 4097$ we were unable to compute the expected running time of EG1/EG2 because of computational limitations when computing Taylor series expansions needed to evaluate $M(t)$ (cf. formula (12)). We therefore ignore all instances (n, l, g) where $gl \geq 4097$. Notice that in this case the Jacobian $J_C(\mathbb{F}_q)$ has size at least 2^{4097} whence any (cryptographically interesting) HCDLP instance in $J_C(\mathbb{F}_q)$ is infeasible using the known index-calculus algorithms. In particular, if $l = 1$ and $g = 4095$, the smallest running time for EG2 is with $t = 120$ and amounts to $\approx 2^{307}$ random walk iterations, which is more than the expected number of elliptic curve operations using Pollard's rho method for $N = 600$.

The outputs of Algorithm 10 with composite $N \in [100, 600]$ as inputs are listed in Appendix A. For the purpose of illustration, a small excerpt of this table is given in Table 1. In these tables, the entries for I, F, T, and ρ are the *logarithms* (base 2, rounded to the nearest integer) of the number of isomorphism classes of elliptic curves with magic number m relative to n and satisfying (9), the factor base size, the expected number of random walk iterations in the Enge-Gaudry algorithm, and the number of elliptic curve operations in Pollard's rho method, respectively. $D1$ and $D2$ denote the differences $\rho - T$ (if positive) for EG1 and EG2, respectively. If for some N data is given for EG2 but not for EG1, we are in the situation that $gl \geq 4097$ for all divisors $l \leq 24$ of N (such as for $N = 164$ and 166 in Table 1). If for some N data is given for neither EG1 nor EG2, we are in the situation that $gl \geq 4097$ for all l dividing N. The latter occurs for only 5 values of N: 289, 323, 361, 493 and 551.

Remark 16 (*further limitations of our analysis*) Our analysis yields the same running times whenever (g, l) are the same, independently of N (e.g., $T = 53$ when $(g, l) = (15, 13)$ for both $N = 130$ and $N = 195$—see Appendix A). This is because the running time of the Enge-Gaudry algorithm is computed under the assumption that $\#J_C(\mathbb{F}_q) \approx q^g = 2^{gl}$. However, we only expect that $\#J_C(\mathbb{F}_q)$ is divisible by the large prime that divides $\#E(\mathbb{F}_{q^n})$. Hence if $gl \gg N$, it may well be the case that the Jacobian obtained from Weil descent is much smaller in size than q^g, which would then lead to a significantly smaller value $E(t) = \#J_C(k)/M(t)$, and hence also to a significantly smaller running time $T(t)$. This observation is particularly meaningful where $l = 1$, in which case the Hasse-Weil lower bound $(\sqrt{2}-1)^{2g} \le \#J_C(\mathbb{F}_2)$ is trivial. For example, if $(l, g) = (1, 255)$, we have $T = 2^{54}$ for EG1 and $T = 2^{52}$ for EG2, for $N = 117, 153, 170, 171, 187, 190, \text{etc.}, 270, 273$. Thus, caution must be exercised when interpreting our data for those N where $gl \gg N$. Nevertheless, if $gl \approx N$, our running time estimates are precise.

Remark 17 (*success of the GHS attack*) There are some composite $N \in [160, 600]$ for which the GHS attack succeeds on some cryptographically interesting elliptic curves over $\mathbb{F}_{2^N}$. That is, Pollard's rho algorithm is infeasible for solving the ECDLP on these curves, and the GHS attack is successful in reducing instances of the ECDLP on these curves to instances of the HCDLP which are solvable using known algorithms and existing computer technology. Examples of such N are $N = 161, 180, 186, 217, 248, 300$ (cf. §7).

Remark 18 (*failure of the GHS attack*) We can conclude that for those composite $N \in [100, 600]$ for which no values are entered for EG1, the GHS attack does not reduce the level of security offered—Pollard's rho method is the faster algorithm for *all* elliptic curves over $\mathbb{F}_{2^N}$. In particular, this is true for $N = 185$, which is of practical significance because a specific elliptic curve over $\mathbb{F}_{2^{185}}$ is listed in the IETF standard [20] for key establishment. We emphasize that our statements about the failure of the GHS attack for all elliptic curves over some field $\mathbb{F}_{2^N}$ are under the assumption that the Enge-Gaudry algorithm is essentially the best index-calculus algorithm for the HCDLP, and, in particular, that the linear algebra stage is intractable if the factor base size is greater than 10^7. In the particular case $N = 185$ however, the smallest possible factor base in the unmodified Enge-Gaudry algorithm (cf. Remark 9) is of size 2^{36}.

Remark 19 (*effectiveness of the GHS attack*) When $D1 > 0$ for some composite $N \in [100, 600]$, the level of security offered by some cryptographically interesting elliptic curves defined over $\mathbb{F}_{2^N}$ may be reduced due to the GHS attack. However, note that our data corresponds to elliptic curves with *least possible* magic numbers and genera, and only a small proportion of elliptic curves yield this minimal magic number. For example, if $N = 161$, then only $\approx 2^{94}$ out of $\approx 2^{162}$ elliptic curves over $\mathbb{F}_{2^{161}}$ have magic number $m = 4$ relative to $n = 7$. Correspondingly, for $N = 165$ the proportion of elliptic curves with magic number $m = 5$ relative to $n = 15$ is only $\approx 2^{58}$ out of 2^{166}, whereas for $N = 162$, the proportion of curves having magic number $m = 7$ relative to $n = 54$ is even smaller, namely $\approx 2^{21}$ out of 2^{163}. Galbraith, Hess and Smart [13] (see also [12]) presented an algorithm with expected average running time of $O(q^{n/4+\epsilon})$ for explicitly computing an isogeny between two isogenous elliptic curve over $\mathbb{F}_{q^n}$. (Two elliptic curves $E_1/\mathbb{F}_{q^n}$ and $E_2/\mathbb{F}_{q^n}$ are said to be *isogenous* over $\mathbb{F}_{q^n}$ if $\#E_1(\mathbb{F}_{q^n}) = \#E_2(\mathbb{F}_{q^n})$.) They observed that this algorithm can be used to extend the effectiveness of the GHS attack. Namely, given an ECDLP instance on some cryptographically interesting elliptic curve $E_1/\mathbb{F}_{2^N}$, one can check if E_1 is isogenous to some elliptic curve $E_2/\mathbb{F}_{2^N}$ which yields an easier HCDLP than E_1, and then use an isogeny $\phi : E_1 \to E_2$ to map the ECDLP instance to an instance of the ECDLP in $E_2(\mathbb{F}_{2^N})$. For example, in the case $N = 165$, we can expect that roughly 2^{135} out of

2^{166} elliptic curves over $\mathbb{F}_{2^{165}}$ are isogenous to one of the $\approx 2^{58}$ elliptic curves over $\mathbb{F}_{2^{165}}$ having magic number $m = 5$ relative to $n = 15$. Note, however, that finding a curve with $m = 5$ isogenous to a given elliptic curve over $\mathbb{F}_{2^{165}}$ (assuming that such an isogenous curve exists) may be difficult as one essentially has to search through the entire set of 2^{58} curves.

Remark 20 (*finding cryptographically interesting elliptic curves with given (N, l, m) parameters*) One can attempt to find a cryptographically interesting elliptic curve with given (N, l, m) parameters as follows. First select arbitrary b from the set $B = \{b \in \mathbb{F}_{2^N} : m(b) = m\}$; that the elements of B can be efficiently enumerated can be seen from Theorem 5(i). Next, compute $H = \#E_b(\mathbb{F}_{2^N})$ where $E_b : y^2 + xy = x^3 + b$ using Satoh's algorithm [31, 8], and test if either H or $2^{N+1} + 2 - H$ (the order of the twist of E_b) is almost a prime. Observe that if $b \in B$, then $b^2 \in B$. Moreover, E_b and E_{b^2} are isogenous over $\mathbb{F}_{2^N}$. Thus, if $b \in B$ has already been tested, then one should not select b^{2^i} for any $1 \leq i \leq N-1$. Now, it is known that the order of a randomly selected elliptic curve over $\mathbb{F}_{2^N}$ is roughly uniformly distributed over the even integers in the Hasse interval $[(2^{N/2}-1)^2, (2^{N/2}+1)^2]$. Thus, if the set B has sufficiently large cardinality (which can be determined from Lemma 7), then we can expect to quickly find an elliptic curve of almost prime order.

6 Elliptic Curves from ANSI X9.62

The ANSI X9.62 standard [1] lists in its Appendix H.4 specific elliptic curves over fields of characteristic two of the composite extension degrees $N = 176, 208, 272, 304, 368$. These N factor as $16 \cdot p$ where $p \in \{11, 13, 17, 19, 23\}$ is prime. Table 2 lists the elliptic curve parameters in hexadecimal notation, where each curve is defined by the equation $y^2 + xy = x^3 + ax^2 + b$. Notice that in all cases the coefficients a and b lie in the proper subfield $\mathbb{F}_{2^{16}}$ of $\mathbb{F}_{2^N}$, whence $\#E(\mathbb{F}_{2^N}) = rd$ with r prime and $d \in [2^{16} + 1 - 2^9, 2^{16} + 1 + 2^9]$.

For a curve defined over a proper subfield of $\mathbb{F}_{q^n}$ containing $\mathbb{F}_q$, it cannot be argued that the kernel of the map ϕ defined in (8) would not contain the large subgroup of order r of $E(\mathbb{F}_{q^n})$. In fact, the opposite is true.

Remark 21 (*failure of GHS-attack for subfield curves*) Let $E/\mathbb{F}_{q^n}$ be an elliptic curve defined by the equation $y^2 + xy = x^3 + ax^2 + b$. Let $\mathbb{F}_q(a, b)$ be the smallest extension of $\mathbb{F}_q$ over which E is defined. Then for any extension field K of $\mathbb{F}_q(a, b)$ the GHS Weil descent of E/K down to $\mathbb{F}_q$ is independent of K. That is, the GHS Weil descent of E/K down to $\mathbb{F}_q$ yields the same (upto birational equivalence) hyperelliptic curve $C/\mathbb{F}_q$ as the GHS Weil descent of $E/\mathbb{F}_q(a, b)$ [19]. This can be derived from the facts that the defining equations for $\mathfrak{D}$ in Lemma 2 of [17] depend only on $\mathbb{F}_q(a, b)$ but not on K, and that the same is true for the set Δ_0 in the proof of Lemma 6 of [17]. Thus, if $\mathbb{F}_q(a, b) \neq \mathbb{F}_{q^n}$, only points in the small subgroup $E(\mathbb{F}_q(a, b))$ of $E(\mathbb{F}_{q^n})$ are likely to be mapped to non-trivial divisors in the Jacobian $J_C(\mathbb{F}_q)$, while points in the subgroup of order r will be mapped to the zero divisor, which is of no use for solving ECDLPs in $E(\mathbb{F}_{q^n})$.

Remark 22 (*success of GHS-attack for subfield curves*) If $\mathbb{F}_q(a, b) = \mathbb{F}_{q^n}$, the same arguments as in the non-subfield case apply, and the GHS Weil descent should yield a map ϕ whose kernel does not

E176, $N = 176$, $\mathbb{F}_{2^{176}} = \mathbb{F}_2[z]/(z^{176} + z^{43} + z^2 + z + 1)$, $\#\mathrm{E176}(\mathbb{F}_{2^{176}}) = 65390 \cdot r$
$a =$ `E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B`
$b =$ `5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2`
$r =$ `10092537397ECA4F6145799D62B0A19CE06FE26AD`
E208, $N = 208$, $\mathbb{F}_{2^{208}} = \mathbb{F}_2[z]/(z^{208} + z^{83} + z^2 + z + 1)$, $\#\mathrm{E208}(\mathbb{F}_{2^{208}}) = 65096 \cdot r$, $a = 0$
$b =$ `C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E`
$r =$ `101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D`
E272, $N = 272$, $\mathbb{F}_{2^{272}} = \mathbb{F}_2[z]/(z^{272} + z^{56} + z^3 + z + 1)$, $\#\mathrm{E272}(\mathbb{F}_{2^{272}}) = 65286 \cdot r$
$a =$ `91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20`
$b =$ `7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7`
$r =$ `100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521`
E304, $N = 304$, $\mathbb{F}_{2^{304}} = \mathbb{F}_2[z]/(z^{304} + z^{11} + z^2 + z + 1)$, $\#\mathrm{E304}(\mathbb{F}_{2^{304}}) = 65070 \cdot r$
$a =$ `FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288078365A0396C8E681`
$b =$ `BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14039601E55827340BE`
$r =$ `101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA6899164443051D`
E368, $N = 368$, $\mathbb{F}_{2^{368}} = \mathbb{F}_2[z]/(z^{368} + z^{85} + z^2 + z + 1)$, $\#\mathrm{E368}(\mathbb{F}_{2^{368}}) = 65392 \cdot r$
$a =$ `E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94778C576D62F0AB751` `9CCD2A1A906AE30D`
$b =$ `FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54917E1C2112D84D164` `F444F8F74786046A`
$r =$ `10090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579BD87E909AE40A6F13` `1E9CFCE5BD967`

Table 2: Sample elliptic curves from ANSI X9.62.

					EG1					EG2				
EN	n	l	m	g	t	F	T	ρ	$D1$	t	F	T	ρ	$D2$
E176	2	88	2	2	–	–	–	–	–	1	87	88	78	–
	4	**44**	**4**	**8**	–	–	–	–	–	**1**	**43**	**58**	**78**	**20**
	8	**22**	**8**	**128**	**1**	**21**	**737**	**78**	–	6	128	222	78	–
	16	11	16	$2^{15}(-1)$	–	–	–	–	–	–	–	–	–	–
E208	2	104	2	2	–	–	–	–	–	1	103	104	94	–
	4	**52**	**4**	**8**	–	–	–	–	–	**1**	**51**	**66**	**94**	**28**
	8	26	7	64	–	–	–	–	–	4	101	161	94	–
	16	13	14	$2^{13}(-1)$	–	–	–	–	–	–	–	–	–	–
E272	2	136	2	2	–	–	–	–	–	1	135	136	126	–
	4	**68**	**4**	**8**	–	–	–	–	–	**1**	**67**	**82**	**126**	**44**
	8	34	8	128	–	–	–	–	–	5	167	285	126	–
	16	17	16	$2^{15}(-1)$	–	–	–	–	–	–	–	–	–	–
E304	2	152	2	2	–	–	–	–	–	1	151	153	142	–
	4	**76**	**4**	**8**	–	–	–	–	–	**1**	**75**	**90**	**142**	**52**
	8	38	8	128	–	–	–	–	–	4	149	305	142	–
	16	19	16	$2^{15}(-1)$	–	–	–	–	–	–	–	–	–	–
E368	2	184	2	2	–	–	–	–	–	1	183	184	174	–
	4	**92**	**4**	**8**	–	–	–	–	–	**1**	**91**	**106**	**174**	**68**
	8	46	7	64	–	–	–	–	–	3	135	222	664	–
	16	23	13	$2^{12}(-1)$	–	–	–	–	–	–	–	–	–	–

Table 3: GHS attack data for some elliptic curves from ANSI X9.62.

contain the subgroup of order r. Let n^* be the smallest integer such that $a, b \in \mathbb{F}_{2^{n^*}}$. Then, with $q = 2^l$, we have that $\mathbb{F}_q(a, b) = \mathbb{F}_{q^n}$ if and only if $\operatorname{lcm}(n^*, l) = N$.

For the curves given in Table 2, $n^* = 16$ and $p = N/n^*$ is prime. Remarks 21 and 22 imply that we need to analyze exactly those descents from $\mathbb{F}_{q^n}$ down to $\mathbb{F}_q$ for which $\gcd(n, p) = 1$.

We can compute the values of m using formula (6) of Theorem 1 for the various decompositions $N = nl$ without actually performing the GHS reduction. Having computed m and using that $g = 2^{m-1}$ or $2^{m-1} - 1$, for each decomposition $N = nl$ we can estimate the respective running times for the Enge-Gaudry algorithm as explained in §4.2. Our results for the five ANSI X9.62 curves are listed in Table 3. For all cases where $m < 13$, we performed the GHS reductions to determine the exact genera of the resulting hyperelliptic curves; we found that in all cases, $g = 2^{m-1}$ (and never the case that $g = 2^{m-1} - 1$). For each (n, l, m, g) we then computed the optimal smoothness bound t, the estimated size F of the factor base, and the corresponding expected running time T for the Enge-Gaudry algorithm with (EG1) and without (EG2) the upper bound 10^7 on the factor base size. For comparison, we list the expected running time $\rho = 2\sqrt{\pi r/N}$ of Pollard's rho method in a subgroup of order r combined with the speedup of [15, 34] that is applicable since the elliptic curves are defined over $\mathbb{F}_{2^{16}}$. In Table 3, the entries for F, T and ρ are the *logarithms* (base 2, rounded to the nearest integer) of the actual values. $D1$ and $D2$ denote the difference (if positive) between the entries in column ρ and column T, respectively. For each curve, the data corresponding to the smallest value of T is given in bold face.

Regardless of the fact that ϕ maps points in the large prime-order subgroup of $E(\mathbb{F}_{q^n})$ to the zero divisor (class) of the resulting Jacobian of the hyperelliptic curve, we determined the attack data also for those descents where $\gcd(n,p) > 1$, i.e., where $l = 2^i$ for $i \in \{0,1,2,3,4\}$. We found that in all except two cases either the m-values are too small for the Jacobians to potentially contain the large prime-order subgroup (see also Remark 24), or the genera of the hyperelliptic curves are larger than $2^{12}-1$ and thus too large for the resulting HCDLP to be feasible. The two exceptions to this are E176 with $(n,m,g) = (88,8,128)$ and E272 with $(n,m,g) = (136,8,128)$, for which we would have the following attack data if the GHS descent were not doomed to fail due to the reasons given in Remark 21.

					EG1					EG2				
EN	n	l	m	g	t	F	T	ρ	$D1$	t	F	T	ρ	$D2$
E176	88	2	8	128	13	22	54	78	24	17	29	51	78	27
E272	136	2	8	128	13	22	54	126	72	17	29	51	126	75

Remark 23 (*failure of the GHS attack for E176 and E272*) When evaluating the mapping $\phi : E(\mathbb{F}_{2^{176}}) \to J_C(\mathbb{F}_{2^2})$ (where E = E176) constructed by the GHS attack we found that the large subgroup $\langle P \rangle$ of prime order $r \approx 2^{160}$ is contained in the kernel of ϕ, and thus is of no use for solving ECDLPs in $E(\mathbb{F}_{2^{176}})$. The same situation was observed with the mapping $\phi : E(\mathbb{F}_{2^{272}}) \to J_C(\mathbb{F}_{2^2})$ for E = E272.

Remark 24 (*m values for the cases $l = 1,2,4,8,16$*) Suppose that $l \in \{1,2,4,8,16\}$, and let $\sigma : \alpha \mapsto \alpha^{2^l}$ be the Frobenius map on $\mathbb{F}_{2^N}$. Then, since $b \in \mathbb{F}_{2^{16}} \setminus \mathbb{F}_{2^8}$, we have that $(\sigma+1)^{16/l} b = 0$ but $(\sigma+1)^{8/l} b \neq 0$. Thus we expect that $8/l < m \leq 16/l$.

Remark 25 (*applicability of the GHS reduction*) For E176, E272 and E304 we have $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 1$, so that condition (7) of Theorem 1 is not satisfied for these curves whenever $m(b) \neq n$. However, the weaker condition (9) of Lemma 6 does hold, and that is why the GHS reduction does produce hyperelliptic curves of genus 2^{m-1} or $2^{m-1}-1$ over $\mathbb{F}_q$ even when $m \neq n$.

Remark 26 (*existence of isogenous curves which may yield easier HCDLPs*) To exclude the applicability of the Extended GHS attack (see [13] and Remark 19) we checked if any of the ANSI X9.62 curves are isogenous to an elliptic curve for which the GHS reduction produces an easier HCDLP. For this, we use a modification of Algorithm 10 that allows the elliptic curve to be defined over a proper subfield $\mathbb{F}_{2^\nu}$ of $\mathbb{F}_{2^N}$ with $\nu \leq 16$ iff $\gcd(n,p) = 1$ (see Remarks 21 and 22). That is, if $\gcd(n,p) = 1$, in Algorithm 10 we accept m even if Corollary 14 applies, as long as $l \cdot \lceil \log_2 m \rceil \leq 16$.

Since this time we are not only interested in the best instance (N,n,m) but in any instance for which the GHS attack yields an algorithm more efficient than Pollard rho, we give the estimated running times for *all* decompositions $N = nl$ in Table 4. The notation is the same as in Table 1. Observe that for all parameters listed here curves exist that are defined over the full field $\mathbb{F}_{q^n}$ and no proper subfield of it.

(i) E176. The only possibility to improve on the GHS attack highlighted in Table 3 is to find a curve isogenous to E176 and for which $(n,m) = (8,5)$. Since there are $I \approx 2^{110}$ isomorphism classes of curves over $\mathbb{F}_{2^{176}}$ with these parameters, it is well possible that such a curve exists. However, finding such a curve is very likely to be much harder than solving the ECDLP using Pollard rho.

			EG1								EG2							
EN	n	l	m	g	I	t	F	T	ρ	$D1$	m	g	I	t	F	T	ρ	$D2$
E176	2	88	–	–	–	–	–	–	–	–	2	2	177	1	87	88	87	–
	4	44	–	–	–	–	–	–	–	–	3	4	132	1	43	48	87	39
	8	22	5	16	110	1	21	65	87	22	5	16	110	2	42	61	87	26
	11	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	16	11	9	256	99	2	20	842	87	–	9	256	99	12	127	226	87	–
	22	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	44	4	11	1023	44	6	21	1352	87	–	11	1023	44	42	162	284	87	–
	88	2	11	1023	22	13	22	563	87	–	11	1023	22	57	108	188	87	–
	176	1	11	1023	12	28	23	232	87	–	11	1023	12	77	71	124	87	–
E208	2	104	–	–	–	–	–	–	–	–	2	2	209	1	103	104	103	–
	4	52	–	–	–	–	–	–	–	–	3	4	156	1	51	56	103	47
	8	26	–	–	–	–	–	–	–	–	5	16	130	2	50	69	103	34
	13	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	16	13	9	256	117	1	12	1696	103	–	9	256	117	11	139	249	103	–
	26	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	52	4	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	104	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	208	1	13	4095	14	28	23	1208	103	–	13	4095	14	120	113	307	103	–
E272	2	136	–	–	–	–	–	–	–	–	2	2	273	1	135	136	135	–
	4	68	–	–	–	–	–	–	–	–	3	4	204	1	67	72	135	63
	8	34	–	–	–	–	–	–	–	–	5	16	170	1	33	77	135	58
	16	17	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	17	16	9	255	146	1	15	1691	135	–	9	255	146	10	156	280	135	–
	34	8	9	255	73	3	21	548	135	–	9	255	73	14	107	187	135	–
	68	4	9	256	37	6	21	257	135	–	9	256	37	19	71	123	135	12
	136	2	9	255	19	13	22	110	135	25	9	255	19	26	47	80	135	55
	272	1	9	255	10	28	23	53	135	82	9	255	10	35	30	51	135	84
E304	2	152	–	–	–	–	–	–	–	–	2	2	305	1	151	152	151	–
	4	76	–	–	–	–	–	–	–	–	3	4	228	1	75	80	151	71
	8	38	–	–	–	–	–	–	–	–	5	16	190	1	37	81	151	70
	16	19	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	19	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	38	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	76	4	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	152	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	304	1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E368	2	184	–	–	–	–	–	–	–	–	2	2	369	1	183	184	183	–
	4	92	–	–	–	–	–	–	–	–	3	4	276	1	91	96	183	87
	8	46	–	–	–	–	–	–	–	–	5	16	230	1	45	89	183	94
	16	23	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	23	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	46	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	92	4	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	184	2	12	2047	25	13	22	1287	183	–	12	2047	25	84	161	284	183	–
	368	1	12	2047	13	28	23	529	183	–	12	2047	13	114	107	189	183	–

Table 4: Extended GHS attack data for the ANSI X9.62 elliptic curves.

(ii) E208. Only when allowing a factor base up to 2^{50} elements can we possibly improve on the GHS attack highlighted in Table 3. This is far beyond what is considered feasible today. In addition, finding a curve isogenous to E208 with $(n, m) = (4, 3)$ or $(n, m) = (8, 5)$ among 2^{156} or 2^{130} isomorphism classes, respectively, does not seem feasible.

(iii) E272. The existence of a curve isogenous to E272 with $(n, m) = (136, 9)$ or $(n, m) = (272, 9)$ would considerably improve on Pollard's rho method using the Extended GHS attack. But exhaustive search through the 524288 isomorphism classes of elliptic curves over $\mathbb{F}_{2^{272}}$ with $(n, m) = (136, 9)$ and through the 1276 isomorphism classes of curves over $\mathbb{F}_{2^{272}}$ with $(n, m) = (272, 9)$ showed that none of these curves is isogenous to E272. The next best option would be to find a curve isogenous to E272 with $(n, m) = (8, 5)$. But even if working with a factor base of size 2^{33} were feasible, finding such a curve among the 2^{170} isomorphism classes seems well beyond the realm of feasibility.

(iv) E304. For the same reasons as in the last case for E272, it is not possible to improve on the GHS attack using isogenies.

(v) E368. Same as E304.

7 ECDLP Challenges

We present some cryptographically interesting ECDLP instances that we hope will help stimulate interest in both computational and theoretical work on the ECDLP, Weil descent, and the HCDLP. Appendix B provides details on how the ECDLP instances were generated verifiably at random in such a way that the solutions are not a priori known to us. The ECDLP instances themselves, as well as the hyperelliptic curves and divisors produced by invoking Hess's KASH program [18] for performing the GHS reduction, are presented in Appendix C. The remainder of this section provides rationale for the choice of elliptic curves.

The cryptographically interesting elliptic curves E161, E180, E186, E217, E248 and E300 were specially selected from the class of elliptic curves over $\mathbb{F}_{2^{161}}$, $\mathbb{F}_{2^{180}}$, $\mathbb{F}_{2^{186}}$, $\mathbb{F}_{2^{217}}$, $\mathbb{F}_{2^{248}}$ and $\mathbb{F}_{2^{300}}$, respectively, for which the GHS attack yields HCDLP instances that are within reach of the Enge-Gaudry algorithm. Furthermore, Pollard's rho algorithm for solving the ECDLP on these elliptic curves is infeasible. E186, E217 and E248 are extensions of the E62, E93, E124 and E155 series of elliptic curves analyzed in [21]—these are elliptic curves defined over $\mathbb{F}_{2^{31l}}$ for which the GHS attack yields a genus 31 hyperelliptic curve over $\mathbb{F}_{2^l}$. The low genus of 31 is possible because the multiplicative order of 2 modulo 31 is small (cf. Theorem 8).

Table 5 lists the (n, l, g) GHS attack parameters which yield HCDLP instances that can be solved in $\approx 2^T$ steps using a smoothness bound of t and a factor base of size $\approx 2^F$. Note that $T \ll \rho$, where 2^ρ is the approximate time to solve an ECDLP instance using Pollard's rho algorithm. The Enge-Gaudry parameters (t, F, T) were selected to minimize the running time T subject to the restriction $F \leq 24$ on the factor base size. Table 6 illustrates how the factor base size, expected number of random walk steps ($\approx 2^E$) to find a smooth divisor, and the total expected running time depend on the smoothness bound t. The ECDLP in E161 is expected to be a little easier than the ECDLP in the E155 curve of

Curve	N	n	l	g	t	F	T	ρ
E161	161	7	23	7	1	22	34	80
E180	180	15	12	15	2	22	39	89
E186	186	31	6	31	4	21	41	92
E217	217	31	7	31	3	18	49	108
E248	248	31	8	31	3	21	52	123
E300	300	15	20	15	1	19	59	149
E176	176	88	2	128	13	22	54	87
E272	272	136	2	128	13	22	54	135
E161-2	161	7	23	64	1	22	318	80

Table 5: GHS attack parameters for the challenge curves.

[21] which has $T = 37$. The latter problem was concluded to be tractable in [21] based on experimental data gathered by solving the ECDLP in E62, E93 and E124.

We emphasize that these ECDLP challenge problems may become more tractable if advances are made in index-calculus methods for the HCDLP, or in techniques for solving large systems of sparse linear equations. Another avenue for improvement is applying the Weil descent methodology to efficiently map the ECDLP to the DLP in abelian varieties (not necessarily hyperelliptic) which are easier to solve that the HCDLP instances produced by the GHS attack. For an illustration of this possibility, see [2] where Weil descent is used to reduce the ECDLP in elliptic curves over characteristic 3 finite fields to the DLP in C_{ab} curves. See also [6] for a study on Weil restriction.

The E176 and E272 elliptic curves are from ANSI X9.62. As discussed in §6, the GHS reduction maps these elliptic curves to hyperelliptic curves of genus 128 over $\mathbb{F}_{2^2}$ where the HCDLP is feasible. However, the large prime-order subgroup is mapped to the zero divisor since for both curves, $\mathbb{F}_{2^2}(a, b) = \mathbb{F}_{2^{16}} \neq \mathbb{F}_{q^n}$. It is an open problem whether and how the GHS attack could be modified in this case so that the resulting map does not kill the large prime order subgroup. Diem ([6], Proposition 3.13) shows how Weil descent could be applied to reduce an ECDLP in an elliptic curve $E(\mathbb{F}_{2^{pt}})$ defined over $\mathbb{F}_{2^t}$ to a DLP in the group $\mathrm{Cl}^0(C)$ of divisor classes of degree zero of a curve C of genus $\leq 2^{2t} - 1$ defined over $\mathbb{F}_{2^{2t}}$. Here p is an odd prime, and $t = \mathrm{ord}_2(p)$ denotes the order of 2 modulo p. For example, an elliptic curve over $\mathbb{F}_{2^{136}}$ defined over $\mathbb{F}_{2^8}$ could be transformed to the DLP in $\mathrm{Cl}^0(C)$ of a curve C of genus $\leq 2^{16} - 1$ defined over $\mathbb{F}_{2^{16}}$; however, Diem's result does not apply to E176 or E272.

Finally, the E161-2 elliptic curve was generated at random from the set of all cryptographically interesting elliptic curves over $\mathbb{F}_{2^{161}}$ (see Appendix B). The GHS reduction yielded $(m, g) = (7, 64)$ for $(n, l) = (7, 23)$, $m = 23$ for $(n, l) = (23, 7)$, and $m = 158$ for $(n, l) = (161, 1)$. All three resulting HCDLPs are outside the realm of feasibility of the Enge-Gaudry algorithm. However, from the results in [13] (cf. Remark 19), it is likely that there exists an elliptic curve E' over $\mathbb{F}_{2^{161}}$ that is isogenous to E161-2, and for which the GHS reduction produces a hyperelliptic curve of genus 7 over $\mathbb{F}_{2^{23}}$ in which the HCDLP is feasible. If such an elliptic curve E' can be found (this is no easy task since there are approximately 2^{94} isomorphism classes of elliptic curves over $\mathbb{F}_{2^{161}}$ with $m = 4$ for $n = 7$), then the isogeny could be computed using the algorithm in [13].

E161															
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F	22	44	66	89	112	134	157	180	203	226	249	271	294	317	340
E	12	4	2	1	1	0	0	0	0	0	0	0	0	0	0
T	34	48	68	90	112	135	157	180	203	226	249	271	294	317	340
E180															
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F	11	22	33	45	57	68	80	92	104	116	128	139	151	163	175
E	40	17	9	6	4	3	2	1	1	1	1	0	0	0	0
T	51	39	43	51	61	71	82	93	105	116	128	140	152	163	175
E186															
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F	5	10	15	21	27	32	38	44	50	56	62	67	73	79	85
E	109	51	30	20	15	11	8	7	5	4	4	3	3	2	2
T	114	61	46	41	41	43	47	51	55	60	65	70	76	81	87
E217															
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F	6	12	18	25	32	38	45	52	59	66	73	79	86	93	100
E	112	51	30	20	15	11	8	7	5	4	4	3	3	2	2
T	118	63	49	45	46	49	54	59	64	70	76	82	89	95	102
E248															
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F	7	14	21	29	37	44	52	60	68	76	84	91	99	107	115
E	112	51	30	20	15	11	8	7	5	4	4	3	3	2	2
T	119	65	52	49	51	55	61	67	73	80	87	94	102	109	117
E300															
t	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
F	19	38	57	77	97	116	136	156	176	196	216	235	255	275	295
E	40	17	9	6	4	3	2	1	1	1	1	0	0	0	0
T	59	55	67	83	101	119	138	157	177	196	216	236	256	275	295

Table 6: Some Enge-Gaudry parameters for the challenge curves.

8 Conclusions

We analyzed the GHS Weil descent attack on the ECDLP for elliptic curves defined over characteristic two finite fields $\mathbb{F}_{2^N}$ of composite extension degree $N \in [100, 600]$. For some such fields, there are cryptographically interesting elliptic curves over $\mathbb{F}_{2^N}$ where the ECDLP succumbs to the GHS attack. We provided ECDLP "challenges" over six such fields: $\mathbb{F}_{2^{161}}$, $\mathbb{F}_{2^{180}}$, $\mathbb{F}_{2^{186}}$, $\mathbb{F}_{2^{217}}$, $\mathbb{F}_{2^{248}}$ and $\mathbb{F}_{2^{300}}$. For other such fields $\mathbb{F}_{2^N}$, our results demonstrate that there are no cryptographically interesting elliptic curves over $\mathbb{F}_{2^N}$ for which the GHS attack yields an ECDLP solver that is faster than Pollard's rho method. Our analysis suggests that the five elliptic curves over $\mathbb{F}_{2^{176}}$, $\mathbb{F}_{2^{208}}$, $\mathbb{F}_{2^{272}}$, $\mathbb{F}_{2^{304}}$ and $\mathbb{F}_{2^{368}}$ in ANSI X9.62 resist the GHS attack.

We stress that any statement we have made regarding the failure of the GHS attack on some elliptic curves over some field $\mathbb{F}_{2^N}$ is dependent on the assumption that the Enge-Gaudry algorithm cannot be significantly improved, and, in particular, that the linear algebra stage is intractable if the factor base size is greater than 10^7. Also, we stress that failure of the GHS attack does not imply failure of the Weil descent methodology—there may be other useful curves which lie on the Weil restriction $W_{E/k}$ that were not constructed by the GHS method. We thus hope that our work can serve as a stimulus for further work on the Weil descent method, on subexponential-time index-calculus methods for the HCDLP, and on algorithms for solving large systems of sparse linear equations.

Acknowledgements

We used KASH, Magma, Maple and NTL in our work. We would like to thank Antoine Joux, Steven Galbraith, Florian Hess and Nigel Smart for their helpful advice and comments. We would also like to thank NSERC for providing partial funding for this research.

References

[1] ANSI X9.62, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)*, 1999.

[2] S. Arita, "Weil descent of elliptic curves over finite fields of characteristic three", *Advances in Cryptology–Asiacrypt 2000*, LNCS **1976**, 2000, 248-259.

[3] E. Artin. "Quadratische Körper im Gebiete der höheren Kongruenzen", *Mathematische Zeitschrift*, **19** (1924), 207-246.

[4] D. Cantor, "Computing in the jacobian of a hyperelliptic curve", *Mathematics of Computation*, **48** (1987), 95-101.

[5] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig and K. Wildanger, "KANT V4", *Journal of Symbolic Computation*, **24** (1997), 267-283.

[6] C. Diem, *A Study on Theoretical and Practical Aspects of Weil-Restrictions of Varieties*, Ph.D. thesis, University of Essen, 2001.

[7] A. Enge and P. Gaudry, "A general framework for subexponential discrete logarithm algorithms", *Acta Arithmetica*, to appear.

[8] M. Fouquet, P. Gaudry and R. Harley, "An extension of Satoh's algorithm and its implementation", *Journal of the Ramanujan Mathematical Society*, **15** (2000), 281-318.

[9] G. Frey, "How to disguise an elliptic curve (Weil descent)", Talk at ECC '98, Waterloo, 1998. Slides available from http://www.cacr.math.uwaterloo.ca/conferences/1998/ecc98/slides.html

[10] G. Frey, "Applications of arithmetical geometry to cryptographic constructions", *Proceedings of the Fifth International Conference on Finite Fields and Applications*, Springer-Verlag, 2001, 128-161.

[11] G. Frey and H. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of Computation*, **62** (1994), 865-874.

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

[13] S. Galbraith, F. Hess and N. Smart, "Extending the GHS Weil descent attack", preprint, 2001.

[14] S. Galbraith and N. Smart, "A cryptographic application of Weil descent", *Codes and Cryptography*, LNCS **1746**, 1999, 191-200.

[15] R. Gallant, R. Lambert and S. Vanstone, "Improving the parallelized Pollard lambda search on anomalous binary curves", *Mathematics of Computation*, **69** (2000), 1699-1705.

[16] P. Gaudry, "An algorithm for solving the discrete log problem on hyperelliptic curves", *Advances in Cryptology–Eurocrypt 2000*, LNCS **1807**, 2000, 19-34.

[17] P. Gaudry, F. Hess and N. Smart, "Constructive and destructive facets of Weil descent on elliptic curves", *Journal of Cryptology*, to appear.

[18] F. Hess, KASH program for performing the GHS attack, 2000.

[19] F. Hess. Personal communication. September 2001.

[20] Internet Engineering Task Force, *The OAKLEY Key Determination Protocol*, IETF RFC 2412, November 1998.

[21] M. Jacobson, A. Menezes and A. Stein, "Solving elliptic curve discrete logarithm problems using Weil descent", *Journal of the Ramanujan Mathematical Society*, to appear.

[22] A. Joux. Personal communication. June 2001.

[23] A. Joux and R. Lercier, "Improvements on the general number field sieve for discrete logarithms in finite fields", *Mathematics of Computation*, to appear.

[24] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *IEEE Transactions on Information Theory*, **39** (1993), 1639-1646.

[25] A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[26] A. Menezes and M. Qu, "Analysis of the Weil descent attack of Gaudry, Hess and Smart", *Topics in Cryptology–CT-RSA 2001*, LNCS **2020**, 2001, 308-318.

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

[28] S. Paulus and H. Rück, "Real and imaginary quadratic representations of hyperelliptic function fields", *Mathematics of Computation*, **68** (1999), 1233-1241.

[29] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance", *IEEE Transactions on Information Theory*, **24** (1978), 106-110.

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

[31] T. Satoh, "The canonical lift of an ordinary elliptic curve over a finite field and its point counting", *Journal of the Ramanujan Mathematical Society*, **15** (2000), 247-270.

[32] N. Smart, "How secure are elliptic curves over composite extension fields?", *Advances in Cryptology–Eurocrypt 2001*, LNCS **2045**, 2001.

[33] E. Teske, "Speeding up Pollard's rho method for computing discrete logarithms", *Algorithmic Number Theory*, LNCS **1423**, 1998, 541-554.

[34] M. Wiener and R. Zuccherato, "Faster attacks on elliptic curve cryptosystems", *Selected Areas in Cryptography*, LNCS **1556**, 1999, 190-200.

A Results of our Analysis

For an explanation of the notation used in the following tables, see §5.

N	$EG1$										$EG2$									
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
100	100	1	8	127	8	23	19	32	49	17	4	25	3	4	75	1	24	29	49	20
102	6	17	4	7	69	1	16	28	50	22	6	17	4	7	69	1	16	28	50	22
104	8	13	5	16	65	1	12	56	51	–	4	26	3	4	78	1	25	30	51	21
105	7	15	4	7	62	1	14	26	52	26	7	15	4	7	62	1	14	26	52	26
106	–	–	–	–	–	–	–	–	–	–	2	53	2	2	107	1	52	53	52	–
108	36	3	6	32	19	6	15	26	53	27	36	3	6	32	19	6	15	26	53	27
110	10	11	5	15	55	2	20	37	54	17	10	11	5	15	55	2	20	37	54	17
111	–	–	–	–	–	–	–	–	–	–	3	37	3	3	112	1	36	39	55	16
112	7	16	4	7	66	1	15	27	55	28	7	16	4	7	66	1	15	27	55	28
114	6	19	4	7	77	1	18	30	56	26	6	19	4	7	77	1	18	30	56	26
115	5	23	5	15	116	1	22	62	57	–	5	23	5	15	116	2	44	61	57	–
116	–	–	–	–	–	–	–	–	–	–	4	29	3	4	87	1	28	33	57	24
117	117	1	9	255	10	28	23	53	58	5	3	39	3	3	118	1	38	41	58	17
118	–	–	–	–	–	–	–	–	–	–	2	59	2	2	119	1	58	59	58	–
119	7	17	4	7	70	1	16	28	59	31	7	17	4	7	70	1	16	28	59	31
120	6	20	4	7	81	1	19	31	59	28	6	20	4	7	81	1	19	31	59	28
121	121	1	11	1023	12	28	23	232	60	–	121	1	11	1023	12	77	71	124	60	–
122	–	–	–	–	–	–	–	–	–	–	2	61	2	2	123	1	60	61	60	–
123	–	–	–	–	–	–	–	–	–	–	3	41	3	3	124	1	40	43	61	18
124	31	4	6	31	28	5	17	31	61	30	31	4	6	31	28	5	17	31	61	30
125	–	–	–	–	–	–	–	–	–	–	5	25	5	15	126	1	24	64	62	–
126	7	18	4	7	74	1	17	29	62	33	7	18	4	7	74	1	17	29	62	33
128	8	16	5	16	80	1	15	59	63	4	4	32	3	4	96	1	31	36	63	27
129	–	–	–	–	–	–	–	–	–	–	3	43	3	3	130	1	42	45	64	19
130	10	13	5	15	65	1	12	52	64	12	10	13	5	15	65	2	24	41	64	23
132	132	1	8	127	8	23	19	32	65	33	132	1	8	127	8	23	19	32	65	33
133	7	19	4	7	78	1	18	30	66	36	7	19	4	7	78	1	18	30	66	36
134	–	–	–	–	–	–	–	–	–	–	2	67	2	2	135	1	66	67	66	–
135	15	9	5	15	48	2	16	33	67	34	15	9	5	15	48	2	16	33	67	34
136	136	1	9	255	10	28	23	53	67	14	4	34	3	4	102	1	33	38	67	29
138	6	23	4	7	93	1	22	34	68	34	6	23	4	7	93	1	22	34	68	34
140	7	20	4	7	82	1	19	31	69	38	7	20	4	7	82	1	19	31	69	38
141	–	–	–	–	–	–	–	–	–	–	3	47	3	3	142	1	46	49	70	21
142	–	–	–	–	–	–	–	–	–	–	2	71	2	2	143	1	70	71	70	–
143	143	1	11	1023	12	28	23	232	71	–	143	1	11	1023	12	77	71	124	71	–
144	72	2	7	64	16	11	18	32	71	39	72	2	7	64	16	11	18	32	71	39
145	–	–	–	–	–	–	–	–	–	–	5	29	5	15	146	1	28	68	72	4
146	146	1	10	512	13	28	23	106	72	–	2	73	2	2	147	1	72	73	72	–
147	7	21	4	7	86	1	20	32	73	41	7	21	4	7	86	1	20	32	73	41
148	–	–	–	–	–	–	–	–	–	–	4	37	3	4	111	1	36	41	73	32
150	15	10	5	15	53	2	18	35	74	39	15	10	5	15	53	2	18	35	74	39
152	8	19	5	16	95	1	18	62	75	13	4	38	3	4	114	1	37	42	75	33
153	153	1	9	255	13	28	23	53	76	23	153	1	9	255	13	35	30	51	76	25
154	7	22	4	7	90	1	21	33	76	43	7	22	4	7	90	1	21	33	76	43

N	$EG1$										$EG2$									
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
155	31	5	6	31	34	5	22	36	77	41	31	5	6	31	34	5	22	36	77	41
156	12	13	5	15	66	1	12	52	77	25	6	26	4	7	105	1	25	37	77	40
158	–	–	–	–	–	–	–	–	–	–	2	79	2	2	159	1	78	79	78	–
159	–	–	–	–	–	–	–	–	–	–	3	53	3	3	160	1	52	55	79	24
160	20	8	6	31	48	3	21	52	79	27	4	40	3	4	120	1	39	44	79	35
161	7	23	4	7	94	1	22	34	80	46	7	23	4	7	94	1	22	34	80	46
162	54	3	7	63	21	9	23	42	80	38	6	27	4	7	109	1	26	38	80	42
164	–	–	–	–	–	–	–	–	–	–	4	41	3	4	123	1	40	45	81	36
165	15	11	5	15	58	2	20	37	82	45	15	11	5	15	58	2	20	37	82	45
166	–	–	–	–	–	–	–	–	–	–	2	83	2	2	167	1	82	83	82	–
168	7	24	4	7	98	1	23	35	83	48	7	24	4	7	98	1	23	35	83	48
169	169	1	13	4095	14	28	23	1208	84	–	169	1	13	4095	14	120	113	307	84	–
170	170	1	9	255	12	28	23	53	84	31	10	17	5	15	85	2	32	49	84	35
171	171	1	9	255	10	28	23	53	85	32	171	1	9	255	10	35	30	51	85	34
172	–	–	–	–	–	–	–	–	–	–	4	43	3	4	129	1	42	47	85	38
174	–	–	–	–	–	–	–	–	–	–	6	29	4	7	117	1	28	40	86	46
175	35	5	7	63	36	5	22	65	87	22	7	25	4	7	102	1	24	36	87	51
176	8	22	5	16	110	1	21	65	87	22	4	44	3	4	132	1	43	48	87	39
177	–	–	–	–	–	–	–	–	–	–	3	59	3	3	178	1	58	61	88	27
178	178	1	12	2047	15	28	23	529	88	–	2	89	2	2	179	1	88	89	88	–
180	15	12	5	15	63	2	22	39	89	50	15	12	5	15	63	2	22	39	89	50
182	14	13	5	15	67	1	12	52	90	38	7	26	4	7	106	1	25	37	90	53
183	–	–	–	–	–	–	–	–	–	–	3	61	3	3	184	1	60	63	91	28
184	8	23	5	16	115	1	22	66	91	25	4	46	3	4	138	1	45	50	91	41
185	–	–	–	–	–	–	–	–	–	–	5	37	5	15	186	1	36	76	92	16
186	31	6	6	31	40	4	21	41	92	51	31	6	6	31	40	5	27	41	92	51
187	187	1	9	255	11	28	23	53	93	40	187	1	9	255	11	35	30	51	93	42
188	–	–	–	–	–	–	–	–	–	–	4	47	3	4	141	1	46	51	93	42
189	63	3	7	63	25	9	23	42	94	52	7	27	4	7	110	1	26	38	94	56
190	190	1	9	255	9	28	23	53	94	41	190	1	9	255	9	35	30	51	94	43
192	24	8	6	31	50	3	21	52	95	43	6	32	4	7	129	1	31	43	95	52
194	–	–	–	–	–	–	–	–	–	–	2	97	2	2	195	1	96	97	96	–
195	15	13	5	15	68	1	12	52	97	45	15	13	5	15	68	2	24	41	97	56
196	28	7	6	31	43	3	18	49	97	48	7	28	4	7	114	1	27	39	97	58
198	198	1	9	255	9	28	23	53	98	45	6	33	4	7	133	1	32	44	98	54
200	200	1	9	255	9	28	23	53	99	46	100	2	8	127	17	17	29	51	99	48
201	–	–	–	–	–	–	–	–	–	–	3	67	3	3	202	1	66	69	100	31
202	–	–	–	–	–	–	–	–	–	–	2	101	2	2	203	1	100	101	100	–
203	–	–	–	–	–	–	–	–	–	–	7	29	4	7	118	1	28	40	101	61
204	204	1	9	255	12	28	23	53	101	48	6	34	4	7	137	1	33	45	101	56
205	–	–	–	–	–	–	–	–	–	–	5	41	5	15	206	1	40	80	102	22
206	–	–	–	–	–	–	–	–	–	–	2	103	2	2	207	1	102	103	102	–
207	207	1	9	255	10	28	23	53	103	50	207	1	9	255	10	35	30	51	103	52
208	208	1	13	4095	14	28	23	1208	103	–	4	52	3	4	156	1	51	56	103	47
209	209	1	11	1023	12	28	23	232	104	–	209	1	11	1023	12	77	71	124	104	–
210	30	7	6	31	45	3	18	49	104	55	7	30	4	7	122	1	29	41	104	63
212	–	–	–	–	–	–	–	–	–	–	4	53	3	4	159	1	52	57	105	48

N	$EG1$										$EG2$									
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
213	–	–	–	–	–	–	–	–	–	–	3	71	3	3	214	1	70	73	106	33
214	–	–	–	–	–	–	–	–	–	–	2	107	2	2	215	1	106	107	106	–
215	–	–	–	–	–	–	–	–	–	–	5	43	5	15	216	1	42	82	107	25
216	216	1	9	255	11	28	23	53	107	54	6	36	4	7	145	1	35	47	107	60
217	31	7	6	31	46	3	18	49	108	59	7	31	4	7	126	1	30	42	108	66
218	–	–	–	–	–	–	–	–	–	–	2	109	2	2	219	1	108	109	108	–
219	219	1	10	511	14	28	23	105	109	4	3	73	3	3	220	1	72	75	109	34
220	220	1	9	255	9	28	23	53	109	56	220	1	9	255	9	35	30	51	109	58
221	221	1	9	255	11	28	23	53	110	57	221	1	9	255	11	35	30	51	110	59
222	–	–	–	–	–	–	–	–	–	–	6	37	4	7	149	1	36	48	110	62
224	28	8	6	31	49	3	21	52	111	59	7	32	4	7	130	1	31	43	111	68
225	225	1	9	255	12	28	23	53	112	59	15	15	5	15	78	2	28	45	112	67
226	–	–	–	–	–	–	–	–	–	–	2	113	2	2	227	1	112	113	112	–
228	228	1	9	255	9	28	23	53	113	60	6	38	4	7	153	1	37	49	113	64
230	230	1	9	255	9	28	23	53	114	61	230	1	9	255	9	35	30	51	114	63
231	231	1	9	255	11	28	23	53	115	62	7	33	4	7	134	1	32	44	115	71
232	–	–	–	–	–	–	–	–	–	–	4	58	3	4	174	1	57	62	115	53
234	234	1	9	255	9	28	23	53	116	63	6	39	4	7	157	1	38	50	116	66
235	–	–	–	–	–	–	–	–	–	–	5	47	5	15	236	1	46	86	117	31
236	–	–	–	–	–	–	–	–	–	–	4	59	3	4	177	1	58	63	117	54
237	–	–	–	–	–	–	–	–	–	–	3	79	3	3	238	1	78	81	118	37
238	238	1	9	255	10	28	23	53	118	65	7	34	4	7	138	1	33	45	118	73
240	30	8	6	31	51	3	21	52	119	67	15	16	5	15	83	2	30	47	119	72
242	242	1	11	1023	11	28	23	232	120	–	2	121	2	2	243	1	120	121	120	–
243	243	1	9	255	10	28	23	53	121	68	243	1	9	255	10	35	30	51	121	70
244	–	–	–	–	–	–	–	–	–	–	4	61	3	4	183	1	60	65	121	56
245	49	5	7	63	36	5	22	65	122	57	7	35	4	7	142	1	34	46	122	76
246	–	–	–	–	–	–	–	–	–	–	6	41	4	7	165	1	40	52	122	70
247	247	1	13	4095	14	28	23	1208	123	–	247	1	13	4095	14	120	113	307	123	–
248	31	8	6	31	52	3	21	52	123	71	31	8	6	31	52	4	29	49	123	74
249	–	–	–	–	–	–	–	–	–	–	3	83	3	3	250	1	82	85	124	39
250	250	1	9	255	9	28	23	53	124	71	250	1	9	255	9	35	30	51	124	73
252	252	1	9	255	13	28	23	53	125	72	7	36	4	7	146	1	35	47	125	78
253	253	1	11	1023	12	28	23	232	126	–	253	1	11	1023	12	77	71	124	126	2
254	254	1	9	255	13	28	23	53	126	73	127	2	8	127	21	17	29	51	126	75
255	255	1	9	255	15	28	23	53	127	74	15	17	5	15	88	2	32	49	127	78
256	256	1	9	255	8	28	23	53	127	74	256	1	9	255	8	35	30	51	127	76
258	–	–	–	–	–	–	–	–	–	–	6	43	4	7	173	1	42	54	128	74
259	–	–	–	–	–	–	–	–	–	–	7	37	4	7	150	1	36	48	129	81
260	260	1	9	255	9	28	23	53	129	76	260	1	9	255	9	35	30	51	129	78
261	261	1	9	255	10	28	23	53	130	77	261	1	9	255	10	35	30	51	130	79
262	–	–	–	–	–	–	–	–	–	–	2	131	2	2	263	1	130	131	130	–
264	264	1	9	255	10	28	23	53	131	78	132	2	8	127	17	17	29	51	131	80
265	–	–	–	–	–	–	–	–	–	–	5	53	5	15	266	1	52	92	132	40
266	14	19	5	15	97	1	18	58	132	74	7	38	4	7	154	1	37	49	132	83
267	267	1	12	2047	16	28	23	529	133	–	3	89	3	3	268	1	88	91	133	42
268	–	–	–	–	–	–	–	–	–	–	4	67	3	4	201	1	66	71	133	62

	$EG1$										$EG2$									
N	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
270	270	1	9	255	12	28	23	53	134	81	15	18	5	15	93	2	34	51	134	83
272	272	1	9	255	10	28	23	53	135	82	272	1	9	255	10	35	30	51	135	84
273	273	1	9	255	11	28	23	53	136	83	7	39	4	7	158	1	38	50	136	86
274	–	–	–	–	–	–	–	–	–	–	2	137	2	2	275	1	136	137	136	–
275	275	1	11	1023	12	28	23	232	137	–	5	55	5	15	276	1	54	94	137	43
276	276	1	9	256	9	28	23	53	137	84	276	1	9	256	9	35	30	51	137	86
278	–	–	–	–	–	–	–	–	–	–	2	139	2	2	279	1	138	139	138	–
279	31	9	6	31	58	2	16	67	139	72	31	9	6	31	58	4	33	53	139	86
280	14	20	5	15	102	1	19	59	139	80	7	40	4	7	162	1	39	51	139	88
282	–	–	–	–	–	–	–	–	–	–	6	47	4	7	189	1	46	58	140	82
284	–	–	–	–	–	–	–	–	–	–	4	71	3	4	213	1	70	75	141	66
285	15	19	5	15	98	1	18	58	142	84	15	19	5	15	98	2	36	53	142	89
286	286	1	11	1023	11	28	23	232	142	–	286	1	11	1023	11	77	71	124	142	18
287	–	–	–	–	–	–	–	–	–	–	7	41	4	7	166	1	40	52	143	91
288	12	24	5	15	121	1	23	63	143	80	6	48	4	7	193	1	47	59	143	84
289	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
290	290	1	10	511	10	28	23	105	144	39	10	29	5	15	145	1	28	68	144	76
291	–	–	–	–	–	–	–	–	–	–	3	97	3	3	292	1	96	99	145	46
292	292	1	10	511	13	28	23	105	145	40	4	73	3	4	219	1	72	77	145	68
294	14	21	5	15	107	1	20	60	146	86	7	42	4	7	170	1	41	53	146	93
295	–	–	–	–	–	–	–	–	–	–	5	59	5	15	296	1	58	98	147	49
296	–	–	–	–	–	–	–	–	–	–	4	74	3	4	222	1	73	78	147	69
297	27	11	7	63	78	2	20	157	148	–	27	11	7	63	78	5	52	95	148	53
298	–	–	–	–	–	–	–	–	–	–	2	149	2	2	299	1	148	149	148	–
299	299	1	12	2047	14	28	23	529	149	–	299	1	12	2047	14	114	107	189	149	–
300	15	20	5	15	103	1	19	59	149	90	15	20	5	15	103	2	38	55	149	94
301	–	–	–	–	–	–	–	–	–	–	7	43	4	7	174	1	42	54	150	96
302	–	–	–	–	–	–	–	–	–	–	2	151	2	2	303	1	150	151	150	–
303	–	–	–	–	–	–	–	–	–	–	3	101	3	3	304	1	100	103	151	48
304	–	–	–	–	–	–	–	–	–	–	4	76	3	4	228	1	75	80	151	71
305	–	–	–	–	–	–	–	–	–	–	5	61	5	15	306	1	60	100	152	52
306	306	1	10	511	13	28	23	105	152	47	6	51	4	7	205	1	50	62	152	90
308	14	22	5	15	112	1	21	61	153	92	7	44	4	7	178	1	43	55	153	98
309	–	–	–	–	–	–	–	–	–	–	3	103	3	3	310	1	102	105	154	49
310	62	5	7	63	39	5	22	65	154	89	31	10	6	31	64	4	37	57	154	97
312	312	1	10	511	11	28	23	105	155	50	6	52	4	7	209	1	51	63	155	92
314	–	–	–	–	–	–	–	–	–	–	2	157	2	2	315	1	156	157	156	–
315	15	21	5	15	108	1	20	60	157	97	7	45	4	7	182	1	44	56	157	101
316	–	–	–	–	–	–	–	–	–	–	4	79	3	4	237	1	78	83	157	74
318	–	–	–	–	–	–	–	–	–	–	6	53	4	7	213	1	52	64	158	94
319	319	1	11	1023	12	28	23	232	159	–	319	1	11	1023	12	77	71	124	159	35
320	320	1	10	511	11	28	23	105	159	54	10	32	5	15	160	1	31	71	159	88
321	–	–	–	–	–	–	–	–	–	–	3	107	3	3	322	1	106	109	160	51
322	14	23	5	15	117	1	22	62	160	98	7	46	4	7	186	1	45	57	160	103
323	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
324	108	3	8	127	26	9	23	77	161	84	6	54	4	7	217	1	53	65	161	96
325	325	1	13	4095	16	28	23	1208	162	–	5	65	5	15	326	1	64	104	162	58

	$EG1$										$EG2$									
N	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
326	–	–	–	–	–	–	–	–	–	–	2	163	2	2	327	1	162	163	162	–
327	–	–	–	–	–	–	–	–	–	–	3	109	3	3	328	1	108	111	163	52
328	–	–	–	–	–	–	–	–	–	–	8	41	5	16	205	1	40	84	163	79
329	–	–	–	–	–	–	–	–	–	–	7	47	4	7	190	1	46	58	164	106
330	15	22	5	15	113	1	21	61	164	103	15	22	5	15	113	2	42	59	164	105
332	–	–	–	–	–	–	–	–	–	–	4	83	3	4	249	1	82	87	165	78
333	–	–	–	–	–	–	–	–	–	–	3	111	3	3	334	1	110	113	166	53
334	–	–	–	–	–	–	–	–	–	–	2	167	2	2	335	1	166	167	166	–
335	–	–	–	–	–	–	–	–	–	–	5	67	5	15	336	1	66	106	167	61
336	14	24	5	15	122	1	23	63	167	104	7	48	4	7	194	1	47	59	167	108
338	338	1	13	4095	13	28	23	1208	168	–	2	169	2	2	339	1	168	169	168	–
339	–	–	–	–	–	–	–	–	–	–	3	113	3	3	340	1	112	115	169	54
340	340	1	10	511	12	28	23	105	169	64	10	34	5	15	170	1	33	73	169	96
341	31	11	6	31	70	2	20	71	170	99	31	11	6	31	70	3	30	61	170	109
342	342	1	10	511	10	28	23	105	170	65	6	57	4	7	229	1	56	68	170	102
343	49	7	7	63	50	3	18	103	171	68	7	49	4	7	198	1	48	60	171	111
344	–	–	–	–	–	–	–	–	–	–	8	43	5	16	215	1	42	86	171	85
345	15	23	5	15	118	1	22	62	172	110	15	23	5	15	118	2	44	61	172	111
346	–	–	–	–	–	–	–	–	–	–	2	173	2	2	347	1	172	173	172	–
348	348	1	10	511	10	28	23	105	173	68	12	29	5	15	146	1	28	68	173	105
350	350	1	10	511	11	28	23	105	174	69	7	50	4	7	202	1	49	61	174	113
351	117	3	9	255	28	9	23	165	175	10	117	3	9	255	28	22	61	103	175	72
352	352	1	11	1023	12	28	23	232	175	–	8	44	5	16	220	1	43	87	175	88
354	–	–	–	–	–	–	–	–	–	–	6	59	4	7	237	1	58	70	176	106
355	–	–	–	–	–	–	–	–	–	–	5	71	5	15	356	1	70	110	177	67
356	356	1	12	2047	15	28	23	529	177	–	4	89	3	4	267	1	88	93	177	84
357	357	1	10	511	13	28	23	105	178	73	7	51	4	7	206	1	50	62	178	116
358	–	–	–	–	–	–	–	–	–	–	2	179	2	2	359	1	178	179	178	–
360	15	24	5	15	123	1	23	63	179	116	15	24	5	15	123	2	46	63	179	116
361	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
362	–	–	–	–	–	–	–	–	–	–	2	181	2	2	363	1	180	181	180	–
363	363	1	11	1023	14	28	23	232	181	–	3	121	3	3	364	1	120	123	181	58
364	364	1	10	511	13	28	23	105	181	76	7	52	4	7	210	1	51	63	181	118
365	365	1	10	511	14	28	23	105	182	77	365	1	10	511	14	52	46	80	182	102
366	–	–	–	–	–	–	–	–	–	–	6	61	4	7	245	1	60	72	182	110
368	368	1	12	2047	13	28	23	529	183	–	8	46	5	16	230	1	45	89	183	94
369	–	–	–	–	–	–	–	–	–	–	3	123	3	3	370	1	122	125	184	59
370	370	1	10	511	10	28	23	105	184	79	10	37	5	15	185	1	36	76	184	108
371	–	–	–	–	–	–	–	–	–	–	7	53	4	7	214	1	52	64	185	121
372	31	12	6	31	76	2	22	73	185	112	31	12	6	31	76	3	33	64	185	121
374	374	1	10	511	11	28	23	105	186	81	187	2	9	255	20	26	47	80	186	106
375	375	1	11	1023	13	28	23	232	187	–	15	25	5	15	128	1	24	64	187	123
376	–	–	–	–	–	–	–	–	–	–	8	47	5	16	235	1	46	90	187	97
377	377	1	13	4095	14	28	23	1208	188	–	377	1	13	4095	14	120	113	307	188	–
378	126	3	8	127	29	9	23	77	188	111	7	54	4	7	218	1	53	65	188	123
380	380	1	10	511	9	28	23	105	189	84	10	38	5	15	190	1	37	77	189	112
381	127	3	8	127	29	9	23	77	190	113	127	3	8	127	29	14	37	66	190	124

	EG1										EG2									
N	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
382	–	–	–	–	–	–	–	–	–	–	2	191	2	2	383	1	190	191	190	–
384	384	1	10	511	11	28	23	105	191	86	12	32	5	15	161	1	31	71	191	120
385	35	11	7	63	78	2	20	157	192	35	7	55	4	7	222	1	54	66	192	126
386	–	–	–	–	–	–	–	–	–	–	2	193	2	2	387	1	192	193	192	–
387	–	–	–	–	–	–	–	–	–	–	3	129	3	3	388	1	128	131	193	62
388	–	–	–	–	–	–	–	–	–	–	4	97	3	4	291	1	96	101	193	92
390	390	1	10	511	13	28	23	105	194	89	15	26	5	15	133	1	25	65	194	129
391	391	1	12	2047	14	28	23	529	195	–	391	1	12	2047	14	114	107	189	195	6
392	56	7	7	63	52	3	18	103	195	92	7	56	4	7	226	1	55	67	195	128
393	–	–	–	–	–	–	–	–	–	–	3	131	3	3	394	1	130	133	196	63
394	–	–	–	–	–	–	–	–	–	–	2	197	2	2	395	1	196	197	196	–
395	–	–	–	–	–	–	–	–	–	–	5	79	5	15	396	1	78	118	197	79
396	132	3	8	127	25	9	23	77	197	120	132	3	8	127	25	14	37	66	197	131
398	–	–	–	–	–	–	–	–	–	–	2	199	2	2	399	1	198	199	198	–
399	399	1	10	511	13	28	23	105	199	94	7	57	4	7	230	1	56	68	199	131
400	400	1	10	511	11	28	23	105	199	94	10	40	5	15	200	1	39	79	199	120
402	–	–	–	–	–	–	–	–	–	–	6	67	4	7	269	1	66	78	200	122
403	31	13	6	31	82	1	12	125	201	76	31	13	6	31	82	3	36	67	201	134
404	–	–	–	–	–	–	–	–	–	–	4	101	3	4	303	1	100	105	201	96
405	45	9	7	63	66	2	16	153	202	49	15	27	5	15	138	1	26	66	202	136
406	406	1	10	511	11	28	23	105	202	97	14	29	5	15	147	1	28	68	202	134
407	407	1	11	1023	12	28	23	232	203	–	407	1	11	1023	12	77	71	124	203	79
408	408	1	10	511	12	28	23	105	203	98	12	34	5	15	171	1	33	73	203	130
410	410	1	10	511	10	28	23	105	204	99	10	41	5	15	205	1	40	80	204	124
411	–	–	–	–	–	–	–	–	–	–	3	137	3	3	412	1	136	139	205	66
412	–	–	–	–	–	–	–	–	–	–	4	103	3	4	309	1	102	107	205	98
413	–	–	–	–	–	–	–	–	–	–	7	59	4	7	238	1	58	70	206	136
414	414	1	10	511	10	28	23	105	206	101	6	69	4	7	277	1	68	80	206	126
415	–	–	–	–	–	–	–	–	–	–	5	83	5	15	416	1	82	122	207	85
416	416	1	13	4095	14	28	23	1208	207	–	8	52	5	16	260	1	51	95	207	112
417	–	–	–	–	–	–	–	–	–	–	3	139	3	3	418	1	138	141	208	67
418	418	1	11	1023	11	28	23	232	208	–	418	1	11	1023	11	77	71	124	208	84
420	60	7	7	63	52	3	18	103	209	106	15	28	5	15	143	1	27	67	209	142
422	–	–	–	–	–	–	–	–	–	–	2	211	2	2	423	1	210	211	210	–
423	–	–	–	–	–	–	–	–	–	–	3	141	3	3	424	1	140	143	211	68
424	–	–	–	–	–	–	–	–	–	–	8	53	5	16	265	1	52	96	211	115
425	85	5	9	255	49	5	22	315	212	–	5	85	5	15	426	1	84	124	212	88
426	–	–	–	–	–	–	–	–	–	–	6	71	4	7	285	1	70	82	212	130
427	–	–	–	–	–	–	–	–	–	–	7	61	4	7	246	1	60	72	213	141
428	–	–	–	–	–	–	–	–	–	–	4	107	3	4	321	1	106	111	213	102
429	429	1	11	1023	14	28	23	232	214	–	429	1	11	1023	14	77	71	124	214	90
430	430	1	10	511	10	28	23	105	214	109	430	1	10	511	10	52	46	80	214	134
432	432	1	10	511	12	28	23	105	215	110	12	36	5	15	181	1	35	75	215	140
434	62	7	7	63	53	3	18	103	216	113	14	31	5	15	157	1	30	70	216	146
435	435	1	11	1023	13	28	23	232	217	–	15	29	5	15	148	1	28	68	217	149
436	–	–	–	–	–	–	–	–	–	–	4	109	3	4	327	1	108	113	217	104
437	437	1	12	2047	14	28	23	529	218	–	437	1	12	2047	14	114	107	189	218	29

N	$EG1$										$EG2$									
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
438	438	1	10	511	13	28	23	105	218	113	438	1	10	511	13	52	46	80	218	138
440	440	1	10	511	10	28	23	105	219	114	220	2	9	255	18	26	47	80	219	139
441	63	7	7	63	53	3	18	103	220	117	63	7	7	63	53	6	38	72	220	148
442	442	1	10	511	11	28	23	105	220	115	221	2	9	255	20	26	47	80	220	140
444	444	1	10	511	10	28	23	105	221	116	12	37	5	15	186	1	36	76	221	145
445	445	1	12	2047	16	28	23	529	222	–	5	89	5	15	446	1	88	128	222	94
446	–	–	–	–	–	–	–	–	–	–	2	223	2	2	447	1	222	223	222	–
447	–	–	–	–	–	–	–	–	–	–	3	149	3	3	448	1	148	151	223	72
448	448	1	10	511	13	28	23	105	223	118	14	32	5	15	162	1	31	71	223	152
450	450	1	10	511	13	28	23	105	224	119	15	30	5	15	153	1	29	69	224	155
451	451	1	11	1023	12	28	23	232	225	–	451	1	11	1023	12	77	71	124	225	101
452	–	–	–	–	–	–	–	–	–	–	4	113	3	4	339	1	112	117	225	108
453	–	–	–	–	–	–	–	–	–	–	3	151	3	3	454	1	150	153	226	73
454	–	–	–	–	–	–	–	–	–	–	2	227	2	2	455	1	226	227	226	–
455	455	1	11	1023	12	28	23	232	227	–	7	65	4	7	262	1	64	76	227	151
456	456	1	10	511	11	28	23	105	227	122	12	38	5	15	191	1	37	77	227	150
458	–	–	–	–	–	–	–	–	–	–	2	229	2	2	459	1	228	229	228	–
459	153	3	9	255	31	9	23	165	229	64	153	3	9	255	31	22	61	103	229	126
460	460	1	10	511	9	28	23	105	229	124	230	2	9	255	18	26	47	80	229	149
462	462	1	10	511	13	28	23	105	230	125	14	33	5	15	167	1	32	72	230	158
464	–	–	–	–	–	–	–	–	–	–	8	58	5	16	290	1	57	101	231	130
465	465	1	10	511	15	28	23	105	232	127	15	31	5	15	158	1	30	70	232	162
466	–	–	–	–	–	–	–	–	–	–	2	233	2	2	467	1	232	233	232	–
468	468	1	10	511	11	28	23	105	233	128	12	39	5	15	196	1	38	78	233	155
469	–	–	–	–	–	–	–	–	–	–	7	67	4	7	270	1	66	78	234	156
470	470	1	10	511	10	28	23	105	234	129	470	1	10	511	10	52	46	80	234	154
471	–	–	–	–	–	–	–	–	–	–	3	157	3	3	472	1	156	159	235	76
472	–	–	–	–	–	–	–	–	–	–	8	59	5	16	295	1	58	102	235	133
473	473	1	11	1023	12	28	23	232	236	4	473	1	11	1023	12	77	71	124	236	112
474	–	–	–	–	–	–	–	–	–	–	6	79	4	7	317	1	78	90	236	146
475	–	–	–	–	–	–	–	–	–	–	5	95	5	15	476	1	94	134	237	103
476	476	1	10	511	13	28	23	105	237	132	14	34	5	15	172	1	33	73	237	164
477	–	–	–	–	–	–	–	–	–	–	3	159	3	3	478	1	158	161	238	77
478	–	–	–	–	–	–	–	–	–	–	2	239	2	2	479	1	238	239	238	–
480	480	1	10	511	13	28	23	105	239	134	15	32	5	15	163	1	31	71	239	168
481	481	1	13	4095	14	28	23	1208	240	–	481	1	13	4095	14	120	113	307	240	–
482	–	–	–	–	–	–	–	–	–	–	2	241	2	2	483	1	240	241	240	–
483	483	1	10	511	13	28	23	105	241	136	7	69	4	7	278	1	68	80	241	161
484	484	1	11	1023	11	28	23	232	241	9	484	1	11	1023	11	77	71	124	241	117
485	–	–	–	–	–	–	–	–	–	–	5	97	5	15	486	1	96	136	242	106
486	486	1	10	511	10	28	23	105	242	137	243	2	9	255	19	26	47	80	242	162
488	–	–	–	–	–	–	–	–	–	–	8	61	5	16	305	1	60	104	243	139
489	–	–	–	–	–	–	–	–	–	–	3	163	3	3	490	1	162	165	244	79
490	490	1	10	511	11	28	23	105	244	139	14	35	5	15	177	1	34	74	244	170
492	492	1	10	511	10	28	23	105	245	140	12	41	5	15	206	1	40	80	245	165
493	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
494	494	1	13	4095	13	28	23	1208	246	–	2	247	2	2	495	1	246	247	246	–

N	$EG1$										$EG2$									
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
495	45	11	7	63	80	2	20	157	247	90	15	33	5	15	168	1	32	72	247	175
496	496	1	10	511	12	28	23	105	247	142	31	16	6	31	100	3	45	76	247	171
497	–	–	–	–	–	–	–	–	–	–	7	71	4	7	286	1	70	82	248	166
498	–	–	–	–	–	–	–	–	–	–	6	83	4	7	333	1	82	94	248	154
500	500	1	10	511	9	28	23	105	249	144	250	2	9	255	18	26	47	80	249	169
501	–	–	–	–	–	–	–	–	–	–	3	167	3	3	502	1	166	169	250	81
502	–	–	–	–	–	–	–	–	–	–	2	251	2	2	503	1	250	251	250	–
504	504	1	10	511	15	28	23	105	251	146	14	36	5	15	182	1	35	75	251	176
505	–	–	–	–	–	–	–	–	–	–	5	101	5	15	506	1	100	140	252	112
506	506	1	11	1023	11	28	23	232	252	20	506	1	11	1023	11	77	71	124	252	128
507	507	1	13	4095	16	28	23	1208	253	–	3	169	3	3	508	1	168	171	253	82
508	508	1	10	511	13	28	23	105	253	148	127	4	8	127	37	13	47	80	253	173
510	510	1	10	511	15	28	23	105	254	149	15	34	5	15	173	1	33	73	254	181
511	511	1	10	511	17	28	23	105	255	150	511	1	10	511	17	52	46	80	255	175
512	–	–	–	–	–	–	–	–	–	–	8	64	5	16	320	1	63	107	255	148
513	171	3	9	255	28	9	23	165	256	91	171	3	9	255	28	22	61	103	256	153
514	–	–	–	–	–	–	–	–	–	–	2	257	2	2	515	1	256	257	256	–
515	–	–	–	–	–	–	–	–	–	–	5	103	5	15	516	1	102	142	257	115
516	516	1	10	511	10	28	23	105	257	152	516	1	10	511	10	52	46	80	257	177
517	517	1	11	1023	12	28	23	232	258	26	517	1	11	1023	12	77	71	124	258	134
518	518	1	10	511	11	28	23	105	258	153	14	37	5	15	187	1	36	76	258	182
519	–	–	–	–	–	–	–	–	–	–	3	173	3	3	520	1	172	175	259	84
520	520	1	10	511	10	28	23	105	259	154	260	2	9	255	18	26	47	80	259	179
522	522	1	10	511	10	28	23	105	260	155	261	2	9	255	19	26	47	80	260	180
524	–	–	–	–	–	–	–	–	–	–	4	131	3	4	393	1	130	135	261	126
525	525	1	10	511	14	28	23	105	262	157	15	35	5	15	178	1	34	74	262	188
526	–	–	–	–	–	–	–	–	–	–	2	263	2	2	527	1	262	263	262	–
527	31	17	6	31	106	1	16	129	263	134	31	17	6	31	106	3	48	79	263	184
528	528	1	10	511	11	28	23	105	263	158	132	4	8	128	33	13	47	80	263	183
529	529	1	12	2047	14	28	23	529	264	–	529	1	12	2047	14	114	107	189	264	75
530	530	1	10	511	10	28	23	105	264	159	530	1	10	511	10	52	46	80	264	184
531	–	–	–	–	–	–	–	–	–	–	3	177	3	3	532	1	176	179	265	86
532	532	1	10	511	13	28	23	105	265	160	14	38	5	15	192	1	37	77	265	188
533	533	1	13	4095	14	28	23	1208	266	–	533	1	13	4095	14	120	113	307	266	–
534	534	1	12	2048	15	28	23	529	266	–	6	89	4	7	357	1	88	100	266	166
535	–	–	–	–	–	–	–	–	–	–	5	107	5	15	536	1	106	146	267	121
536	–	–	–	–	–	–	–	–	–	–	8	67	5	16	335	1	66	110	267	157
537	–	–	–	–	–	–	–	–	–	–	3	179	3	3	538	1	178	181	268	87
538	–	–	–	–	–	–	–	–	–	–	2	269	2	2	539	1	268	269	268	–
539	49	11	7	63	78	2	20	157	269	112	7	77	4	7	310	1	76	88	269	181
540	30	18	6	31	111	1	17	130	269	139	15	36	5	15	183	1	35	75	269	194
542	–	–	–	–	–	–	–	–	–	–	2	271	2	2	543	1	270	271	270	–
543	–	–	–	–	–	–	–	–	–	–	3	181	3	3	544	1	180	183	271	88
544	544	1	11	1023	12	28	23	232	271	39	8	68	5	16	340	1	67	111	271	160
545	–	–	–	–	–	–	–	–	–	–	5	109	5	15	546	1	108	148	272	124
546	546	1	11	1023	14	28	23	232	272	40	14	39	5	15	197	1	38	78	272	194
548	–	–	–	–	–	–	–	–	–	–	4	137	3	4	411	1	136	141	273	132

N	$EG1$										$EG2$									
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$
549	–	–	–	–	–	–	–	–	–	–	3	183	3	3	550	1	182	185	274	89
550	550	1	11	1023	11	28	23	232	274	42	10	55	5	15	275	1	54	94	274	180
551	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
552	24	23	6	31	140	1	22	135	275	140	12	46	5	15	231	1	45	85	275	190
553	–	–	–	–	–	–	–	–	–	–	7	79	4	7	318	1	78	90	276	186
554	–	–	–	–	–	–	–	–	–	–	2	277	2	2	555	1	276	277	276	–
555	555	1	11	1023	13	28	23	232	277	45	15	37	5	15	188	1	36	76	277	201
556	–	–	–	–	–	–	–	–	–	–	4	139	3	4	417	1	138	143	277	134
558	31	18	6	31	112	1	17	130	278	148	31	18	6	31	112	3	51	82	278	196
559	559	1	13	4095	14	28	23	1208	279	–	559	1	13	4095	14	120	113	307	279	–
560	28	20	6	31	121	1	19	132	279	147	14	40	5	15	202	1	39	79	279	200
561	187	3	9	255	29	9	23	165	280	115	187	3	9	255	29	22	61	103	280	177
562	–	–	–	–	–	–	–	–	–	–	2	281	2	2	563	1	280	281	280	–
564	564	1	11	1023	10	28	23	232	281	49	12	47	5	15	236	1	46	86	281	195
565	–	–	–	–	–	–	–	–	–	–	5	113	5	15	566	1	112	152	282	130
566	–	–	–	–	–	–	–	–	–	–	2	283	2	2	567	1	282	283	282	–
567	63	9	7	63	67	2	16	153	283	130	63	9	7	63	67	6	50	84	283	199
568	–	–	–	–	–	–	–	–	–	–	8	71	5	16	355	1	70	114	283	169
570	30	19	6	31	117	1	18	131	284	153	15	38	5	15	193	1	37	77	284	207
572	572	1	11	1023	11	28	23	232	285	53	572	1	11	1023	11	77	71	124	285	161
573	–	–	–	–	–	–	–	–	–	–	3	191	3	3	574	1	190	193	286	93
574	574	1	11	1023	12	28	23	232	286	54	14	41	5	15	207	1	40	80	286	206
575	575	1	12	2047	14	28	23	529	287	–	5	115	5	15	576	1	114	154	287	133
576	24	24	6	31	146	1	23	136	287	151	12	48	5	15	241	1	47	87	287	200
578	–	–	–	–	–	–	–	–	–	–	2	289	2	2	579	1	288	289	288	–
579	–	–	–	–	–	–	–	–	–	–	3	193	3	3	580	1	192	195	289	94
580	580	1	11	1023	10	28	23	232	289	57	10	58	5	15	290	1	57	97	289	192
581	–	–	–	–	–	–	–	–	–	–	7	83	4	7	334	1	82	94	290	196
582	–	–	–	–	–	–	–	–	–	–	6	97	4	7	389	1	96	108	290	182
583	583	1	11	1023	12	28	23	232	291	59	583	1	11	1023	12	77	71	124	291	167
584	584	1	11	1023	13	28	23	232	291	59	8	73	5	16	365	1	72	116	291	175
585	195	3	9	255	30	9	23	165	292	127	15	39	5	15	198	1	38	78	292	214
586	–	–	–	–	–	–	–	–	–	–	2	293	2	2	587	1	292	293	292	–
588	28	21	6	31	127	1	20	133	293	160	14	42	5	15	212	1	41	81	293	212
589	31	19	6	31	118	1	18	131	294	163	31	19	6	31	118	3	54	85	294	209
590	–	–	–	–	–	–	–	–	–	–	10	59	5	15	295	1	58	98	294	196
591	–	–	–	–	–	–	–	–	–	–	3	197	3	3	592	1	196	199	295	96
592	–	–	–	–	–	–	–	–	–	–	8	74	5	16	370	1	73	117	295	178
594	54	11	7	63	77	2	20	157	296	139	54	11	7	63	77	5	52	95	296	201
595	595	1	11	1023	12	28	23	232	297	65	7	85	4	7	342	1	84	96	297	201
596	–	–	–	–	–	–	–	–	–	–	4	149	3	4	447	1	148	153	297	144
597	–	–	–	–	–	–	–	–	–	–	3	199	3	3	598	1	198	201	298	97
598	598	1	12	2047	13	28	23	529	298	–	598	1	12	2047	13	114	107	189	298	109
600	30	20	6	31	123	1	19	132	299	167	15	40	5	15	203	1	39	79	299	220

B Elliptic and Hyperelliptic Curve Selection

We describe how the elliptic curve E186 was selected, and how a random instance of the ECDLP in E186 was generated and reduced to an instance of the HCDLP in C186. The elliptic curves E161, E180, E217, E248, E300 and the corresponding hyperelliptic curves listed in Appendix C were generated in an analogous manner. Note that the hyperelliptic curves produced by the GHS reduction are not unique—we merely list the hyperelliptic curves generated by an invocation of Hess's KASH program [18]. Including the hyperelliptic curves and divisors will assist those who wish to implement the index-calculus methods for the HCDLP without first having to perform the complicated GHS reduction. The elliptic curve E161-2 was generated verifiably at random by selecting the curve $E_b : y^2 + xy = x^3 + x^2 + b$ where b is the element in $\mathbb{F}_{2^{161}}$ identified (see below) with the smallest integer $\geq 2^{160}$ for which $\#E_b(\mathbb{F}_{2^{161}})$ is twice a prime. Finally, the elliptic curves E176 and E272 are from ANSI X9.62 [1].

Elliptic Curve Generation. Let $n = 31$, and $q = 2^6$. Let a be an arbitrary element of trace 1 in $\mathbb{F}_{2^{186}}$. The order of 2 modulo n is $t = 5$. Let $s = 6$, and let f_i, $0 \leq i \leq s$, be the monic irreducible factors of $x^{31} - 1$ over $\mathbb{F}_2$ with $f_0(x) = x - 1$ (cf. Theorem 8). Let $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be the Frobenius map defined by $x \mapsto x^q$. Define

$$B = \{b \in \mathbb{F}_{q^n} \backslash \mathbb{F}_q \ : \ (\sigma + 1) f_i(\sigma)(b) = 0 \text{ for some } 1 \leq i \leq s\}.$$

The elliptic curve E186 was chosen by selecting random elements $b \in B$ until the number of $\mathbb{F}_{2^{186}}$-rational points on $y^2 + xy = x^3 + ax^2 + b$ is twice a prime.

The elements of $\mathbb{F}_{2^{186}}$ are represented as binary polynomials modulo the irreducible polynomial $z^{186} + z^{11} + 1$. We identify a 186-bit integer $c = c_{185}2^{185} + c_{184}2^{184} + \cdots + c_0$ with the element $c_{185}z^{185} + c_{184}z^{184} + \cdots + c_0$ of $\mathbb{F}_{2^{186}}$. The defining equation for the elliptic curve E186 is $y^2 + xy = x^3 + ax^2 + b$ where

$$\begin{aligned} a &= \texttt{3D7D03F4CB539C5B728D256DAD2E5E8ADDB81B524F7D68D} \text{ and} \\ b &= \texttt{35108742308B720FAABCFFB70D33E3840F8D93323635F7E} \end{aligned}$$

in hexadecimal notation. The number of $\mathbb{F}_{2^{186}}$-rational points on E186 is $2r$, where

$$r = \texttt{20000000000000000000000000E5BED0151962E91F6CDF581}$$

is prime.

ECDLP Instance Generation. We selected two points P, Q from E186($\mathbb{F}_{2^{186}}$) *verifiably at random* as follows. We first defined 160-bit integers m_1 and m_2 to be the 160-bit outputs of the SHA-1 cryptographic hash function with inputs the strings "" and "a", respectively[1]. We identify a 160-bit integer $c = c_{159}2^{159} + c_{158}2^{158} + \cdots + c_0$ with the element $c_{159}z^{159} + c_{158}z^{158} + \cdots + c_0$ of $\mathbb{F}_{2^{186}}$. Then, for each $i \in \{1, 2\}$, we define n_i to be the smallest integer $\geq m_i$ for which the field element corresponding to n_i is the x-coordinate of some point of order not equal to 2 in E186($\mathbb{F}_{2^{186}}$); for such an n_i we arbitrarily

[1] These two strings are commonly used as inputs to generate test vectors for hash functions; see Table 9.6 of [25].

select one of the two possible y-coordinates to obtain two points P' and Q' and then set $P = 2P'$ and $Q = 2Q'$. In this way, we derive the following two points of order r:

$$\begin{aligned} P &= (\texttt{6FE4D23FBAFBAF66317050A0D102E23075572174ADC304}, \\ &\quad\ \texttt{24E2CB9E1DAF261EA25FD0413F85CF067DB5FE50F4849B2}), \\ Q &= (\texttt{EFD00F993676085F97D9BB9117E00A34F6185104629F42}, \\ &\quad\ \texttt{1EBBB1F436A53B00B4C74A93CF6E613F3C60D566BDB9653}). \end{aligned}$$

The ECDLP challenge is to find the integer $\lambda \in [0, r-1]$ such that $Q = \lambda P$. Note that since P and Q were (pseudo)randomly generated, the discrete logarithm λ is not known a priori by us.

HCDLP Instance Generation. Hess's KASH program [18] for the Weil restriction represents elliptic curve points as zero divisors. For technical reasons, it excludes the point at infinity from occurring in the support of the divisors. Thus, instead of representing an elliptic curve point P by a zero divisor $(P) - (\infty)$, we represent P by the equivalent zero divisor $(P + R) - (R)$, where R is an arbitrary point on the curve. We arbitrarily selected the following point of order r:

$$\begin{aligned} R &= (\texttt{3A9EE09AEC0996B46F3680D80835FF3081D795A93AB58FF}, \\ &\quad\ \texttt{FC867E29309F63717894B647A611E743919B511E204862}). \end{aligned}$$

Let $P_1 = P+R$, $P_2 = Q+R$ and $P_3 = R$. Hess's KASH program was used to reduce (E186, P_1, P_2, P_3) to (C186, D_1, D_2, D_3), where C186 is a genus-31 hyperelliptic curve over $\mathbb{F}_{2^6}$ and D_1, D_2, D_3 are divisors in $J_{\mathrm{C186}}(\mathbb{F}_{2^6})$. The elements of $\mathbb{F}_{2^6}$ are represented as binary polynomials modulo the irreducible polynomial $w^6 + w^4 + w^3 + w + 1$. The Weierstrass equation for the hyperelliptic curve C186 is $v^2 + h(u)v = f(u)$, where

$$\begin{aligned} f(u) &= w^{30}u^{63} + w^{10}u^{62} + w^{40}u^{60} + w^{54}u^{56} + w^{23}u^{48} + w^{26}, \\ h(u) &= w^{15}u^{31} + wu^{30} + w^{21}u^{28} + w^{59}u^{24} + w^{41}u^{16} + w^{10}. \end{aligned}$$

The divisors D_1, D_2 and D_3 are:

$$\begin{aligned} D_1 = \mathrm{div}(&u^{31}+w^{32}u^{30}+w^{58}u^{29}+w^{57}u^{28}+w^{11}u^{27}+w^{25}u^{26}+w^{39}u^{24}+w^{37}u^{23}+w^{59}u^{22}+w^{19}u^{21}+w^{3}u^{20}+ \\ &w^{45}u^{19}+w^{47}u^{18}+wu^{16}+w^{40}u^{15}+w^{6}u^{14}+w^{53}u^{13}+w^{48}u^{12}+w^{30}u^{11}+w^{33}u^{10}+w^{19}u^{9}+w^{55}u^{8}+ \\ &w^{28}u^{7}+w^{7}u^{6}+w^{20}u^{5}+w^{5}u^{4}+w^{38}u^{3}+w^{29}u^{2}+w^{60}u+w^{11},\ w^{36}u^{30}+w^{28}u^{29}+w^{27}u^{28}+w^{24}u^{27}+ \\ &w^{12}u^{26}+w^{58}u^{25}+w^{62}u^{24}+w^{8}u^{23}+w^{13}u^{22}+w^{41}u^{21}+w^{22}u^{20}+w^{11}u^{19}+w^{40}u^{18}+w^{26}u^{17}+w^{39}u^{16}+ \\ &w^{19}u^{15}+w^{39}u^{14}+w^{43}u^{13}+w^{3}u^{12}+w^{58}u^{11}+w^{52}u^{10}+w^{54}u^{9}+w^{6}u^{8}+w^{53}u^{7}+w^{42}u^{6}+w^{50}u^{5}+ \\ &w^{18}u^{4}+w^{2}u^{3}+w^{38}u^{2}+w^{11}u+w), \end{aligned}$$

$$\begin{aligned} D_2 = \mathrm{div}(&u^{31}+w^{9}u^{30}+w^{23}u^{29}+w^{17}u^{28}+w^{23}u^{27}+w^{37}u^{26}+w^{34}u^{25}+w^{25}u^{24}+w^{46}u^{23}+w^{21}u^{22}+w^{61}u^{21}+ \\ &w^{42}u^{20}+w^{39}u^{19}+w^{7}u^{18}+w^{43}u^{17}+w^{50}u^{16}+w^{43}u^{15}+w^{22}u^{14}+w^{24}u^{13}+w^{31}u^{12}+w^{24}u^{11}+w^{5}u^{10}+ \\ &w^{28}u^{9}+w^{62}u^{8}+w^{34}u^{7}+u^{6}+w^{45}u^{5}+w^{18}u^{4}+w^{15}u^{3}+w^{54}u^{2}+w^{4}u+1,\ w^{12}u^{30}+w^{32}u^{29}+w^{19}u^{28}+ \\ &w^{62}u^{27}+w^{25}u^{26}+w^{45}u^{25}+w^{50}u^{24}+w^{18}u^{23}+w^{51}u^{22}+wu^{21}+w^{36}u^{20}+w^{5}u^{19}+w^{58}u^{18}+w^{60}u^{17}+ \\ &w^{22}u^{16}+w^{11}u^{15}+w^{12}u^{14}+w^{25}u^{13}+w^{47}u^{12}+w^{4}u^{11}+w^{62}u^{9}+w^{60}u^{8}+w^{33}u^{7}+w^{52}u^{6}+w^{21}u^{5}+ \\ &w^{43}u^{4}+w^{36}u^{3}+w^{50}u^{2}+w^{5}u+w^{20}), \end{aligned}$$

$$
\begin{aligned}
D_3 = \operatorname{div}(& u^{31}+w^{54}u^{30}+w^{42}u^{29}+w^{62}u^{28}+w^{38}u^{27}+w^{11}u^{26}+w^{15}u^{25}+w^{2}u^{24}+w^{62}u^{23}+w^{54}u^{22}+w^{8}u^{21}+ \\
& w^{53}u^{20}+w^{17}u^{19}+w^{6}u^{18}+u^{17}+w^{51}u^{16}+w^{22}u^{15}+w^{61}u^{14}+w^{2}u^{13}+w^{61}u^{12}+w^{40}u^{11}+w^{12}u^{10}+ \\
& w^{14}u^{9}+w^{3}u^{8}+w^{13}u^{7}+w^{31}u^{6}+w^{60}u^{5}+w^{16}u^{4}+w^{43}u^{3}+w^{3}u^{2}+w^{9}u+w^{7}\ ,\ w^{25}u^{30}+w^{24}u^{29}+ \\
& w^{62}u^{28}+w^{13}u^{27}+w^{17}u^{26}+w^{53}u^{25}+w^{52}u^{24}+w^{43}u^{23}+w^{20}u^{22}+w^{51}u^{21}+w^{23}u^{20}+w^{59}u^{19}+ \\
& w^{60}u^{18}+w^{49}u^{17}+w^{20}u^{16}+w^{47}u^{15}+w^{53}u^{14}+w^{40}u^{13}+w^{49}u^{12}+w^{28}u^{11}+w^{3}u^{10}+w^{6}u^{9}+w^{35}u^{8}+ \\
& w^{41}u^{7}+w^{6}u^{6}+w^{46}u^{5}+w^{57}u^{3}+w^{9}u^{2}+w^{21}u+w^{53}).
\end{aligned}
$$

The task is to solve the following discrete logarithm problem in $J_{\mathrm{C186}}(\mathbb{F}_{2^6})$: find the integer $\lambda \in [0, r-1]$ such that $(D_2 - D_3) = \lambda(D_1 - D_3)$.

C ECDLP Challenge Parameters

For an explanation of the notation used in the following tables, see §7 and Appendix B.

E161, $N = 161$, $\mathbb{F}_{2^{161}} = \mathbb{F}_2[z]/(z^{161} + z^{18} + 1)$, $\#\mathrm{E161}(\mathbb{F}_{2^{161}}) = 2 \cdot r$, $a = 1$
$b =$ `1102A36EE3EEE95C1DDA26A51A954391733728D22`
$r =$ `FFFFFFFFFFFFFFFFFFFFFD03F975D827A7D20F89`
$P = ($`1CBF654BEEF0AE9F525F8E9F5FA1DED1D10C7D781`, `175984F97695A39291B94B6D9BD89860C9AF5DF80`$)$
$Q = ($`AE24976AE483ED2E33A77FD48F78DAE06ED0F54E`, `186EBA8B979ADAA320D47C7763CFF8EF810A970EB`$)$
$R = ($`1E7958EF1FA48A2B92889B442DADE6E9A6A7C173`, `4EE6671B1A5D69A5578EFE30C05704FA69C78345`$)$
C161, $q = 2^{23}$, $\mathbb{F}_{2^{23}} = \mathbb{F}_2[w]/(w^{23} + w^5 + 1)$
$f(u) = w^{6691705}u^{15} + w^{4316786}u^{14} + w^{4857716}u^{12} + w^{4289455}u^{8} + w^{7257339}$
$h(u) = w^{7540156}u^{7} + w^{4708240}u^{6} + w^{2060647}u^{4} + w^{7822973}$
$D_1 = \operatorname{div}(u^7+w^{111674}u^6+w^{6262987}u^5+w^{5507868}u^4+w^{5024071}u^3+w^{7360243}u^2+w^{4982988}u+w^{3476956},$ $w^{7214579}u^6+w^{1039748}u^5+w^{5362902}u^4+w^{5575575}u^3+w^{6046318}u^2+w^{783556}u+w^{7954483})$
$D_2 = \operatorname{div}(u^7+w^{2418740}u^6+w^{6332447}u^5+w^{5288518}u^4+w^{6581623}u^3+w^{3461659}u^2+w^{663714}u+w^{2094946},$ $w^{5819570}u^6+w^{5789770}u^5+w^{3853008}u^4+w^{3628267}u^3+w^{4786898}u^2+w^{3463517}u+w^{2504145})$
$D_3 = \operatorname{div}(u^7+w^{7595037}u^6+w^{6492024}u^5+w^{5128797}u^4+w^{1479702}u^3+w^{3764869}u^2+w^{2973617}u+w^{3579984},$ $w^{5819570}u^6+w^{5789770}u^5+w^{3853008}u^4+w^{3628267}u^3+w^{4786898}u^2+w^{3463517}u+w^{2504145})$

E180, $N = 180$, $\mathbb{F}_{2^{180}} = \mathbb{F}_2[z]/(z^{180} + z^3 + 1)$, $\#\mathrm{E180}(\mathbb{F}_{2^{180}}) = 2 \cdot r$

$a =$ `B3C8B5AF89342D73C9D12F1F5ACDD36011626BBC675C1`

$b =$ `990D04982994434CB4C14DB21204025865B40069225B2`

$r =$ `800000000000000000000023ABAE178BD70C3E01FDC31`

$P = ($`EE4AB1D7C359522ED9CABE52021DAD0EAF613C1ECE8CB`,
`670775621CD859D56079BB52298C0A509AB4E689593F9`$)$

$Q = ($`7F13258D03372C8A571E8C199DD9416A7642DDA05C515`,
`1182432B1B3C6C1856D47B139B28E003B6D9F440574FF`$)$

$R = ($`BAD2E0D1D655559AF62E346BE2090135E40AEC22EE5C3`,
`B5B71A32C4498B8CF0DF6BB90911D91CC16F506D508C5`$)$

C180, $q = 2^{12}$, $\mathbb{F}_{2^{12}} = \mathbb{F}_2[w]/(w^{12} + w^7 + w^6 + w^5 + w^3 + w + 1)$

$f(u) = w^{1977}u^{31} + w^{3517}u^{30} + w^{3954}u^{28} + w^{3666}u^{24} + w^{3749}u^{16} + w^{2880}$

$h(u) = w^{3036}u^{15} + w^{4031}u^{14} + w^{1455}u^{12} + w^{2278}u^{8} + w^{2024}$

$D_1 = \mathrm{div}(u^{15}+w^{913}u^{14}+w^{120}u^{13}+w^{1222}u^{12}+w^{717}u^{11}+w^{1158}u^{10}+w^{406}u^{9}+w^{3864}u^{8}+w^{3391}u^{7}+ w^{3302}u^{6}+w^{906}u^{5}+w^{2528}u^{4}+w^{3620}u^{3}+w^{1164}u^{2}+w^{119}u+w^{68},\ w^{3862}u^{14}+w^{1139}u^{13}+w^{4055}u^{12}+ w^{3324}u^{11}+w^{1436}u^{10}+w^{1968}u^{9}+w^{1488}u^{8}+w^{22}u^{7}+w^{3071}u^{6}+w^{1736}u^{5}+w^{394}u^{4}+w^{1892}u^{3}+ w^{3461}u^{2}+w^{923}u+w^{2371})$

$D_2 = \mathrm{div}(u^{15}+w^{2828}u^{14}+w^{2507}u^{13}+w^{2845}u^{12}+w^{3821}u^{11}+w^{550}u^{10}+w^{837}u^{9}+w^{3146}u^{8}+w^{1040}u^{7}+ w^{1551}u^{6}+w^{2806}u^{5}+w^{2321}u^{4}+w^{251}u^{3}+w^{3983}u^{2}+w^{1482}u+w^{1796},\ w^{2370}u^{14}+w^{3993}u^{13}+w^{2270}u^{12}+ w^{3787}u^{11}+w^{2128}u^{10}+w^{2948}u^{9}+w^{72}u^{8}+w^{27}u^{7}+w^{1515}u^{6}+w^{1684}u^{5}+w^{385}u^{4}+w^{3635}u^{3}+w^{1076}u^{2}+ w^{1654}u+w^{3081})$

$D_3 = \mathrm{div}(u^{15}+w^{2485}u^{14}+w^{1754}u^{13}+w^{1638}u^{12}+w^{2078}u^{11}+w^{4039}u^{10}+w^{2857}u^{9}+w^{2716}u^{8}+w^{230}u^{7}+ w^{1139}u^{6}+w^{1330}u^{5}+w^{851}u^{4}+w^{1926}u^{3}+w^{428}u^{2}+w^{2628}u+w^{2729},\ w^{2543}u^{14}+w^{998}u^{13}+w^{37}u^{12}+ w^{1097}u^{11}+w^{2830}u^{10}+w^{770}u^{9}+w^{2604}u^{8}+w^{3011}u^{7}+w^{2334}u^{6}+w^{863}u^{5}+w^{1952}u^{4}+w^{1777}u^{3}+ w^{1122}u^{2}+w^{1754}u+w^{3677})$

E186, $N = 186$, $\mathbb{F}_{2^{186}} = \mathbb{F}_2[z]/(z^{186} + z^{11} + 1)$, $\#\mathrm{E186}(\mathbb{F}_{2^{186}}) = 2 \cdot r$

$a =$ `3D7D03F4CB539C5B728D256DAD2E5E8ADDB81B524F7D68D`

$b =$ `35108742308B720FAABCFFB70D33E3840F8D93323635F7E`

$r =$ `200000000000000000000000E5BED0151962E91F6CDF581`

$P = ($`6FE4D23FBAFBAF66317050A0D102E23075572174ADC304`,
`24E2CB9E1DAF261EA25FD0413F85CF067DB5FE50F4849B2`$)$

$Q = ($`EFD00F993676085F97D9BB9117E00A34F6185104629F42`,
`1EBBB1F436A53B00B4C74A93CF6E613F3C60D566BDB9653`$)$

$R = ($`3A9EE09AEC0996B46F3680D80835FF3081D795A93AB58FF`,
`FC867E29309F63717894B647A611E743919B511E204862`$)$

C186, $q = 64$, $\mathbb{F}_{2^6} = \mathbb{F}_2[w]/(w^6 + w^4 + w^3 + w + 1)$

$f(u) = w^{30}u^{63} + w^{10}u^{62} + w^{40}u^{60} + w^{54}u^{56} + w^{23}u^{48} + w^{26}$

$h(u) = w^{15}u^{31} + wu^{30} + w^{21}u^{28} + w^{59}u^{24} + w^{41}u^{16} + w^{10}$

$D_1 = \mathrm{div}(u^{31}+w^{32}u^{30}+w^{58}u^{29}+w^{57}u^{28}+w^{11}u^{27}+w^{25}u^{26}+w^{39}u^{24}+w^{37}u^{23}+w^{59}u^{22}+w^{19}u^{21}+ w^{3}u^{20}+w^{45}u^{19}+w^{47}u^{18}+wu^{16}+w^{40}u^{15}+w^{6}u^{14}+w^{53}u^{13}+w^{48}u^{12}+w^{30}u^{11}+w^{33}u^{10}+w^{19}u^{9}+ w^{55}u^{8}+w^{28}u^{7}+w^{7}u^{6}+w^{20}u^{5}+w^{5}u^{4}+w^{38}u^{3}+w^{29}u^{2}+w^{60}u+w^{11},\ w^{36}u^{30}+w^{28}u^{29}+w^{27}u^{28}+ w^{24}u^{27}+w^{12}u^{26}+w^{58}u^{25}+w^{62}u^{24}+w^{8}u^{23}+w^{13}u^{22}+w^{41}u^{21}+w^{22}u^{20}+w^{11}u^{19}+w^{40}u^{18}+ w^{26}u^{17}+w^{39}u^{16}+w^{19}u^{15}+w^{39}u^{14}+w^{43}u^{13}+w^{3}u^{12}+w^{58}u^{11}+w^{52}u^{10}+w^{54}u^{9}+w^{6}u^{8}+w^{53}u^{7}+ w^{42}u^{6}+w^{50}u^{5}+w^{18}u^{4}+w^{2}u^{3}+w^{38}u^{2}+w^{11}u+w)$

$D_2 = \mathrm{div}(u^{31}+w^{9}u^{30}+w^{23}u^{29}+w^{17}u^{28}+w^{23}u^{27}+w^{37}u^{26}+w^{34}u^{25}+w^{25}u^{24}+w^{46}u^{23}+w^{21}u^{22}+w^{61}u^{21}+ w^{42}u^{20}+w^{39}u^{19}+w^{7}u^{18}+w^{43}u^{17}+w^{50}u^{16}+w^{43}u^{15}+w^{22}u^{14}+w^{24}u^{13}+w^{31}u^{12}+w^{24}u^{11}+w^{5}u^{10}+ w^{28}u^{9}+w^{62}u^{8}+w^{34}u^{7}+u^{6}+w^{45}u^{5}+w^{18}u^{4}+w^{15}u^{3}+w^{54}u^{2}+w^{4}u+1,\ w^{12}u^{30}+w^{32}u^{29}+w^{19}u^{28}+ w^{62}u^{27}+w^{25}u^{26}+w^{45}u^{25}+w^{50}u^{24}+w^{18}u^{23}+w^{51}u^{22}+wu^{21}+w^{36}u^{20}+w^{5}u^{19}+w^{58}u^{18}+w^{60}u^{17}+ w^{22}u^{16}+w^{11}u^{15}+w^{12}u^{14}+w^{25}u^{13}+w^{47}u^{12}+w^{4}u^{11}+w^{62}u^{9}+w^{60}u^{8}+w^{33}u^{7}+w^{52}u^{6}+w^{21}u^{5}+ w^{43}u^{4}+w^{36}u^{3}+w^{50}u^{2}+w^{5}u+w^{20})$

$D_3 = \mathrm{div}(u^{31}+w^{54}u^{30}+w^{42}u^{29}+w^{62}u^{28}+w^{38}u^{27}+w^{11}u^{26}+w^{15}u^{25}+w^{2}u^{24}+w^{62}u^{23}+w^{54}u^{22}+w^{8}u^{21}+ w^{53}u^{20}+w^{17}u^{19}+w^{6}u^{18}+u^{17}+w^{51}u^{16}+w^{22}u^{15}+w^{61}u^{14}+w^{2}u^{13}+w^{61}u^{12}+w^{40}u^{11}+w^{12}u^{10}+ w^{14}u^{9}+w^{3}u^{8}+w^{13}u^{7}+w^{31}u^{6}+w^{60}u^{5}+w^{16}u^{4}+w^{43}u^{3}+w^{3}u^{2}+w^{9}u+w^{7}\ , w^{25}u^{30}+w^{24}u^{29}+ w^{62}u^{28}+w^{13}u^{27}+w^{17}u^{26}+w^{53}u^{25}+w^{52}u^{24}+w^{43}u^{23}+w^{20}u^{22}+w^{51}u^{21}+w^{23}u^{20}+w^{59}u^{19}+ w^{60}u^{18}+w^{49}u^{17}+w^{20}u^{16}+w^{47}u^{15}+w^{53}u^{14}+w^{40}u^{13}+w^{49}u^{12}+w^{28}u^{11}+w^{3}u^{10}+w^{6}u^{9}+w^{35}u^{8}+ w^{41}u^{7}+w^{6}u^{6}+w^{46}u^{5}+w^{57}u^{3}+w^{9}u^{2}+w^{21}u+w^{53})$

E217, $N = 217$, $\mathbb{F}_{2^{217}} = \mathbb{F}_2[z]/(z^{217} + z^{45} + 1)$, $\#\mathrm{E217}(\mathbb{F}_{2^{217}}) = 2 \cdot r$, $a = 1$

$b =$ `11E8F97F344082577BB4D782D3F433FBE30D8F3D65684AE499694BA`

$r =$ `10000000000000000000000000000598FB15077594E7069CED749A1`

$P = ($`1B3E0A79E37A60852C959F1C776AEA48D328A75F8C683696CE74D55`,
`1CE258C697FC2A36401ADFC3DE84BB7EF5253E142159E79A474EA1`$)$

$Q = ($`13AC35CCA7052FE1368820D1CAFC23DB5F004681EB781C9319F39A1`,
`CD31941B339D9E6C6E54759E6C77C9A5FAF0BF5AB928F1EE63668F`$)$

$R = ($`19524EC31D1843F21AA0D8CF5318D83FA150A17FA519ACAF2E571A5`,
`DA7F2D3B1A16E78BF0704A07DD4FB438A0F23DCE8EEC04B3A50B2A`$)$

C217, $q = 128$, $\mathbb{F}_{2^7} = \mathbb{F}_2[w]/(w^7 + w + 1)$

$f(u) = w^{96}u^{63} + w^{79}u^{62} + w^{24}u^{60} + w^{122}u^{56} + w^{63}u^{48} + w^{60}u^{32} + w^{64}$

$h(u) = w^{48}u^{31} + w^{74}u^{30} + w^{36}u^{28} + w^{107}u^{24} + w^{11}u^{16} + w^{32}$

$$D_1 = \mathrm{div}(u^{31}+w^{97}u^{30}+w^{66}u^{29}+w^{111}u^{28}+w^{125}u^{27}+w^{58}u^{26}+w^{88}u^{25}+w^{96}u^{24}+w^{106}u^{23}+w^{68}u^{22}+ wu^{21}+w^{93}u^{20}+w^{108}u^{19}+w^{81}u^{18}+w^{107}u^{17}+w^{78}u^{16}+w^{113}u^{15}+w^{68}u^{14}+w^{115}u^{13}+w^{92}u^{12}+ w^{86}u^{11}+w^{67}u^{10}+w^{73}u^{9}+w^{42}u^{8}+wu^{7}+w^{46}u^{6}+w^{51}u^{5}+w^{116}u^{4}+w^{28}u^{3}+w^{99}u^{2}+w^{105}u+w^{29}, w^{7}u^{30}+w^{22}u^{29}+wu^{28}+w^{37}u^{27}+w^{114}u^{26}+w^{93}u^{25}+w^{57}u^{24}+w^{121}u^{23}+w^{117}u^{22}+w^{7}u^{21}+ w^{81}u^{20}+w^{98}u^{18}+w^{107}u^{17}+w^{84}u^{16}+w^{45}u^{15}+w^{86}u^{14}+w^{108}u^{13}+w^{90}u^{12}+w^{50}u^{11}+u^{10}+ w^{111}u^{9}+w^{16}u^{8}+w^{21}u^{7}+w^{44}u^{6}+w^{14}u^{5}+w^{93}u^{4}+w^{36}u^{3}+w^{118}u^{2}+w^{97}u+w^{3})$$

$$D_2 = \mathrm{div}(u^{31}+w^{47}u^{30}+w^{40}u^{29}+w^{39}u^{28}+w^{108}u^{27}+w^{113}u^{26}+w^{99}u^{25}+w^{87}u^{24}+w^{84}u^{23}+w^{33}u^{22}+ w^{46}u^{21}+w^{34}u^{20}+w^{16}u^{19}+w^{51}u^{18}+w^{39}u^{17}+w^{116}u^{16}+w^{41}u^{15}+w^{50}u^{14}+w^{121}u^{13}+w^{108}u^{12}+ w^{82}u^{11}+w^{74}u^{10}+w^{4}u^{9}+w^{118}u^{8}+w^{17}u^{7}+w^{95}u^{6}+w^{13}u^{5}+w^{23}u^{4}+w^{44}u^{3}+w^{29}u^{2}+w^{52}u+w^{7}, w^{105}u^{30}+w^{124}u^{29}+w^{91}u^{28}+w^{92}u^{27}+w^{102}u^{26}+w^{76}u^{25}+w^{2}u^{24}+w^{53}u^{23}+w^{98}u^{22}+w^{24}u^{21}+ w^{58}u^{20}+w^{64}u^{19}+w^{76}u^{18}+w^{24}u^{17}+w^{58}u^{16}+w^{5}u^{15}+w^{14}u^{14}+w^{19}u^{13}+w^{33}u^{12}+w^{14}u^{11}+ w^{71}u^{10}+w^{61}u^{9}+w^{125}u^{8}+w^{29}u^{7}+w^{73}u^{6}+w^{31}u^{5}+w^{25}u^{4}+w^{115}u^{3}+w^{73}u^{2}+w^{62}u+w^{70})$$

$$D_3 = \mathrm{div}(u^{31}+w^{111}u^{30}+w^{5}u^{29}+w^{74}u^{28}+w^{44}u^{27}+w^{25}u^{26}+w^{53}u^{25}+w^{15}u^{24}+w^{13}u^{23}+w^{44}u^{22}+ w^{23}u^{21}+w^{46}u^{20}+w^{122}u^{19}+w^{52}u^{18}+w^{55}u^{17}+w^{35}u^{16}+w^{81}u^{15}+w^{97}u^{14}+w^{14}u^{13}+w^{89}u^{12}+ w^{114}u^{11}+w^{24}u^{10}+w^{33}u^{9}+w^{87}u^{8}+w^{18}u^{7}+w^{83}u^{6}+w^{60}u^{5}+w^{100}u^{4}+w^{125}u^{3}+w^{68}u^{2}+ w^{44}u+w^{40},\ w^{39}u^{30}+w^{108}u^{29}+w^{51}u^{28}+w^{100}u^{27}+w^{8}u^{26}+w^{43}u^{25}+w^{108}u^{24}+w^{81}u^{23}+w^{12}u^{22}+ w^{21}u^{21}+w^{84}u^{20}+w^{15}u^{19}+w^{109}u^{18}+w^{114}u^{17}+w^{25}u^{16}+w^{18}u^{15}+w^{115}u^{14}+w^{122}u^{13}+u^{12}+ w^{74}u^{11}+w^{34}u^{10}+w^{60}u^{9}+w^{58}u^{8}+w^{6}u^{7}+w^{80}u^{6}+w^{68}u^{5}+w^{7}u^{4}+w^{6}u^{3}+w^{77}u^{2}+w^{31}u)$$

E248, $N = 248$, $\mathbb{F}_{2^{248}} = \mathbb{F}_2[z]/(z^{248} + z^{15} + z^{14} + z^{10} + 1)$, $\#\mathrm{E248}(\mathbb{F}_{2^{248}}) = 2 \cdot r$

$a =$ `C65B1B2B48E3A7B2BC69C365B4CAE385CE3F023A9742C0EF16C40E1D62ADA2`

$b =$ `1649390E2C5BBA8206486E33D3273AE269EE568F91AC46BC86A6A792CF6CEA`

$r =$ `80000000000000000000000000000004B55AAB05CC2C4EE2E6973D0C247E01`

$P =$ (`4AF353C030AADA55B6FAED2BBF314EBC28C8B6FB1DFC092728A28E70F0E73F`, `168FADD57DC3046C69A0121310D284A04C145E0ECB88B91BAD8BE25F58CBE9`)

$Q =$ (`62231B26EEF12154100D6257F7148AC78C5A61FC1295324494368A42CA9FD5`, `403910538623DE3633D0FD6690E12F4D81D1915D3728C5617CD6A65B92AA41`)

$R =$ (`D69A12AFCF86A8CF9F30051B8C655D050B238A215C19C8512D41B547C1ADE2`, `A3FDA75DB34F93EF657FAAB2163AE05E0CC1241175CE1E880841F77A369B8B`)

C248, $q = 256$, $\mathbb{F}_{2^8} = \mathbb{F}_2[w]/(w^8 + w^4 + w^3 + w^2 + 1)$

$f(u) = w^{51}u^{63} + w^{219}u^{62} + w^{223}u^{60} + w^{117}u^{56} + w^{234}u^{48} + wu^{32} + w^{39}$

$h(u) = w^{153}u^{31} + w^{178}u^{30} + w^{217}u^{28} + w^{186}u^{24} + w^{188}u^{16} + w^{187}$

$D_1 = \mathrm{div}(u^{31}+w^{111}u^{30}+w^{221}u^{29}+w^{204}u^{28}+w^{144}u^{27}+w^{62}u^{26}+w^{43}u^{25}+w^{56}u^{24}+w^{131}u^{23}+w^{110}u^{22}+ w^{31}u^{21}+w^{29}u^{20}+w^{47}u^{19}+w^{88}u^{18}+w^{250}u^{17}+w^{32}u^{16}+w^{162}u^{15}+w^{9}u^{14}+w^{19}u^{13}+w^{224}u^{12}+ w^{144}u^{11}+w^{97}u^{10}+w^{195}u^{9}+w^{27}u^{8}+w^{101}u^{7}+w^{60}u^{6}+w^{175}u^{5}+w^{36}u^{4}+w^{195}u^{3}+w^{131}u^{2}+w^{228}u+ w^{168},\ w^{140}u^{30}+w^{159}u^{29}+w^{51}u^{28}+w^{210}u^{27}+w^{180}u^{26}+w^{172}u^{25}+w^{147}u^{24}+w^{20}u^{23}+w^{143}u^{22}+ w^{196}u^{21}+w^{8}u^{20}+w^{126}u^{19}+w^{236}u^{18}+w^{141}u^{17}+w^{174}u^{16}+w^{213}u^{15}+w^{115}u^{14}+w^{66}u^{13}+w^{147}u^{12}+ w^{145}u^{11}+w^{100}u^{10}+w^{105}u^{9}+w^{42}u^{8}+w^{97}u^{7}+w^{219}u^{6}+w^{133}u^{5}+w^{123}u^{4}+w^{47}u^{3}+w^{239}u^{2}+w^{233}u+ w^{58})$

$D_2 = \mathrm{div}(u^{31}+w^{236}u^{30}+w^{210}u^{29}+w^{144}u^{28}+w^{242}u^{27}+w^{40}u^{26}+w^{141}u^{25}+w^{52}u^{24}+w^{137}u^{23}+w^{53}u^{22}+ w^{10}u^{21}+w^{245}u^{20}+w^{175}u^{19}+w^{28}u^{18}+w^{202}u^{17}+w^{23}u^{16}+w^{128}u^{15}+w^{209}u^{14}+w^{13}u^{13}+w^{170}u^{12}+ w^{76}u^{11}+w^{70}u^{10}+w^{116}u^{9}+w^{134}u^{8}+w^{218}u^{7}+w^{93}u^{6}+w^{53}u^{5}+w^{51}u^{4}+w^{168}u^{3}+w^{232}u^{2}+w^{232}u+ w^{22},\ w^{48}u^{30}+w^{223}u^{29}+w^{35}u^{28}+w^{139}u^{27}+w^{66}u^{26}+w^{157}u^{25}+w^{101}u^{24}+w^{251}u^{23}+w^{186}u^{22}+ w^{149}u^{21}+w^{224}u^{20}+w^{83}u^{19}+w^{223}u^{18}+w^{102}u^{17}+w^{154}u^{16}+w^{96}u^{15}+w^{13}u^{14}+w^{123}u^{13}+w^{7}u^{12}+ w^{129}u^{11}+w^{86}u^{10}+w^{115}u^{9}+w^{111}u^{8}+w^{99}u^{7}+w^{161}u^{6}+w^{78}u^{5}+w^{86}u^{4}+w^{60}u^{3}+w^{204}u^{2}+w^{54}u+ w^{85})$

$D_3 = \mathrm{div}(u^{31}+w^{74}u^{30}+w^{68}u^{29}+w^{111}u^{28}+w^{44}u^{27}+w^{242}u^{26}+w^{160}u^{25}+w^{252}u^{24}+w^{111}u^{23}+w^{79}u^{22}+ w^{140}u^{21}+w^{98}u^{20}+w^{35}u^{19}+u^{18}+w^{238}u^{17}+w^{205}u^{16}+w^{77}u^{15}+w^{216}u^{14}+w^{215}u^{13}+w^{195}u^{12}+ w^{138}u^{11}+w^{124}u^{10}+w^{82}u^{9}+w^{113}u^{8}+w^{3}u^{7}+w^{58}u^{6}+w^{231}u^{5}+w^{248}u^{4}+w^{97}u^{3}+w^{140}u^{2}+w^{131}u+ w^{249},\ w^{52}u^{30}+w^{219}u^{29}+w^{5}u^{28}+w^{221}u^{27}+w^{210}u^{26}+w^{177}u^{25}+w^{210}u^{24}+w^{41}u^{23}+w^{198}u^{22}+ w^{62}u^{21}+w^{105}u^{20}+w^{64}u^{19}+w^{163}u^{18}+w^{36}u^{17}+w^{219}u^{16}+w^{238}u^{15}+w^{108}u^{14}+w^{7}u^{13}+w^{21}u^{12}+ w^{131}u^{11}+w^{224}u^{10}+w^{6}u^{9}+w^{50}u^{8}+w^{17}u^{7}+w^{241}u^{6}+w^{84}u^{5}+w^{247}u^{4}+w^{105}u^{3}+w^{37}u^{2}+w^{57}u+ w^{230})$

E300, $N = 300$, $\mathbb{F}_{2^{300}} = \mathbb{F}_2[z]/(z^{300} + z^5 + 1)$, $\#\mathrm{E300}(\mathbb{F}_{2^{300}}) = 2 \cdot r$

$a =$ 8F8EEC356CB05D6FC50A73F3639AB70C19A18E5234A172276EE631E42A6A2CE5A28250424E4

$b =$ 44808A33D47780EC13CC721C66605252A082008AC5910272188638236 8CCB415802A4E95ACE

$r =$ 7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF09A007BD6359747C0A7181FC6DA9704EFB0C1

$P =$ (9F080369EA917727D1E1C709CC5BF2674AA7C79A2DFA5E5B447F364F61690CD6DBAC05F5EFD,
558B8FB728CECBB9D0AA367687E17D6E97793769C71645AA168EEDCA3E2AE03D642B722572)

$Q =$ (F93C3685D5E9AB2A0F7C7BD7F687A9C4E42C10C94BD477F419E5C25B6E643B919F51CB3730B,
4C11A5F31FAD729F839F98D34FB59D279C70A3126FFC3D5C1611F949340EEE12474A66263AC)

$R =$ (FF00541676FD0036D12C0FEC3A1B8D8C692627F4E8DB62F45B708D9431C2E99F299984FD406,
37E09E68926A8157861A512A86696A4A78A0F0C15F9EAC4AECF8BF6D2B818284E8C3F5853BD)

C300, $q = 2^{20}$, $\mathbb{F}_{2^{20}} = \mathbb{F}_2[w]/(w^{20} + w^{10} + w^9 + w^7 + w^6 + w^5 + w^4 + w + 1)$

$f(u) = w^{327321}u^{31} + w^{349092}u^{30} + w^{995286}u^{28} + w^{930226}u^{24} + w^{602756}u^{16} + w^{602843}$

$h(u) = w^{687948}u^{15} + w^{946981}u^{14} + w^{169852}u^{12} + w^{811172}u^8 + w^{458632}$

$D_1 = \mathrm{div}(u^{15}+w^{173675}u^{14}+w^{1014246}u^{13}+w^{193959}u^{12}+w^{558539}u^{11}+w^{376720}u^{10}+w^{149697}u^9+w^{852573}u^8+$
$w^{522198}u^7+w^{78372}u^6+w^{576415}u^5+w^{577000}u^4+w^{1025691}u^3+w^{1030913}u^2+w^{224944}u+w^{165103},$
$w^{153473}u^{14}+w^{159391}u^{13}+w^{624451}u^{12}+w^{540652}u^{11}+w^{1026818}u^{10}+w^{895055}u^9+w^{925553}u^8+$
$w^{700268}u^7+w^{449406}u^6+w^{518791}u^5+w^{428720}u^4+w^{109656}u^3+w^{362556}u^2+w^{818181}u+w^{438018})$

$D_2 = \mathrm{div}(u^{15}+w^{672767}u^{14}+w^{60108}u^{13}+w^{592469}u^{12}+w^{806912}u^{11}+w^{209094}u^{10}+w^{21555}u^9+w^{351715}u^8+$
$w^{1006855}u^7+w^{553595}u^6+w^{115789}u^5+w^{940657}u^4+w^{411255}u^3+w^{553233}u^2+w^{410382}u+w^{440174},$
$w^{456657}u^{14}+w^{165272}u^{13}+w^{940178}u^{12}+w^{506617}u^{11}+w^{970890}u^{10}+w^{791679}u^9+w^{336652}u^8+$
$w^{568666}u^7+w^{937671}u^6+w^{23894}u^5+w^{617541}u^4+w^{400003}u^3+w^{792481}u^2+w^{36607}u+w^{409913})$

$D_3 = \mathrm{div}(u^{15}+w^{745174}u^{14}+w^{152075}u^{13}+w^{759312}u^{12}+w^{254997}u^{11}+w^{718088}u^{10}+w^{134849}u^9+w^{84810}u^8+$
$w^{1017558}u^7+w^{909326}u^6+w^{549738}u^5+w^{64404}u^4+w^{337345}u^3+w^{700483}u^2+w^{960561}u+w^{789792},$
$w^{163511}u^{14}+w^{370136}u^{13}+w^{421951}u^{12}+w^{972631}u^{11}+w^{113274}u^{10}+w^{380219}u^9+w^{648060}u^8+$
$w^{564150}u^7+w^{642068}u^6+w^{819577}u^5+w^{633633}u^4+w^{662299}u^3+w^{542356}u^2+w^{473005}u+w^{146842})$

E161-2, $N = 161$, $\mathbb{F}_{2^{161}} = \mathbb{F}_2[z]/(z^{161} + z^{18} + 1)$, $\#\mathrm{E161}(\mathbb{F}_{2^{161}}) = 2 \cdot r$, $a = 1$

$b =$ `10000000000000000000000000000000000000062`

$r =$ `FFFFFFFFFFFFFFFFFFFFD5D528D29B3677A6BF15`

$P =$ (`1590236CF8BCADEA57D2ABABDC7C918CD991F7FD1`, `16019BB593140463E7C859426E4AD76188D4EA3C8`)

$Q =$ (`ACA7F2D366101B27A6043551C0B0D8C60A32ED98`, `C15307FE705B5A5D638B40DF023D202E434D7D75`)

E176, $N = 176$, $\mathbb{F}_{2^{176}} = \mathbb{F}_2[z]/(z^{176} + z^{43} + z^2 + z + 1)$, $\#\mathrm{E176}(\mathbb{F}_{2^{176}}) = 65390 \cdot r$

$a =$ `E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B`

$b =$ `5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2`

$r =$ `10092537397ECA4F6145799D62B0A19CE06FE26AD`

$P =$ (`96E2498B189AAD455FC2431323B24E0603155C4EEE24`,
`2056F497331B645ACAB8519F3F71099A71EBDD7E2D06`)

$Q =$ (`8CE8805EA1D92A77975F69988FF0B2C99A3C344D469D`,
`27A65C20DA08E0732D6327CF41E3C4B27AB9DB63706A`)

E272, $N = 272$, $\mathbb{F}_{2^{272}} = \mathbb{F}_2[z]/(z^{272} + z^{56} + z^3 + z + 1)$, $\#\mathrm{E272}(\mathbb{F}_{2^{272}}) = 65286 \cdot r$

$a =$ `91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBACDB586FB20`

$b =$ `7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8482E540F7`

$r =$ `100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E629521`

$P =$ (`DE9DE5CD3B90447A206BEFE8167505CB7A28616DADABC639B421DF763F961D689DA9`,
`49831637686123445336FE8B59FF791C71CF455823A4C375280A148B043DE7ECF17F`)

$Q =$ (`C9189420F828C242771E2D64768930089AB56BA7E6D3A1DB294AEDAD60BAC9591E65`,
`EB0123561D81715B23575A5DF3B13A771C8521523C4EA853C0C4DF3294F70BF65AAA`)