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

Abstract

In this paper, the authors 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 $\mathbb{F}_{2^N}$, $N \in [100, 600]$, elliptic curve parameters are identified 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 $\mathbb{F}_{2^N}$. The feasibility of the GHS attack on the specific elliptic curves is examined over $\mathbb{F}_{2^{176}}$, $\mathbb{F}_{2^{208}}$, $\mathbb{F}_{2^{272}}$, $\mathbb{F}_{2^{304}}$ and $\mathbb{F}_{2^{368}}$, which are provided as examples in the ANSI X9.62 standard for the elliptic curve signature scheme ECDSA. Finally, several concrete instances are provided of the ECDLP over $\mathbb{F}_{2^N}$, N composite, of increasing difficulty; these resist all previously known attacks, but are within reach of the GHS attack.

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 as follows: 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 provide maximum resistance to the Pohlig–Hellman [28] and Pollard's rho [29, 26] 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 resist the Weil pairing [24] and Tate pairing [11] attacks.

Frey [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 [13]. 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 for the security of elliptic curve cryptographic schemes.

The GHS attack was analyzed in [17, 23]. It was proven to fail for *all* cryptographically interesting elliptic curves over $\mathbb{F}_{2^N}$, where $N \in [160, 600]$ is prime. In other words, the hyperelliptic curves C that are 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 ($g \geqslant 2^{16} - 1$, 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. Section 2 provides a brief introduction to the relevant theory of hyperelliptic curves. The GHS Weil descent attack is outlined in Section 3, and an overview of the best methods known for solving the ECDLP and HCDLP is given in Section 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 Section 5. In Section 6, a detailed analysis is presented of the feasibility of the GHS attack on certain elliptic curves specified in the ANSI X9.62 standard. Section 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 Section 8.

2. *Hyperelliptic curves*

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

2.1. *Hyperelliptic curves*

Let $k = \mathbb{F}_q$ denote the finite field of order q. The *algebraic closure* of $\mathbb{F}_q$ is $\bar{k} = \bigcup_{n \geqslant 1} \mathbb{F}_{q^n}$. 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 $\deg h \leqslant g$. 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 $\tilde{P} = (x, -y - h(x))$; we also define $\tilde{\infty} = \infty$. Note that $\tilde{P} \in C(L)$. 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.

2.2. *The Jacobian of a hyperelliptic curve*

The set D^0 of *degree zero divisors* of C is the set of formal sums $\sum_{P \in C(\bar{k})} m_P P$, where $m_P \in \mathbb{Z}$, $\sum m_P = 0$, and only a finite number of the values of m_P 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 $\sigma : \bar{k} \to \bar{k}$ be the *Frobenius map* defined by $x \mapsto x^q$. The map σ extends to $C(\bar{k})$ 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

$$D_k^0 = \{D \in D^0 \;:\; D^\sigma = D\}.$$

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 $z \in k(C)$, the *divisor of z* is $\operatorname{div}(z) = \sum_{P \in C(\bar{k})} v_P(z) P$, where $v_P(z)$ denotes the multiplicity of P as a root of z. Now the set $\operatorname{Prin}_k = \{\operatorname{div}(z) \;:\; z \in k(C)\}$ is a subgroup of D_k^0. The *Jacobian* of C (over k) is the quotient group $J_C(k) = D_k^0/\operatorname{Prin}_k$.

2.3. *Properties of the Jacobian*

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

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

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* – that is, a divisor $\sum_{P \neq \infty} m_P P - (\sum_{P \neq \infty} m_P) \infty$ satisfying: (i) $m_P \geqslant 0$ for all P; (ii) if $m_P \geqslant 1$ and $P \neq \tilde{P}$, then $m_{\tilde{P}} = 0$; (iii) m_P is equal to 0 or 1 if $P = \tilde{P}$; and (iv) $\sum m_P \leqslant g$. Such a *reduced divisor* D can be uniquely represented by a pair of polynomials $a, b \in k[u]$, where: (i) $\deg b < \deg a \leqslant g$; (ii) a is monic; and (iii) $a | (b^2 + bh - f)$. We write $D = \operatorname{div}(a, b)$ to mean that $D = \gcd(\operatorname{div}(a), \operatorname{div}(b - v))$, 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, 22] can be used to compute the sum of two reduced divisors efficiently, and to express the sum in reduced form.

2.4. *Artin's bound*

In the above, we considered only 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. Then $h = 0$ in (1). Artin [3] showed that

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

Here, $\tau_v = \sum_{\deg F = v} [f/F]$, where the summation is over all degree-v monic polynomials $F \in \mathbb{F}_p[u]$ coprime to f, and $[f/F]$ is the polynomial Legendre symbol. We trivially have $|\tau_v| \leqslant p^v$, and Artin showed that $|\tau_v| \leqslant p^g$ ($0 \leqslant v \leqslant 2g$) if $\deg f = 2g + 1$, and $\tau_{2g+1} = -p^g$ and $|\tau_v| \leqslant 2p^g$ ($1 \leqslant v \leqslant 2g$) 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 $\chi(F) = [f/F]$ by the general quadratic character. That is, for a monic irreducible polynomial $F \in \mathbb{F}_q[u]$ coprime to f, let $\chi(F)$ be equal to 1 or -1, depending on whether the equation $v^2 + h(u)v \equiv f(u) \pmod{F(u)}$ has a solution $v \pmod{F(u)}$, or not. It follows that

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

Since over constant fields of characteristic two the real case is strictly more general than the imaginary case (see [**27**]), we work with

$$B_2 := \big((2g + 1)^2 - g(g + 1)\big)q^g + \sum_{\nu=1}^{g} \nu q^\nu \tag{3}$$

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

$$B_1 := (\sqrt{q} + 1)^{2g}. \tag{4}$$

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 eventually obtain the hyperelliptic curve C from an irreducible reduced component in the intersection. We call their reduction algorithm, together with the fastest known algorithm for solving the hyperelliptic curve discrete logarithm problem (see Subsection 4.2), the *GHS attack* on the ECDLP. The following theorem is proved 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 $0 \leqslant i \leqslant n - 1$. Let the magic number *for E relative to n be*

$$m = m(b) = \dim_{\mathbb{F}_2} \big(\mathrm{Span}_{\mathbb{F}_2} \big\{ \big(1, b_0^{1/2}\big), \big(1, b_1^{1/2}\big), \ldots, \big(1, b_{n-1}^{1/2}\big) \big\} \big). \tag{5}$$

Assume that

$$n \text{ is odd}, \quad or \quad m(b) = n, \quad or \quad \mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0. \tag{6}$$

Then the GHS reduction constructs an explicit group homomorphism

$$\phi : E(\mathbb{F}_{q^n}) \to J_C(\mathbb{F}_q), \tag{7}$$

where C is a hyperelliptic curve defined over $\mathbb{F}_q$ of genus g equal to 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; that is, $\#E(\mathbb{F}_{q^n}) = rd$, 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 $J_C(\mathbb{F}_q)$. In other words, given $P, Q \in \langle P \rangle$, 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 $ng \leqslant 1000$, our extensive experiments suggest that Hess's KASH implementation [**18, 6**] of the algorithm takes at most a few hours on a workstation.

Formula (5) was analyzed in [**23**], and Theorem 5 below 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 are distinct irreducible polynomials over $\mathbb{F}_2$ with $\deg(f_i) = d_i$ and $1 = d_0 < d_1 \leqslant d_2 \leqslant \cdots \leqslant d_s$. 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 that divides $\mathrm{Ord}_b(x)$. The *type* of b is defined to be $(j_0, j_1, \ldots, j_s)$.

THEOREM 5 (*see* [**23**]). *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*

$$\prod_{i=0, \, j_i \neq 0}^{s} \left(q^{j_i d_i} - q^{(j_i - 1) d_i} \right).$$

Lemma 6 asserts that condition (6) 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 (6) can be replaced by the following, weaker, condition:*

$$n \text{ is odd}, \quad or \quad j_0 = 2^e, \quad or \quad \mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0. \tag{8}$$

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 $j_0 = 2^e$. Thus, (6) indeed implies (8).

Now, let $\overline{f} = (x - 1)^c \prod_{i=0}^{s} f_i^{j_i}$, 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 [**17**, Proof of Lemma 11].) Let $\overline{h} = (x^n - 1)/\overline{f}$. From [**17**, Proof of Lemma 11] 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 $j_0 = 2^e$, the lemma is established. $\qquad\square$

The following equivalent formulation, which has been adapted from [**33**], is also useful.

LEMMA 7. *Condition (8) is equivalent to the following condition:*

$$\gcd \left(\frac{x^n - 1}{\mathrm{lcm}(\mathrm{Ord}_b(x), x - 1)}, x - 1 \right) = 1 \quad or \quad \mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0. \tag{9}$$

Proof. Let $H(x) = \gcd((x^n - 1)/(\mathrm{lcm}(\mathrm{Ord}_b(x), x - 1), x - 1))$. We show that $H(x) = 1$ if and only if n is odd or $j_0 = 2^e$. If n is odd, then $x - 1$ exactly divides $x^n - 1$, and thus

$H(x) = 1$. Now assume that n is even. Then $n = 2^e n_1$ with n_1 odd and $e \geqslant 1$. Let $h = 2^e$. Since $\mathrm{Ord}_b(x)$ divides $x^n - 1$ and $x^n - 1 = (f_0 f_1 \cdots f_s)^h$, we have

$$H(x) = 1 \iff (x - 1) \nmid \frac{x^n - 1}{\mathrm{lcm}(\mathrm{Ord}_b(x), x - 1)}$$
$$\iff f_0{}^h \| \mathrm{Ord}_b(x)$$
$$\iff j_0 = h.$$

This completes the proof. $\qquad\square$

There are $2^{N+1} - 2$ isomorphism classes of elliptic curves over $\mathbb{F}_{2^N}$ with representatives $y^2 + xy = x^3 + b$ and $y^2 + xy = x^3 + ax^2 + b$, 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 (8) can be efficiently computed using the following lemma.

LEMMA 8. *Let* $n, m \in [1, n]$ *be fixed. Let* $c_{i,j} = q^{jd_i} - q^{(j-1)d_i}$ *for* $0 \leqslant i \leqslant s$ *and* $1 \leqslant j \leqslant h$. *Let*

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

Let $F_i(z) = 1 + \sum_{j=1}^h c_{i,j} z^{jd_i}$ *for* $1 \leqslant i \leqslant s$, *and let* $F(z) = F_0(z) \prod_{i=1}^s F_i(z)$. *Then the number of isomorphism classes of elliptic curves over* $\mathbb{F}_{2^N}$ *with magic number* m *relative to* n *and satisfying* (8) *is* $I = [z^m] F(z)$, *where '[ ]' denotes the coefficient operator.*

Proof. This follows immediately from Theorem 5 and Lemma 6. $\qquad\square$

In Section 5, we shall be interested in cryptographically interesting elliptic curves that have a magic number m relative to n. For certain pairs (n, m), some (or even all) of the elliptic curves that have a magic number m relative to n should be eliminated from consideration because they are defined over a proper subfield $\mathbb{F}_{q^\mu}$ of $\mathbb{F}_{q^n}$ (with $q^\mu \geqslant 8$), in which case $\#E(\mathbb{F}_{q^\mu})$ is a non-trivial factor of $\#E(\mathbb{F}_{q^n})$, whence E is not cryptographically interesting. Such subfield curves can be identified by the following result.

LEMMA 9. *Let* $E/\mathbb{F}_{q^n}$ *be an elliptic curve defined by the equation* $y^2 + xy = x^3 + ax^2 + b$, *and suppose that* (9) *holds. Let* μ *be the smallest divisor of* n *such that* $\mathrm{Ord}_b(x)$ *divides* $x^\mu - 1$ *over* $\mathbb{F}_2$. *Then* E *is isomorphic to an elliptic curve defined over* $\mathbb{F}_{q^\mu}$.

Proof. By assumption, we have $\sigma^\mu(b) - b = 0$; that is, $b^{q^\mu} = b$. Therefore, $b \in \mathbb{F}_{q^\mu}$, and (because of the minimality of μ) b is not contained in a proper subfield of $\mathbb{F}_{q^\mu}$. Now, if n/μ is odd, there exists an element $c \in \mathbb{F}_{q^\mu}$ such that $\mathrm{Tr}_{K/\mathbb{F}_2}(c) = 1$. Therefore, both for $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$ and for $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 1$, there exists a curve isomorphic to E that is defined over $\mathbb{F}_{q^\mu}$ but not over any proper subfield of $\mathbb{F}_{q^\mu}$. On the other hand, if n/μ is even, then μ divides $n/2$ and $x^\mu - 1$ divides $x^{n/2} - 1$. Since $\mathrm{lcm}(\mathrm{Ord}_b(x), x - 1)$ divides $x^\mu - 1$, this implies that $\gcd((x^n - 1)(\mathrm{lcm}(\mathrm{Ord}_b(x), x - 1)), x - 1) = x - 1$, so that by (9) we have $\mathrm{Tr}_{K/\mathbb{F}_2}(a) = 0$. Again, it follows that there exists a curve isomorphic to E that is defined over $\mathbb{F}_{q^\mu}$ but not over any proper subfield of $\mathbb{F}_{q^\mu}$. $\qquad\square$

COROLLARY 10. *Let* $E/\mathbb{F}_{q^n}$ *be an elliptic curve defined by the equation* $y^2 + xy = x^3 + ax^2 + b$, *and suppose that* (9) *holds. Then* E *is isomorphic to an elliptic curve defined over a proper subfield* $\mathbb{F}_{q^\mu}$ *of* $\mathbb{F}_{q^n}$ *if and only if* $\mathrm{Ord}_b(x)$ *divides* $x^\mu - 1$ *for some proper divisor* μ *of* n.

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

THEOREM 11 (*see* [23]). *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 the following statements hold.*

(i) *$x^n - 1$ factors over $\mathbb{F}_2$ as $(x-1)f_1 f_2 \cdots f_s$, where the functions f_i 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*

$$B = \left\{ b \in \mathbb{F}_{q^n} \setminus \mathbb{F}_q : (\sigma - 1) f_i(\sigma)(b) = 0 \text{ for some } 1 \leqslant i \leqslant s \right\},$$

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 [29, 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 [26]), 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.

DEFINITION 12 (ENGE–GAUDRY ALGORITHM). We describe the Enge–Gaudry (EG) index-calculus algorithm [16, 8] 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 $\max\{\deg a_i\} \leqslant t$.

In the Enge–Gaudry algorithm, a *smoothness bound* t is first chosen. Next, the *factor base* $\{P_1, P_2, \dots, P_w\}$ is constructed: for each prime divisor $D = \mathrm{div}(a, b)$ of degree less than or equal to t, exactly one of D and $-D$ is included in the factor base. Then, a random walk (á la Teske [32]) 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

$$\sum_{i=1}^{w+5} \gamma_i (e_{i1}, e_{i2}, \dots, e_{iw}) = (0, 0, \dots, 0).$$

Thus $\sum_{i=1}^{w+5} \gamma_i R_i = 0$, whence

$$\sum \gamma_i (\alpha_i D_1 + \beta_i D_2) = 0 \quad \text{and} \quad \log_{D_1} D_2 = -\left(\sum \gamma_i \alpha_i\right) / \left(\sum \gamma_i \beta_i\right) \bmod r.$$

4.3. Analysis

The EG algorithm has a subexponential-time running time of

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

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 [20]. A good approximation for the number A_l of prime divisors of degree l in the factor base is

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

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

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

By [20, 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

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

The system of sparse linear equations can be solved using Lanczos's algorithm [5]. A good estimate for the expected running time is $\alpha(F(t) + 5)^2$ arithmetic operations modulo n, where α is the average number of non-zero coefficients in an equation. Since $\alpha \leqslant g$, the approximation

$$L(t) = F(t)^2 \tag{15}$$

that we will use henceforth for the running time of the linear algebra stage is a reasonably good one.

5. Analysis

For each composite $N \in [100, 600]$, we determine and compare the running times of the GHS attack and Pollard's rho method for solving the ECDLP in (potentially) cryptographically interesting elliptic curves over $\mathbb{F}_{2^N}$.

Algorithm 13 determines the elliptic curve parameters (in terms of n, m and g) such that:

(i) there should exist (see Remark 21) 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 $\mathbb{F}_{2^N}$.

5.1. *Cases of Algorithm* 13

Three cases are considered.

Case 1. The first case, denoted by EG1, considers only GHS attack parameters where the factor base has size at most $10^7 \approx 2^{23}$. Solving sparse linear systems of this dimension is on the edge of what is considered feasible today [21]. Thus the EG1 running times are restricted to ECDLP instances where the linear algebra stage of the GHS attack is feasible today.

If the number A_1 of degree-one divisors is greater than 10^7 for some hyperelliptic curve of genus g over $\mathbb{F}_{2^l}$, then, in order to achieve a factor base size less than or equal to 10^7, the Enge–Gaudry algorithm could be modified by selecting the factor base to consist of only a proportion $1/\varepsilon$ of all prime divisors of degree 1; see [17]. However, the expected time to find a smooth divisor will be increased by a factor of ε^g. We therefore decided not to consider this modification in our analysis.

Case 2. The second case, denoted by EG2, places no restriction on the factor base size, nor does it take into account the running time of the linear algebra stage when selecting the optimal elliptic curve parameters. Listing EG2 running times is important, because they will become relevant should faster algorithms be discovered for solving sparse linear systems.

Case 3. The third case, denoted by EG3, places no restriction on the factor base size, but *does* consider the running time of the linear algebra stage when selecting the optimal elliptic curve parameters.

5.2. *Running times*

We express the running time for Pollard's rho method in terms of elliptic curve operations. For the EG1 and EG2 cases, the running times for the GHS attack are expressed in terms of random-walk iterations in the Jacobian of the hyperelliptic curve. We do not consider the different bit-complexities of operations for elliptic and hyperelliptic curves, since these are expected to be roughly the same. For the running time of the GHS attack in the EG3 case, both the number of random-walk iterations and the number of steps in the linear algebra stage are considered. Comparing the running times of the two stages is problematic because of the different bit-complexities for the basic operations involved and because, unlike the linear algebra stage, the random-walk stage can be easily parallelized on a large distributed system of computers, since the individual processors do not have to communicate with each other. Nevertheless, for the sake of concreteness, we select GHS attack parameters in the EG3 case, so that the maximum of the running times of the two stages is minimized. As was justified in Remark 3, we can ignore the time spent on mapping the ECDLP instance to a HCDLP instance in each of the EG1, EG2 and EG3 cases.

ALGORITHM 13 (FINDING OPTIMAL GHS ATTACK PARAMETERS).
INPUT: N, 'EG1' or 'EG2' or 'EG3'.
OUTPUT: Parameters n, m and g, for which there should exist a cryptographically interesting elliptic curve over $\mathbb{F}_{2^N}$ whose ECDLP is most easily solved with the GHS attack; optimal smoothness bound t; (estimated) factor base size F; (estimated) expected running time T in terms of random-walk iterations; and, in the EG3 case, (estimated) maximum T_M of the running times of the random-walk and linear algebra stages.

1. For all divisors $n \geqslant 2$ 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 $l \geqslant 25$, 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) { Find the irreducible factors of $x^{n_1} - 1$ over $\mathbb{F}_2$ and their degrees. }
       Factor $x^{n_1} - 1 = f_0(x) f_1(x) \cdots f_s(x)$, where the f_i are irreducible over $\mathbb{F}_2$, and where $1 = d_0 \leqslant d_1 \leqslant d_2 \leqslant \cdots \leqslant d_s$, where $d_i = \deg(f_i)$.
   (e) { Compute a lower bound m' on the magic number m relative to n that yields a large enough Jacobian (see Remark 14). }
       For $m' = 2, 3, \ldots, n$, do the following.
       (i) Set $g \leftarrow 2^{m'-1} - 1$. Compute B_1 and B_2 as defined in (4) and (3).
       (ii) If $\min\{\log_2 B_1, \log_2 B_2\} \geqslant N - 3$, then go to step 1(f).
       (iii) Set $g \leftarrow 2^{m'-1}$. Compute B_1 and B_2 as defined in (4) and (3).
       (iv) If $\min\{\log_2 B_1, \log_2 B_2\} \geqslant N - 3$, then go to step 1(f).
   (f) { Find the smallest admissible magic number m relative to n (see 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 $0 \leqslant j_i \leqslant h$, $j_0 \geqslant 1$, then:
           { Determine if there are any elliptic curves having magic number m relative to n that are *not* defined over a proper subfield $\mathbb{F}_{q^\mu}$ of $\mathbb{F}_{q^n}$ (see Remark 15). }
           For each expression $m = \sum_{i=0}^{s} d_i j_i$ with $0 \leqslant j_i \leqslant h$, $j_0 \geqslant 1$, do the following.
           (i) Let $f(x) = \prod_{i=0}^{s} f_i(x)^{j_i}$.
           (ii) Let μ be the smallest divisor of n such that $f(x)$ divides $x^\mu - 1$.
           (iii) If $\mu = n$, 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 (that is, if $gl \leqslant 4096$; see Remark 16), 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 $\#J_C(\mathbb{F}_q) = 2^{gl}$,
       (14) to estimate the expected running time $T(t)$ of the random-walk stage, and
       (15) to estimate the running time $L(t)$ of the linear algebra stage. }
       If $gl \geqslant 4097$, then set $T_n \leftarrow \infty$.
       Else:
       (i) Case EG1: set $S \leftarrow \{1 \leqslant t \leqslant 120 \ : \ F(t) \leqslant 10^7\}$.
           Case EG2 or EG3: set $S \leftarrow \{1, 2, \ldots, 120\}$.

(ii) Case EG1 or EG2: let t be the index in S that minimizes $T(t)$.
     Case EG3: let t be the index in S that minimizes $T_M(t) = \max\{T(t), L(t)\}$.

(iii) Set $m_n \leftarrow m$; $g_n \leftarrow g$; $t_n \leftarrow t$; $F_n \leftarrow F(t_n)$.
      Case EG1 or EG2: set $T_n \leftarrow T(t_n)$.
      Case EG3: set $T_n \leftarrow T_M(t_n)$.

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

5.3. *Explanations of some steps of Algorithm* 13

REMARK 14 (LOWER BOUND ON $\log_2 B_1$ AND $\log_2 B_2$). 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

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

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

REMARK 15 (ELIMINATION OF SUBFIELD CURVES). 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 these is 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 (see Lemma 6, condition (8)), we need $\text{Tr}_{K/\mathbb{F}_2}(a) = 0$; that is, 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 the 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 $\#E(\mathbb{F}_{2^{152}})$. Corollary 10 is therefore used in step 1(f) of Algorithm 13 to eliminate from consideration elliptic curves defined over a proper subfield $\mathbb{F}_{q^\mu}$ of $\mathbb{F}_{q^n}$. Note that step 1(f) does not exclude elliptic curves E defined over proper subfields of $\mathbb{F}_{q^n}$ not containing $\mathbb{F}_q$. However, we expect that such elliptic curves will be uniformly distributed among the classes of curves identified by $\text{Ord}_b(x)$ (relative to the Frobenius map $\alpha \mapsto \alpha^q$), so they will not significantly affect the counts I of potentially cryptographically interesting elliptic curves having a certain magic number m relative to n.

REMARK 16 (THE RESTRICTION THAT $gl \leqslant 4096$). For $g \geqslant 4097$, we were unable to compute the expected running time of EG1, EG2 or EG3 because of computational limitations when computing the Taylor series expansions needed to evaluate $M(t)$ (see formula (12)). We therefore ignore all instances (n, l, g) where $gl \geqslant 4097$. 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 obtained 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 $N = 600$.

5.4. *Analysis*

The outputs of Algorithm 13 with composite $N \in [100, 600]$ as inputs are listed in Appendix A. For the purposes of illustration, a small excerpt from this table is given in Table 1. In these tables, the entries for F, T, T_M and ρ are the *logarithms* (base 2, rounded to the nearest integer) of the factor base size $F(t)$, the expected number $T(t)$ of random-walk iterations in the Enge–Gaudry algorithm, the maximum $T_M(t)$ of $T(t)$ and $L(t)$, 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, while $D3$ denotes the difference $\rho - T_M$ (if positive) for EG3. I denotes the logarithm (base 2, rounded) of the number of isomorphism classes of elliptic curves which have a magic number m relative to n satisfying (8), and which are not defined over a proper subfield $\mathbb{F}_{q^\mu}$ of $\mathbb{F}_{q^n}$. If for some N data is given for EG2 or EG3 but not for EG1, we are in the situation that $gl \geqslant 4097$ for all divisors $l \leqslant 24$ of N (such as for $N = 164$ and 166 in Table 1). If for some N data is given for none of EG1, EG2 or EG3, we are in the situation that $gl \geqslant 4097$ for all l dividing N (such as for $N = 169$ in Table 1).

REMARK 17 (FURTHER LIMITATIONS OF OUR ANALYSIS). Our analysis yields the same running times whenever (g, l) are the same, independently of N (for example, $T = 59$ when $(g, l) = (15, 20)$ for both $N = 160$ and $N = 280$ in the EG1 case; 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 expect that $\#J_C(\mathbb{F}_q)$ will be divisible only 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 $(\sqrt{2} - 1)^{2g} \leqslant \#J_C(\mathbb{F}_2)$ is trivial. For example, if $(l, g) = (1, 511)$, we have $T = 2^{105}$ for EG1 for $N = 170, 465, 508, 510$ and 511. 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 18 (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 such curves, and the GHS attack is successful in reducing instances of the ECDLP on these curves to instances of the HCDLP that are solvable using known algorithms and existing computer technology. Examples of such N are 161, 180, 186, 217, 248, 300 (see Section 7).

For many other composite $N \in [160, 600]$, the GHS attack, though infeasible today, is successful in that it is significantly faster than Pollard's rho algorithm for solving the ECDLP on a large class of elliptic curves over $\mathbb{F}_{2^N}$. A striking example is $N = 600$, where the GHS attack can solve the ECDLP on 2^{202} curves over $\mathbb{F}_{2^{600}}$ in about 2^{79} steps, which is less than the 2^{299} steps for Pollard's rho algorithm.

Table 1: Sample output of Algorithm 13 (see Appendix A).

EG1	N	n	l	m	g	I	t	F	T	ρ	$D1$
	160	8	20	5	15	100	1	19	59	79	20
	161	7	23	4	7	94	1	22	34	80	46
	162	9	18	7	63	127	1	17	307	80	–
	164	–	–	–	–	–	–	–	–	–	–
	165	15	11	5	15	57	2	20	37	82	45
	166	–	–	–	–	–	–	–	–	–	–
	168	7	24	4	7	98	1	23	35	83	48
	169	–	–	–	–	–	–	–	–	–	–
	170	170	1	10	511	13	28	23	105	84	–

EG2	N	n	l	m	g	I	t	F	T	ρ	$D2$
	160	4	40	3	4	120	1	39	44	79	35
	161	7	23	4	7	94	1	22	34	80	46
	162	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	57	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
	169	–	–	–	–	–	–	–	–	–	–
	170	5	34	5	15	171	1	33	73	84	11

EG3	N	n	l	m	g	I	t	F	T	T_M	ρ	$D3$
	160	8	20	5	15	100	1	19	59	59	79	20
	161	7	23	4	7	94	1	22	34	44	80	36
	162	6	27	4	7	109	1	26	38	52	80	28
	164	4	41	3	4	123	1	40	45	80	81	1
	165	15	11	5	15	57	2	20	37	40	82	42
	166	2	83	2	2	167	1	82	83	164	82	–
	168	28	6	6	31	37	4	21	41	42	83	41
	169	–	–	–	–	–	–	–	–	–	–	–
	170	5	34	5	15	171	1	33	73	73	84	11

There are also many composite N for which the GHS attack is infeasible today, yet it takes less time than Pollard's rho algorithm for solving the ECDLP on *essentially all* elliptic curves over $\mathbb{F}_{2^N}$. Examples of such N are 170, 185, 190, 215, 220 (all with GHS attack parameters $n = 5$, $m = 5$). For $N = 185$, the GHS attack takes about 2^{76} steps, versus about 2^{92} for Pollard's rho algorithm. This case is of practical significance because a specific elliptic curve over $\mathbb{F}_{2^{185}}$ is listed in the IETF standard [19] for key establishment.

REMARK 19 (FAILURE OF THE GHS ATTACK). We can conclude that for those composite $N \in [100, 600]$ for which $D3 < 0$ for EG3, the GHS attack does not reduce the level of security offered: Pollard's rho method is the faster algorithm for *all* elliptic curves over $\mathbb{F}_{2^N}$. We emphasize that our statements about the failure of the GHS attack are made under the assumption that the Enge–Gaudry algorithm is essentially the best index-calculus algorithm for the HCDLP.

REMARK 20 (EFFECTIVENESS OF THE GHS ATTACK). When $D1 > 0$ or $D2 > 0$ or $D3 > 0$ 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 by means of the GHS attack. However, note that our data corresponds to elliptic curves with *least possible* magic numbers and genera, and usually 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 non-subfield elliptic curves with magic number $m = 5$ relative to $n = 15$ is only $\approx 2^{57}$ out of 2^{166}. Galbraith, Hess and Smart [14] (see also [12]) presented an algorithm with expected average running time of $O(q^{n/4+\varepsilon})$ 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. In other words, given an ECDLP instance on some cryptographically interesting elliptic curve $E_1/\mathbb{F}_{2^N}$, one can check whether E_1 is isogenous to some elliptic curve $E_2/\mathbb{F}_{2^N}$ that yields an easier HCDLP than E_1, and then use an isogeny $\phi : E_1 \rightarrow E_2$ 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 $\mathbb{F}_{2^{165}}$ will be isogenous to one of the $\approx 2^{57}$ 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 has essentially to search through the entire set of 2^{57} curves.

REMARK 21. (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 an arbitrary b from the set

$$B = \{b \in \mathbb{F}_{q^n} : m(b) = m \text{ and } b \notin \mathbb{F}_{q^\mu} \text{ for all proper divisors } \mu \text{ of } n\};$$

it can be seen from Theorem 5(i) that the elements of B can be efficiently enumerated. Next, compute $H = \#E_b(\mathbb{F}_{2^N})$, where $E_b : y^2 + xy = x^3 + b$, using Satoh's algorithm [30, 9], and test whether 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 $1 \leqslant i \leqslant N-1$. 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 Theorem 5), 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, Appendix H.4] lists 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 (7) would not contain the large subgroup of order r of $E(\mathbb{F}_{q^n})$. In fact, the opposite is true.

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

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

$a\ =\ $ `E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B`

$b\ =\ $ `5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2`

$r\ =\ $ `10092537397ECA4F6145799D62B0A19CE06FE26AD`

E208, $N{=}208$, $\mathbb{F}_{2^{208}} = \mathbb{F}_2[z]/(z^{208} + z^{83} + z^2 + z + 1)$, $\#E208(\mathbb{F}_{2^{208}}) = 65096 \cdot r$

$a\ =\ 0$

$b\ =\ $ `C8619ED45A62E6212E1160349E2BFA844439FAFC2A3FD1638F9E`

$r\ =\ $ `101BAF95C9723C57B6C21DA2EFF2D5ED588BDD5717E212F9D`

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

$a\ =\ $ `91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C40094DBAC`
       `DB586FB20`

$b\ =\ $ `7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003F99F6CC8`
       `482E540F7`

$r\ =\ $ `100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A167B8F1E`
       `629521`

E304, $N{=}304$, $\mathbb{F}_{2^{304}} = \mathbb{F}_2[z]/(z^{304} + z^{11} + z^2 + z + 1)$, $\#E304(\mathbb{F}_{2^{304}}) = 65070 \cdot r$

$a\ =\ $ `FD0D693149A118F651E6DCE6802085377E5F882D1B510B44160074C1288`
       `078365A0396C8E681`

$b\ =\ $ `BDDB97E555A50A908E43B01C798EA5DAA6788F1EA2794EFCF57166B8C14`
       `039601E55827340BE`

$r\ =\ $ `101D556572AABAC800101D556572AABAC8001022D5C91DD173F8FB561DA`
       `6899164443051D`

E368, $N{=}368$, $\mathbb{F}_{2^{368}} = \mathbb{F}_2[z]/(z^{368} + z^{85} + z^2 + z + 1)$, $\#E368(\mathbb{F}_{2^{368}}) = 65392 \cdot r$

$a\ =\ $ `E0D2EE25095206F5E2A4F9ED229F1F256E79A0E2B455970D8D0D865BD94`
       `778C576D62F0AB7519CCD2A1A906AE30D`

$b\ =\ $ `FC1217D4320A90452C760A58EDCD30C8DD069B3C34453837A34ED50CB54`
       `917E1C2112D84D164F444F8F74786046A`

$r\ =\ $ `10090512DA9AF72B08349D98A5DD4C7B0532ECA51CE03E2D10F3B7AC579`
       `BD87E909AE40A6F131E9CFCE5BD967`

REMARK 22 (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 (up to birational equivalence) hyperelliptic curve $C/\mathbb{F}_q$ as the GHS Weil descent of $E/\mathbb{F}_q(a, b)$. This can be derived from the facts that the defining equations for $\mathfrak{D}$ in [17, Lemma 2] depend only on $\mathbb{F}_q(a, b)$ but not on K, and that the same is true for the set Δ_0 in [17, proof of Lemma 6]. 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 23 (SUCCESS OF THE 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 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 $\mathbb{F}_q(a, b) = \mathbb{F}_{q^n}$ if and only if $\text{lcm}(n^*, l) = N$.

For the curves given in Table 2, $n^* = 16$ and $p = N/n^*$ is prime. Remarks 22 and 23 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 (5) of Theorem 1 for the various decompositions $N = nl$ without actually performing the GHS reduction. Having computed m, and using the fact that g is equal to 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 Section 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 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 times T and T_M for the three cases of the Enge–Gaudry algorithm: with and without the upper bound 10^7 on the factor base size (Cases EG1 and EG2, respectively), and with consideration of the running time for the linear algebra step (Case EG3). 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, T_M and ρ are the *logarithms* (base 2, rounded to the nearest integer) of the actual values. $D1$ and $D2$ denote the differences $\rho - T$ (if positive) for EG1 and EG2, respectively, while $D3$ denotes the difference $\rho - T_M$ (if positive) for EG3. 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 $\gcd(n, p) > 1$; that is, where $l = 2^i$ for $i \in \{0, 1, 2, 3, 4\}$. These data become relevant should means be found such that ϕ does not kill the large prime-order subgroup. 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 25), or the genera of the hyperelliptic curves are larger than $2^{12} - 1$, and are thus too large for the resulting HCDLP to be feasible.

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

EN	n	l	m	g	EG1					EG2					EG3					
					t	F	T	ρ	$D1$	t	F	T	ρ	$D2$	t	F	T	T_M	ρ	$D3$
E176	2	88	2	2	–	–	–	–	–	1	87	88	78	–	1	87	88	174	78	–
	4	**44**	**4**	**8**	–	–	–	–	–	**1**	**43**	**58**	**78**	**20**	**1**	**43**	**58**	**86**	**78**	–
	8	**22**	**8**	**128**	**1**	**21**	**737**	**78**	–	6	128	222	78	–	5	107	225	225	78	–
	16	11	16	2^{15}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E208	2	104	2	2	–	–	–	–	–	1	103	104	94	–	1	103	104	206	94	–
	4	**52**	**4**	**8**	–	–	–	–	–	**1**	**51**	**66**	**94**	**28**	**1**	**51**	**66**	**102**	**94**	–
	8	26	7	64	–	–	–	–	–	4	101	161	94	–	3	75	162	162	94	–
	16	13	14	2^{13}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E272	2	136	2	2	–	–	–	–	–	1	135	136	126	–	1	135	136	270	126	–
	4	**68**	**4**	**8**	–	–	–	–	–	**1**	**67**	**82**	**126**	**44**	**1**	**67**	**82**	**134**	**126**	–
	8	34	8	128	–	–	–	–	–	5	167	285	126	–	4	133	289	289	126	–
	16	17	16	2^{15}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E304	2	152	2	2	–	–	–	–	–	1	151	153	142	–	1	151	152	302	142	–
	4	**76**	**4**	**8**	–	–	–	–	–	**1**	**75**	**90**	**142**	**52**	**1**	**75**	**90**	**150**	**142**	–
	8	38	8	128	–	–	–	–	–	4	149	305	142	–	4	149	305	305	142	–
	16	19	16	2^{15}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E368	2	184	2	2	–	–	–	–	–	1	183	184	174	–	1	183	184	366	174	–
	4	**92**	**4**	**8**	–	–	–	–	–	**1**	**91**	**106**	**174**	**68**	**1**	**91**	**106**	**182**	**174**	–
	8	46	7	64	–	–	–	–	–	3	135	222	174	–	2	90	229	229	174	–
	16	23	13	2^{12}	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

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 attack data as listed in Table 4 if the GHS descent were not doomed to fail for the reasons given in Remark 22.

Table 4: GHS attack data in two special cases.

EG1	EN	n	l	m	g	t	F	T		ρ	$D1$
	E176	88	2	8	128	13	22	54		78	24
	E272	136	2	8	128	13	22	54		126	72

EG2	EN	n	l	m	g	t	F	T		ρ	$D2$
	E176	88	2	8	128	17	29	51		78	27
	E272	136	2	8	128	17	29	51		126	75

EG3	EN	n	l	m	g	t	F	T	T_M	ρ	$D3$
	E176	88	2	8	128	15	26	52	52	78	26
	E272	136	2	8	128	15	26	52	52	126	74

REMARK 24 (FAILURE OF THE GHS ATTACK FOR E176 AND E272). When evaluating the mapping $\phi : E(\mathbb{F}_{2^{176}}) \rightarrow J_C(\mathbb{F}_{2^2})$ (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 indeed contained in the kernel of ϕ, and is thus of no use for solving ECDLPs in $E(\mathbb{F}_{2^{176}})$. The same situation was observed with the mapping $\phi : E(\mathbb{F}_{2^{272}}) \rightarrow J_C(\mathbb{F}_{2^2})$ for E = E272.

REMARK 25 (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 $(\sigma + 1)^{16/l} b = 0$ but $(\sigma + 1)^{8/l} b \neq 0$. Thus we expect that $8/l < m \leqslant 16/l$.

REMARK 26 (APPLICABILITY OF THE GHS REDUCTION). For E176, E272 and E304, we have $\text{Tr}_{K/\mathbb{F}_2}(a) = 1$, so that condition (6) of Theorem 1 is not satisfied for these curves whenever $m(b) \neq n$. However, the weaker condition (8) 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 27 (EXISTENCE OF ISOGENOUS CURVES THAT MAY YIELD EASIER HCDLP INSTANCES). To exclude the applicability of the extended GHS attack (see [**14**] and Remark 20), we checked whether any of the ANSI X9.62 curves are isogenous to an elliptic curve for which the GHS reduction produces an easier HCDLP instance. For this, we use a modification of Algorithm 13 that allows the elliptic curve to be defined over a proper subfield $\mathbb{F}_{2^{l\mu}}$ of $\mathbb{F}_{2^N}$ with $l\mu \leqslant 16$ if and only if $\gcd(n, p) = 1$ (see Remarks 22 and 23). That is, if $\gcd(n, p) = 1$, in Algorithm 13 we accept m even if Corollary 10 applies, as long as $l\mu \leqslant 16$.

Since this time we are interested not only in the best instance (N, n, m), but in any instance for which the GHS attack yields an algorithm that is more efficient than Pollard rho, we give the estimated running times for *all* decompositions $N = nl$ in Table 5. The notation is the same as in Table 1. Observe that with the single exception of $(N, n, m) = (208, 208, 13)$, for all the 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 that is 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 quite possible that such a curve exists. However, finding such a curve seems to be harder than solving the ECDLP using Pollard rho.

(ii) E208. When allowing a factor base up to 2^{25} elements, we could improve on the GHS attack highlighted in Table 3. However, similar to the case of E176, it does not seem feasible to find a curve isogenous to E208 with $(n, m) = (8, 5)$ from among 2^{130} isomorphism classes.

(iii) E272. The 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 from among the 2^{170} isomorphism classes seems well beyond the realm of feasibility.

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

(v) E368. This case is the same as E304.

Table 5: Extended GHS attack data for the ANSI X9.62 elliptic curves.

EN	n	l	m	g	I	EG1					EG2					EG3					
						t	F	T	ρ	$D1$	t	F	T	ρ	$D2$	t	F	T	T_M	ρ	$D3$
E176	2	88	2	2	177	–	–	–	–	–	1	87	88	78	–	1	87	88	174	78	–
	4	44	3	4	132	–	–	–	–	–	1	43	48	78	30	1	43	48	86	78	–
	8	22	5	15	110	1	21	61	78	17	2	42	59	78	19	1	21	61	61	78	17
	11	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	16	11	9	255	99	2	20	839	78	–	12	127	225	78	–	10	106	230	230	78	–
	22	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	44	4	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	88	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	176	1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E208	2	104	2	2	209	–	–	–	–	–	1	103	104	94	–	1	103	104	206	94	–
	4	52	3	4	156	–	–	–	–	–	1	51	56	94	38	1	51	56	102	94	–
	8	26	5	15	130	–	–	–	–	–	1	25	65	94	29	1	25	65	65	94	29
	13	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	16	13	9	255	117	1	12	1688	94	–	11	139	248	94	–	10	126	250	252	94	–
	26	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	52	4	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	104	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	208	1	13	4095	14	28	23	1208	94	–	120	113	307	94	–	120	113	307	307	94	–
E272	2	136	2	2	273	–	–	–	–	–	1	135	136	126	–	1	135	136	270	126	–
	4	68	3	4	204	–	–	–	–	–	1	67	72	126	54	1	67	72	134	126	–
	8	34	5	15	170	–	–	–	–	–	1	33	73	126	53	1	33	73	73	126	53
	16	17	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	17	16	9	255	146	1	15	1691	126	–	10	156	280	126	–	9	140	282	282	126	–
	34	8	10	511	82	3	21	1260	126	–	21	163	283	126	–	18	139	286	286	126	–
	68	4	11	1023	45	6	21	1352	126	–	42	162	284	126	–	37	142	287	287	126	–
	136	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	272	1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E304	2	152	2	2	305	–	–	–	–	–	1	151	152	142	–	1	151	152	302	142	–
	4	76	3	4	228	–	–	–	–	–	1	75	80	142	62	1	75	80	150	142	–
	8	38	5	15	190	–	–	–	–	–	1	37	77	142	65	1	37	77	77	142	65
	16	19	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	19	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	38	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	76	4	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	152	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	304	1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
E368	2	184	2	2	369	–	–	–	–	–	1	183	184	174	–	1	183	184	366	174	–
	4	92	3	4	276	–	–	–	–	–	1	91	96	174	78	1	91	96	182	174	–
	8	46	5	15	230	–	–	–	–	–	1	45	85	174	89	1	45	85	90	174	84
	16	23	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	23	16	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	46	8	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	92	4	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	184	2	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
	368	1	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

Our analysis shows that the extended GHS attack does not yield a faster algorithm to solve the ECDLP for the ANSI X9.62 curves. However, once the problem of finding an isogenous curve from among the most vulnerable isomorphism classes identified above can be solved more efficiently, the GHS attack takes significantly fewer steps than Pollard's rho algorithm.

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 were not known to us a priori. 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 a 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 [**20**]: 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 (see Theorem 11).

Table 6 lists the (n, l, g) GHS attack parameters that yield HCDLP instances that can be solved in $\approx 2^{T_M}$ steps using a smoothness bound of t and a factor base of size $\approx 2^F$. Note that $T_M \ll \rho$, where 2^ρ is the approximate time taken 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_M. Table 7 illustrates how the factor base size, the expected number of random-walk steps ($\approx 2^E$) to find a smooth divisor and the total expected number of random-walk steps 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 [**20**], which has $T_M = 37$. The latter problem was concluded to be tractable in [**20**], on the basis of 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 to apply the Weil descent methodology to map the ECDLP efficiently 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 three finite fields to the DLP in C_{ab} curves. See also [**7**] for a study on Weil restriction.

The E176 and E272 elliptic curves are from ANSI X9.62. As discussed in Section 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 [**7**, Proposition 3.13] shows how Weil descent

Table 6: GHS attack parameters for the challenge curves.

Curve	N	n	l	g	t	F	T	T_M	ρ
E161	161	7	23	7	1	22	34	44	80
E180	180	30	6	31	4	21	41	42	89
E186	186	31	6	31	4	21	41	42	92
E217	217	31	7	31	3	18	49	49	108
E248	248	31	8	31	3	21	52	52	123
E300	300	30	10	31	3	27	58	58	149
E176	176	88	2	128	15	26	52	52	78
E272	272	136	2	128	15	26	52	52	126
E161-2	161	7	23	64	3	66	153	153	80

Table 7: Some Enge–Gaudry parameters for the challenge curves.

							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

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 $\leqslant 2^{2t} - 1$ 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 $\leqslant 2^{16} - 1$ 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 [**14**] (see Remark 20), 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' could 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 [**14**].

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. Also, we stress that failure of the GHS attack does not imply failure of the Weil descent methodology – there may be other useful curves that lie on the Weil restriction $W_{E/k}$, but 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.

Appendix A. *Results of our analysis*

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

Table 8: Results of our analysis

N	EG1										EG2										EG3										
	n	l	m	g	I	t	F	T	ρ	D1	n	l	m	g	I	t	F	T	ρ	D2	n	l	m	g	I	t	F	T	T_M	ρ	D3
100	5	20	5	15	101	1	19	59	49	—	4	25	3	4	75	1	24	29	49	20	4	25	3	4	75	1	24	29	48	49	1
102	6	17	4	7	69	1	16	28	50	22	6	17	4	7	69	1	16	28	50	22	6	17	4	7	69	1	16	28	32	50	18
104	8	13	5	15	65	1	12	52	51	—	4	26	3	4	78	1	25	30	51	21	8	13	5	15	65	2	24	41	48	51	3
105	7	15	4	7	62	1	14	26	52	26	7	15	4	7	62	1	14	26	52	26	7	15	4	7	62	1	14	26	28	52	24
106	—	—	—	—	—	—	—	—	—	—	2	53	2	2	107	1	52	53	52	—	2	53	2	2	107	1	52	53	104	52	—
108	6	18	4	7	73	1	17	29	53	24	6	18	4	7	73	1	17	29	53	24	12	9	5	15	45	2	16	33	33	53	20
110	5	22	5	15	111	1	21	61	54	—	2	55	2	2	111	1	54	55	54	—	5	22	5	15	111	1	21	61	61	54	—
111	—	—	—	—	—	—	—	—	—	—	3	37	3	3	112	1	36	39	55	16	3	37	3	3	112	1	36	39	72	55	—
112	7	16	4	7	66	1	15	27	55	28	7	16	4	7	66	1	15	27	55	28	7	16	4	7	66	1	15	27	30	55	25
114	6	19	4	7	77	1	18	30	56	26	6	19	4	7	77	1	18	30	56	26	6	19	4	7	77	1	18	30	36	56	20
115	5	23	5	15	116	1	22	62	57	—	5	23	5	15	116	2	44	61	57	—	5	23	5	15	116	1	22	62	62	57	—
116	—	—	—	—	—	—	—	—	—	—	4	29	3	4	87	1	28	33	57	24	4	29	3	4	87	1	28	33	56	57	1
117	9	13	7	63	92	1	12	302	58	—	3	39	3	3	118	1	38	41	58	17	3	39	3	3	118	1	38	41	76	58	—
118	—	—	—	—	—	—	—	—	—	—	2	59	2	2	119	1	58	59	58	—	2	59	2	2	119	1	58	59	116	58	—
119	7	17	4	7	70	1	16	28	59	31	7	17	4	7	70	1	16	28	59	31	7	17	4	7	70	1	16	28	32	59	27
120	6	20	4	7	81	1	19	31	59	28	6	20	4	7	81	1	19	31	59	28	15	8	5	15	42	2	14	31	31	59	28
121	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
122	—	—	—	—	—	—	—	—	—	—	2	61	2	2	123	1	60	61	60	—	2	61	2	2	123	1	60	61	120	60	—
123	—	—	—	—	—	—	—	—	—	—	3	41	3	3	124	1	40	43	61	18	3	41	3	3	124	1	40	43	80	61	—
124	31	4	6	31	28	5	17	31	61	30	31	4	6	31	28	5	17	31	61	30	62	2	7	63	17	10	16	32	32	61	29
125	—	—	—	—	—	—	—	—	—	—	5	25	5	15	126	1	24	64	62	—	5	25	5	15	126	1	24	64	64	62	—
126	7	18	4	7	74	1	17	29	62	33	7	18	4	7	74	1	17	29	62	33	63	2	7	63	18	10	16	32	32	62	30
128	8	16	5	15	80	1	15	55	63	8	4	32	3	4	96	1	31	36	63	27	8	16	5	15	80	1	15	55	55	63	8
129	—	—	—	—	—	—	—	—	—	—	3	43	3	3	130	1	42	45	64	19	3	43	3	3	130	1	42	45	84	64	—
130	10	13	6	31	79	1	12	125	64	—	2	65	2	2	131	1	64	65	64	—	5	26	5	15	131	1	25	65	65	64	—
132	6	22	4	7	89	1	21	33	65	32	6	22	4	7	89	1	21	33	65	32	12	11	5	15	55	2	20	37	40	65	25
133	7	19	4	7	78	1	18	30	66	36	7	19	4	7	78	1	18	30	66	36	7	19	4	7	78	1	18	30	36	66	30
134	—	—	—	—	—	—	—	—	—	—	2	67	2	2	135	1	66	67	66	—	2	67	2	2	135	1	66	67	132	66	—

Results of our analysis, *continued*

	EG1										EG2										EG3										
N	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$	n	l	m	g	I	t	F	T	T_M	ρ	$D3$
135	15	9	5	15	47	2	16	33	67	34	15	9	5	15	47	2	16	33	67	34	15	9	5	15	47	2	16	33	33	67	34
136	8	17	5	15	85	1	16	56	67	11	4	34	3	4	102	1	33	38	67	29	8	17	5	15	85	1	16	56	56	67	11
138	6	23	4	7	93	1	22	34	68	34	6	23	4	7	93	1	22	34	68	34	6	23	4	7	93	1	22	34	44	68	24
140	7	20	4	7	82	1	19	31	69	38	7	20	4	7	82	1	19	31	69	38	14	10	5	15	52	2	18	35	36	69	33
141	–	–	–	–	–	–	–	–	–	–	3	47	3	3	142	1	46	49	70	21	3	47	3	3	142	1	46	49	92	70	–
142	–	–	–	–	–	–	–	–	–	–	2	71	2	2	143	1	70	71	70	–	2	71	2	2	143	1	70	71	140	70	–
143	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
144	6	24	4	7	97	1	23	35	71	36	6	24	4	7	97	1	23	35	71	36	12	12	5	15	60	2	22	39	44	71	27
145	–	–	–	–	–	–	–	–	–	–	5	29	5	15	146	1	28	68	72	4	5	29	5	15	146	1	28	68	68	72	4
146	146	1	11	1023	14	28	23	232	72	–	2	73	2	2	147	1	72	73	72	–	73	2	10	511	24	34	62	125	125	72	–
147	7	21	4	7	86	1	20	32	73	41	7	21	4	7	86	1	20	32	73	41	7	21	4	7	86	1	20	32	40	73	33
148	–	–	–	–	–	–	–	–	–	–	4	37	3	4	111	1	36	41	73	32	4	37	3	4	111	1	36	41	72	73	1
150	15	10	5	15	52	2	18	35	74	39	15	10	5	15	52	2	18	35	74	39	15	10	5	15	52	2	18	35	36	74	38
152	8	19	5	15	95	1	18	58	75	17	4	38	3	4	114	1	37	42	75	33	8	19	5	15	95	1	18	58	58	75	17
153	51	3	9	255	30	9	23	165	76	–	3	51	3	3	154	1	50	53	76	23	3	51	3	3	154	1	50	53	100	76	–
154	7	22	4	7	90	1	21	33	76	43	7	22	4	7	90	1	21	33	76	43	14	11	5	15	57	2	20	37	40	76	36
155	31	5	6	31	34	5	22	36	77	41	31	5	6	31	34	5	22	36	77	41	31	5	6	31	34	4	17	37	37	77	40
156	12	13	5	15	65	1	12	52	77	25	6	26	4	7	105	1	25	37	77	40	12	13	5	15	65	2	24	41	48	77	29
158	–	–	–	–	–	–	–	–	–	–	2	79	2	2	159	1	78	79	78	–	2	79	2	2	159	1	78	79	156	78	–
159	–	–	–	–	–	–	–	–	–	–	3	53	3	3	160	1	52	55	79	24	3	53	3	3	160	1	52	55	104	79	–
160	8	20	5	15	100	1	19	59	79	20	4	40	3	4	120	1	39	44	79	35	8	20	5	15	100	1	19	59	59	79	20
161	7	23	4	7	94	1	22	34	80	46	7	23	4	7	94	1	22	34	80	46	7	23	4	7	94	1	22	34	44	80	36
162	9	18	7	63	127	1	17	307	80	–	6	27	4	7	109	1	26	38	80	42	6	27	4	7	109	1	26	38	52	80	28
164	–	–	–	–	–	–	–	–	–	–	4	41	3	4	123	1	40	45	81	36	4	41	3	4	123	1	40	45	80	81	1
165	15	11	5	15	57	2	20	37	82	45	15	11	5	15	57	2	20	37	82	45	15	11	5	15	57	2	20	37	40	82	42
166	–	–	–	–	–	–	–	–	–	–	2	83	2	2	167	1	82	83	82	–	2	83	2	2	167	1	82	83	164	82	–
168	7	24	4	7	98	1	23	35	83	48	7	24	4	7	98	1	23	35	83	48	28	6	6	31	37	4	21	41	42	83	41
169	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–

Results of our analysis, *continued*

N	EG1										EG2										EG3										
	n	l	m	g	I	t	F	T	ρ	D1	n	l	m	g	I	t	F	T	ρ	D2	n	l	m	g	I	t	F	T	T_M	ρ	D3
170	170	1	10	511	13	28	23	105	84	—	5	34	5	15	171	1	33	73	84	11	5	34	5	15	171	1	33	73	73	84	11
171	9	19	7	63	134	1	18	308	85	—	3	57	3	3	172	1	56	59	85	26	3	57	3	3	172	1	56	59	112	85	—
172	—	—	—	—	—	—	—	—	—	—	4	43	3	4	129	1	42	47	85	38	4	43	3	4	129	1	42	47	84	85	1
174	—	—	—	—	—	—	—	—	—	—	6	29	4	7	117	1	28	40	86	46	6	29	4	7	117	1	28	40	56	86	30
175	35	5	8	127	42	5	22	139	87	—	7	25	4	7	102	1	24	36	87	51	7	25	4	7	102	1	24	36	48	87	39
176	8	22	5	15	110	1	21	61	87	26	4	44	3	4	132	1	43	48	87	39	8	22	5	15	110	1	21	61	61	87	26
177	—	—	—	—	—	—	—	—	—	—	3	59	3	3	178	1	58	61	88	27	3	59	3	3	178	1	58	61	116	88	—
178	178	1	13	4095	16	28	23	1208	88	—	2	89	2	2	179	1	88	89	88	—	2	89	2	2	179	1	88	89	176	88	—
180	15	12	5	15	62	2	22	39	89	50	15	12	5	15	62	2	22	39	89	50	30	6	6	31	38	4	21	41	42	89	47
182	14	13	5	15	67	1	12	52	90	38	7	26	4	7	106	1	25	37	90	53	14	13	5	15	67	2	24	41	48	90	42
183	—	—	—	—	—	—	—	—	—	—	3	61	3	3	184	1	60	63	91	28	3	61	3	3	184	1	60	63	120	91	—
184	8	23	5	15	115	1	22	62	91	29	4	46	3	4	138	1	45	50	91	41	8	23	5	15	115	1	22	62	62	91	29
185	—	—	—	—	—	—	—	—	—	—	5	37	5	15	186	1	36	76	92	16	5	37	5	15	186	1	36	76	76	92	16
186	31	6	6	31	40	4	21	41	92	51	31	6	6	31	40	5	27	41	92	51	31	6	6	31	40	4	21	41	42	92	50
187	17	11	9	255	101	2	20	839	93	—	17	11	9	255	101	12	127	225	93	—	17	11	9	255	101	10	106	230	230	93	—
188	—	—	—	—	—	—	—	—	—	—	4	47	3	4	141	1	46	51	93	42	4	47	3	4	141	1	46	51	92	93	1
189	63	3	7	63	25	9	23	42	94	52	7	27	4	7	110	1	26	38	94	56	63	3	7	63	25	8	20	43	43	94	51
190	10	19	6	31	115	1	18	131	94	—	5	38	5	15	191	1	37	77	94	17	5	38	5	15	191	1	37	77	77	94	17
192	12	16	5	15	80	1	15	55	95	40	6	32	4	7	129	1	31	43	95	52	12	16	5	15	80	1	15	55	55	95	40
194	—	—	—	—	—	—	—	—	—	—	2	97	2	2	195	1	96	97	96	—	2	97	2	2	195	1	96	97	192	96	—
195	15	13	5	15	67	1	12	52	97	45	15	13	5	15	67	2	24	41	97	56	15	13	5	15	67	2	24	41	48	97	49
196	28	7	6	31	43	3	18	49	97	48	7	28	4	7	114	1	27	39	97	58	28	7	6	31	43	3	18	49	49	97	48
198	9	22	7	63	155	1	21	311	98	—	6	33	4	7	133	1	32	44	98	54	6	33	4	7	133	1	32	44	64	98	34
200	10	20	6	31	121	1	19	132	99	—	4	50	3	4	150	1	49	54	99	45	8	25	5	15	125	1	24	64	64	99	35
201	—	—	—	—	—	—	—	—	—	—	3	67	3	3	202	1	66	69	100	31	3	67	3	3	202	1	66	69	132	100	—
202	—	—	—	—	—	—	—	—	—	—	2	101	2	2	203	1	100	101	100	—	2	101	2	2	203	1	100	101	200	100	—
203	—	—	—	—	—	—	—	—	—	—	7	29	4	7	118	1	28	40	101	61	7	29	4	7	118	1	28	40	56	101	45
204	12	17	5	15	85	1	16	56	101	45	6	34	4	7	137	1	33	45	101	56	12	17	5	15	85	1	16	56	56	101	45

Results of our analysis, *continued*

N	EG1										EG2										EG3										
	n	l	m	g	I	t	F	T	ρ	D1	n	l	m	g	I	t	F	T	ρ	D2	n	l	m	g	I	t	F	T	T_M	ρ	D3
205	—	—	—	—	—	—	—	—	—	—	5	41	5	15	206	1	40	80	102	22	5	41	5	15	206	1	40	80	80	102	22
206	—	—	—	—	—	—	—	—	—	—	2	103	2	2	207	1	102	103	102	—	2	103	2	2	207	1	102	103	204	102	—
207	9	23	7	63	162	1	22	312	103	—	3	69	3	3	208	1	68	71	103	32	3	69	3	3	208	1	68	71	136	103	—
208	16	13	9	255	117	1	12	1688	103	—	4	52	3	4	156	1	51	56	103	47	8	26	5	15	130	1	25	65	65	103	38
209	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
210	30	7	6	31	44	3	18	49	104	55	7	30	4	7	122	1	29	41	104	63	30	7	6	31	44	3	18	49	49	104	55
212	—	—	—	—	—	—	—	—	—	—	4	53	3	4	159	1	52	57	105	48	4	53	3	4	159	1	52	57	104	105	1
213	—	—	—	—	—	—	—	—	—	—	3	71	3	3	214	1	70	73	106	33	3	71	3	3	214	1	70	73	140	106	—
214	—	—	—	—	—	—	—	—	—	—	2	107	2	2	215	1	106	107	106	—	2	107	2	2	215	1	106	107	212	106	—
215	—	—	—	—	—	—	—	—	—	—	5	43	5	15	216	1	42	82	107	25	5	43	5	15	216	1	42	82	84	107	23
216	12	18	5	15	90	1	17	57	107	50	6	36	4	7	145	1	35	47	107	60	12	18	5	15	90	1	17	57	57	107	50
217	31	7	6	31	46	3	18	49	108	59	7	31	4	7	126	1	30	42	108	66	31	7	6	31	46	3	18	49	49	108	59
218	—	—	—	—	—	—	—	—	—	—	2	109	2	2	219	1	108	109	108	—	2	109	2	2	219	1	108	109	216	108	—
219	73	3	10	511	34	9	23	375	109	—	3	73	3	3	220	1	72	75	109	34	3	73	3	3	220	1	72	75	144	109	—
220	10	22	6	31	133	1	21	134	109	—	4	55	3	4	165	1	54	59	109	50	5	44	5	15	221	1	43	83	86	109	23
221	17	13	9	255	119	1	12	1688	110	—	17	13	9	255	119	11	139	248	110	—	17	13	9	255	119	10	126	250	252	110	—
222	—	—	—	—	—	—	—	—	—	—	6	37	4	7	149	1	36	48	110	62	6	37	4	7	149	1	36	48	72	110	38
224	28	8	6	31	49	3	21	52	111	59	7	32	4	7	130	1	31	43	111	68	28	8	6	31	49	3	21	52	52	111	59
225	15	15	5	15	77	1	14	54	112	58	15	15	5	15	77	2	28	45	112	67	15	15	5	15	77	1	14	54	54	112	58
226	—	—	—	—	—	—	—	—	—	—	2	113	2	2	227	1	112	113	112	—	2	113	2	2	227	1	112	113	224	112	—
228	12	19	5	15	95	1	18	58	113	55	6	38	4	7	153	1	37	49	113	64	12	19	5	15	95	1	18	58	58	113	55
230	10	23	6	31	139	1	22	135	114	—	5	46	5	15	231	1	45	85	114	29	5	46	5	15	231	1	45	85	90	114	24
231	21	11	6	31	68	2	20	71	115	44	7	33	4	7	134	1	32	44	115	71	21	11	6	31	68	3	30	61	61	115	54
232	—	—	—	—	—	—	—	—	—	—	4	58	3	4	174	1	57	62	115	53	8	29	5	15	145	1	28	68	68	115	47
234	18	13	8	127	105	1	12	721	116	—	6	39	4	7	157	1	38	50	116	66	6	39	4	7	157	1	38	50	76	116	40
235	—	—	—	—	—	—	—	—	—	—	5	47	5	15	236	1	46	86	117	31	5	47	5	15	236	1	46	86	92	117	25
236	—	—	—	—	—	—	—	—	—	—	4	59	3	4	177	1	58	63	117	54	4	59	3	4	177	1	58	63	116	117	1
237	—	—	—	—	—	—	—	—	—	—	3	79	3	3	238	1	78	81	118	37	3	79	3	3	238	1	78	81	156	118	—

Results of our analysis, *continued*

N	EG1										EG2										EG3										
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$	n	l	m	g	I	t	F	T	T_M	ρ	$D3$
238	14	17	5	15	87	1	16	56	118	62	7	34	4	7	138	1	33	45	118	73	14	17	5	15	87	1	16	56	56	118	62
240	30	8	6	31	50	3	21	52	119	67	15	16	5	15	82	2	30	47	119	72	30	8	6	31	50	3	21	52	52	119	67
242	–	–	–	–	–	–	–	–	–	–	2	121	2	2	243	1	120	121	120	–	2	121	2	2	243	1	120	121	240	120	–
243	–	–	–	–	–	–	–	–	–	–	3	81	3	3	244	1	80	83	121	38	3	81	3	3	244	1	80	83	160	121	–
244	–	–	–	–	–	–	–	–	–	–	4	61	3	4	183	1	60	65	121	56	4	61	3	4	183	1	60	65	120	121	1
245	35	7	8	127	58	3	18	235	122	–	7	35	4	7	142	1	34	46	122	76	7	35	4	7	142	1	34	46	68	122	54
246	–	–	–	–	–	–	–	–	–	–	6	41	4	7	165	1	40	52	122	70	6	41	4	7	165	1	40	52	80	122	42
247	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
248	31	8	6	31	52	3	21	52	123	71	31	8	6	31	52	4	29	49	123	74	31	8	6	31	52	3	21	52	52	123	71
249	–	–	–	–	–	–	–	–	–	–	3	83	3	3	250	1	82	85	124	39	3	83	3	3	250	1	82	85	164	124	–
250	–	–	–	–	–	–	–	–	–	–	5	50	5	15	251	1	49	89	124	35	5	50	5	15	251	1	49	89	98	124	26
252	252	1	9	255	11	28	23	53	125	72	7	36	4	7	146	1	35	47	125	78	63	4	7	63	32	7	24	52	52	125	73
253	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
254	254	1	9	255	13	28	23	53	126	73	127	2	8	127	21	17	29	51	126	75	127	2	8	127	21	15	26	51	52	126	74
255	255	1	9	255	14	28	23	53	127	74	15	17	5	15	87	2	32	49	127	78	255	1	9	255	14	30	25	52	52	127	75
256	16	16	9	255	144	1	15	1691	127	–	4	64	3	4	192	1	63	68	127	59	8	32	5	15	160	1	31	71	71	127	56
258	–	–	–	–	–	–	–	–	–	–	6	43	4	7	173	1	42	54	128	74	6	43	4	7	173	1	42	54	84	128	44
259	–	–	–	–	–	–	–	–	–	–	7	37	4	7	150	1	36	48	129	81	7	37	4	7	150	1	36	48	72	129	57
260	20	13	7	63	91	1	12	302	129	–	4	65	3	4	195	1	64	69	129	60	10	26	6	31	157	2	50	101	101	129	28
261	–	–	–	–	–	–	–	–	–	–	3	87	3	3	262	1	86	89	130	41	9	29	7	63	204	3	84	169	169	130	–
262	–	–	–	–	–	–	–	–	–	–	2	131	2	2	263	1	130	131	130	–	2	131	2	2	263	1	130	131	260	130	–
264	12	22	5	15	110	1	21	61	131	70	6	44	4	7	177	1	43	55	131	76	12	22	5	15	110	1	21	61	61	131	70
265	–	–	–	–	–	–	–	–	–	–	5	53	5	15	266	1	52	92	132	40	5	53	5	15	266	1	52	92	104	132	28
266	14	19	5	15	97	1	18	58	132	74	7	38	4	7	154	1	37	49	132	83	14	19	5	15	97	1	18	58	58	132	74
267	–	–	–	–	–	–	–	–	–	–	3	89	3	3	268	1	88	91	133	42	3	89	3	3	268	1	88	91	176	133	–
268	–	–	–	–	–	–	–	–	–	–	4	67	3	4	201	1	66	71	133	62	4	67	3	4	201	1	66	71	132	133	1
270	15	18	5	15	92	1	17	57	134	77	15	18	5	15	92	2	34	51	134	83	30	9	6	31	56	3	24	55	55	134	79
272	34	8	10	511	82	3	21	1260	135	–	4	68	3	4	204	1	67	72	135	63	8	34	5	15	170	1	33	73	73	135	62

Results of our analysis, *continued*

	EG1										EG2										EG3										
N	n	l	m	g	I	t	F	T	ρ	D1	n	l	m	g	I	t	F	T	ρ	D2	n	l	m	g	I	t	F	T	T_M	ρ	D3
273	21	13	6	31	80	1	12	125	136	11	7	39	4	7	158	1	38	50	136	86	21	13	6	31	80	3	36	67	72	136	64
274	–	–	–	–	–	–	–	–	–	–	2	137	2	2	275	1	136	137	136	–	2	137	2	2	275	1	136	137	272	136	–
275	–	–	–	–	–	–	–	–	–	–	5	55	5	15	276	1	54	94	137	43	5	55	5	15	276	1	54	94	108	137	29
276	12	23	5	15	115	1	22	62	137	75	6	46	4	7	185	1	45	57	137	80	12	23	5	15	115	1	22	62	62	137	75
278	–	–	–	–	–	–	–	–	–	–	2	139	2	2	279	1	138	139	138	–	2	139	2	2	279	1	138	139	276	138	–
279	31	9	6	31	58	2	16	67	139	72	31	9	6	31	58	4	33	53	139	86	31	9	6	31	58	3	24	55	55	139	84
280	14	20	5	15	102	1	19	59	139	80	7	40	4	7	162	1	39	51	139	88	28	10	6	31	61	3	27	58	58	139	81
282	–	–	–	–	–	–	–	–	–	–	6	47	4	7	189	1	46	58	140	82	6	47	4	7	189	1	46	58	92	140	48
284	–	–	–	–	–	–	–	–	–	–	4	71	3	4	213	1	70	75	141	66	4	71	3	4	213	1	70	75	140	141	1
285	15	19	5	15	97	1	18	58	142	84	15	19	5	15	97	2	36	53	142	89	15	19	5	15	97	1	18	58	58	142	84
286	–	–	–	–	–	–	–	–	–	–	2	143	2	2	287	1	142	143	142	–	2	143	2	2	287	1	142	143	284	142	–
287	–	–	–	–	–	–	–	–	–	–	7	41	4	7	166	1	40	52	143	91	7	41	4	7	166	1	40	52	80	143	63
288	12	24	5	15	120	1	23	63	143	80	6	48	4	7	193	1	47	59	143	84	12	24	5	15	120	1	23	63	63	143	80
289	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
290	–	–	–	–	–	–	–	–	–	–	5	58	5	15	291	1	57	97	144	47	10	29	6	31	175	2	56	107	112	144	32
291	–	–	–	–	–	–	–	–	–	–	3	97	3	3	292	1	96	99	145	46	3	97	3	3	292	1	96	99	192	145	–
292	292	1	12	2047	14	28	23	529	145	–	4	73	3	4	219	1	72	77	145	68	4	73	3	4	219	1	72	77	144	145	1
294	14	21	5	15	107	1	20	60	146	86	7	42	4	7	170	1	41	53	146	93	14	21	5	15	107	1	20	60	60	146	86
295	–	–	–	–	–	–	–	–	–	–	5	59	5	15	296	1	58	98	147	49	5	59	5	15	296	1	58	98	116	147	31
296	–	–	–	–	–	–	–	–	–	–	8	37	5	15	185	1	36	76	147	71	8	37	5	15	185	1	36	76	76	147	71
297	–	–	–	–	–	–	–	–	–	–	3	99	3	3	298	1	98	101	148	47	9	33	7	63	232	3	96	181	192	148	–
298	–	–	–	–	–	–	–	–	–	–	2	149	2	2	299	1	148	149	148	–	2	149	2	2	299	1	148	149	296	148	–
299	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
300	15	20	5	15	102	1	19	59	149	90	15	20	5	15	102	2	38	55	149	94	30	10	6	31	62	3	27	58	58	149	91
301	–	–	–	–	–	–	–	–	–	–	7	43	4	7	174	1	42	54	150	96	7	43	4	7	174	1	42	54	84	150	66
302	–	–	–	–	–	–	–	–	–	–	2	151	2	2	303	1	150	151	150	–	2	151	2	2	303	1	150	151	300	150	–
303	–	–	–	–	–	–	–	–	–	–	3	101	3	3	304	1	100	103	151	48	3	101	3	3	304	1	100	103	200	151	–
304	–	–	–	–	–	–	–	–	–	–	8	38	5	15	190	1	37	77	151	74	8	38	5	15	190	1	37	77	77	151	74

Results of our analysis, *continued*

N	EG1											EG2										EG3										
	n	l	m	g	I	t	F	T	ρ	$D1$		n	l	m	g	I	t	F	T	ρ	$D2$	n	l	m	g	I	t	F	T	T_M	ρ	$D3$
305	—	—	—	—	—	—	—	—	—	—		5	61	5	15	306	1	60	100	152	52	5	61	5	15	306	1	60	100	120	152	32
306	102	3	10	511	33	9	23	375	152	—		6	51	4	7	205	1	50	62	152	90	6	51	4	7	205	1	50	62	100	152	52
308	14	22	5	15	112	1	21	61	153	92		7	44	4	7	178	1	43	55	153	98	14	22	5	15	112	1	21	61	61	153	92
309	—	—	—	—	—	—	—	—	—	—		3	103	3	3	310	1	102	105	154	49	3	103	3	3	310	1	102	105	204	154	—
310	62	5	7	63	39	5	22	65	154	89		31	10	6	31	64	4	37	57	154	97	31	10	6	31	64	3	27	58	58	154	96
312	24	13	7	63	91	1	12	302	155	—		6	52	4	7	209	1	51	63	155	92	12	26	5	15	130	1	25	65	65	155	90
314	—	—	—	—	—	—	—	—	—	—		2	157	2	2	315	1	156	157	156	—	2	157	2	2	315	1	156	157	312	156	—
315	15	21	5	15	107	1	20	60	157	97		7	45	4	7	182	1	44	56	157	101	15	21	5	15	107	1	20	60	60	157	97
316	—	—	—	—	—	—	—	—	—	—		4	79	3	4	237	1	78	83	157	74	4	79	3	4	237	1	78	83	156	157	1
318	—	—	—	—	—	—	—	—	—	—		6	53	4	7	213	1	52	64	158	94	6	53	4	7	213	1	52	64	104	158	54
319	—	—	—	—	—	—	—	—	—	—		—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
320	20	16	7	63	112	1	15	305	159	—		8	40	5	15	200	1	39	79	159	80	8	40	5	15	200	1	39	79	79	159	80
321	—	—	—	—	—	—	—	—	—	—		3	107	3	3	322	1	106	109	160	51	3	107	3	3	322	1	106	109	212	160	—
322	14	23	5	15	117	1	22	62	160	98		7	46	4	7	186	1	45	57	160	103	14	23	5	15	117	1	22	62	62	160	98
323	—	—	—	—	—	—	—	—	—	—		—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
324	18	18	8	127	145	1	17	726	161	—		6	54	4	7	217	1	53	65	161	96	12	27	5	15	135	1	26	66	66	161	95
325	—	—	—	—	—	—	—	—	—	—		5	65	5	15	326	1	64	104	162	58	5	65	5	15	326	1	64	104	128	162	34
326	—	—	—	—	—	—	—	—	—	—		2	163	2	2	327	1	162	163	162	—	2	163	2	2	327	1	162	163	324	162	—
327	—	—	—	—	—	—	—	—	—	—		3	109	3	3	328	1	108	111	163	52	3	109	3	3	328	1	108	111	216	163	—
328	—	—	—	—	—	—	—	—	—	—		8	41	5	15	205	1	40	80	163	83	8	41	5	15	205	1	40	80	80	163	83
329	—	—	—	—	—	—	—	—	—	—		7	47	4	7	190	1	46	58	164	106	7	47	4	7	190	1	46	58	92	164	72
330	15	22	5	15	112	1	21	61	164	103		15	22	5	15	112	2	42	59	164	105	15	22	5	15	112	1	21	61	61	164	103
332	—	—	—	—	—	—	—	—	—	—		4	83	3	4	249	1	82	87	165	78	4	83	3	4	249	1	82	87	164	165	1
333	—	—	—	—	—	—	—	—	—	—		3	111	3	3	334	1	110	113	166	53	9	37	7	63	260	2	72	209	209	166	—
334	—	—	—	—	—	—	—	—	—	—		2	167	2	2	335	1	166	167	166	—	2	167	2	2	335	1	166	167	332	166	—
335	—	—	—	—	—	—	—	—	—	—		5	67	5	15	336	1	66	106	167	61	5	67	5	15	336	1	66	106	132	167	35
336	14	24	5	15	122	1	23	63	167	104		7	48	4	7	194	1	47	59	167	108	14	24	5	15	122	1	23	63	63	167	104
338	—	—	—	—	—	—	—	—	—	—		2	169	2	2	339	1	168	169	168	—	2	169	2	2	339	1	168	169	336	168	—

Results of our analysis, *continued*

N	EG1										EG2										EG3										
	n	l	m	g	I	t	F	T	ρ	D1	n	l	m	g	I	t	F	T	ρ	D2	n	l	m	g	I	t	F	T	T_M	ρ	D3
339	−	−	−	−	−	−	−	−	−	−	3	113	3	3	340	1	112	115	169	54	3	113	3	3	340	1	112	115	224	169	−
340	340	1	11	1023	13	28	23	232	169	−	4	85	3	4	255	1	84	89	169	80	170	2	10	511	24	34	62	125	125	169	44
341	31	11	6	31	70	2	20	71	170	99	31	11	6	31	70	3	30	61	170	109	31	11	6	31	70	3	30	61	61	170	109
342	18	19	8	127	153	1	18	727	170	−	6	57	4	7	229	1	56	68	170	102	6	57	4	7	229	1	56	68	112	170	58
343	−	−	−	−	−	−	−	−	−	−	7	49	4	7	198	1	48	60	171	111	7	49	4	7	198	1	48	60	96	171	75
344	−	−	−	−	−	−	−	−	−	−	8	43	5	15	215	1	42	82	171	89	8	43	5	15	215	1	42	82	84	171	87
345	15	23	5	15	117	1	22	62	172	110	15	23	5	15	117	2	44	61	172	111	15	23	5	15	117	1	22	62	62	172	110
346	−	−	−	−	−	−	−	−	−	−	2	173	2	2	347	1	172	173	172	−	2	173	2	2	347	1	172	173	344	172	−
348	−	−	−	−	−	−	−	−	−	−	12	29	5	15	145	1	28	68	173	105	12	29	5	15	145	1	28	68	68	173	105
350	70	5	9	255	47	5	22	315	174	−	7	50	4	7	202	1	49	61	174	113	14	25	5	15	127	1	24	64	64	174	110
351	−	−	−	−	−	−	−	−	−	−	3	117	3	3	352	1	116	119	175	56	9	39	7	63	274	2	76	213	213	175	−
352	−	−	−	−	−	−	−	−	−	−	8	44	5	15	220	1	43	83	175	92	8	44	5	15	220	1	43	83	86	175	89
354	−	−	−	−	−	−	−	−	−	−	6	59	4	7	237	1	58	70	176	106	6	59	4	7	237	1	58	70	116	176	60
355	−	−	−	−	−	−	−	−	−	−	5	71	5	15	356	1	70	110	177	67	5	71	5	15	356	1	70	110	140	177	37
356	−	−	−	−	−	−	−	−	−	−	4	89	3	4	267	1	88	93	177	84	4	89	3	4	267	1	88	93	176	177	1
357	21	17	6	31	104	1	16	129	178	49	7	51	4	7	206	1	50	62	178	116	21	17	6	31	104	2	32	83	83	178	95
358	−	−	−	−	−	−	−	−	−	−	2	179	2	2	359	1	178	179	178	−	2	179	2	2	359	1	178	179	356	178	−
360	15	24	5	15	122	1	23	63	179	116	15	24	5	15	122	2	46	63	179	116	15	24	5	15	122	1	23	63	63	179	116
361	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−
362	−	−	−	−	−	−	−	−	−	−	2	181	2	2	363	1	180	181	180	−	2	181	2	2	363	1	180	181	360	180	−
363	−	−	−	−	−	−	−	−	−	−	3	121	3	3	364	1	120	123	181	58	3	121	3	3	364	1	120	123	240	181	−
364	28	13	6	31	79	1	12	125	181	56	7	52	4	7	210	1	51	63	181	118	14	26	5	15	132	1	25	65	65	181	116
365	73	5	10	511	54	5	22	724	182	−	5	73	5	15	366	1	72	112	182	70	5	73	5	15	366	1	72	112	144	182	38
366	−	−	−	−	−	−	−	−	−	−	6	61	4	7	245	1	60	72	182	110	6	61	4	7	245	1	60	72	120	182	62
368	−	−	−	−	−	−	−	−	−	−	8	46	5	15	230	1	45	85	183	98	8	46	5	15	230	1	45	85	90	183	93
369	−	−	−	−	−	−	−	−	−	−	3	123	3	3	370	1	122	125	184	59	9	41	7	63	288	2	80	217	217	184	−
370	−	−	−	−	−	−	−	−	−	−	5	74	5	15	371	1	73	113	184	71	10	37	6	31	223	2	72	123	144	184	40
371	−	−	−	−	−	−	−	−	−	−	7	53	4	7	214	1	52	64	185	121	7	53	4	7	214	1	52	64	104	185	81

	EG1										EG2										EG3										
N	n	l	m	g	I	t	F	T	ρ	D1	n	l	m	g	I	t	F	T	ρ	D2	n	l	m	g	I	t	F	T	T_M	ρ	D3
372	31	12	6	31	76	2	22	73	185	112	31	12	6	31	76	3	33	64	185	121	31	12	6	31	76	3	33	64	66	185	119
374	–	–	–	–	–	–	–	–	–	–	2	187	2	2	375	1	186	187	186	–	2	187	2	2	375	1	186	187	372	186	–
375	–	–	–	–	–	–	–	–	–	–	15	25	5	15	127	1	24	64	187	123	15	25	5	15	127	1	24	64	64	187	123
376	–	–	–	–	–	–	–	–	–	–	8	47	5	15	235	1	46	86	187	101	8	47	5	15	235	1	46	86	92	187	95
377	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
378	126	3	8	127	27	9	23	77	188	111	7	54	4	7	218	1	53	65	188	123	14	27	5	15	137	1	26	66	66	188	122
380	20	19	7	63	133	1	18	308	189	–	4	95	3	4	285	1	94	99	189	90	20	19	7	63	133	3	54	139	139	189	50
381	127	3	8	127	29	9	23	77	190	113	127	3	8	127	29	14	37	66	190	124	127	3	8	127	29	12	32	68	68	190	122
382	–	–	–	–	–	–	–	–	–	–	2	191	2	2	383	1	190	191	190	–	2	191	2	2	383	1	190	191	380	190	–
384	24	16	7	63	112	1	15	305	191	–	12	32	5	15	160	1	31	71	191	120	12	32	5	15	160	1	31	71	71	191	120
385	35	11	8	127	90	2	20	362	192	–	7	55	4	7	222	1	54	66	192	126	7	55	4	7	222	1	54	66	108	192	84
386	–	–	–	–	–	–	–	–	–	–	2	193	2	2	387	1	192	193	192	–	2	193	2	2	387	1	192	193	384	192	–
387	–	–	–	–	–	–	–	–	–	–	3	129	3	3	388	1	128	131	193	62	9	43	7	63	302	2	84	221	221	193	–
388	–	–	–	–	–	–	–	–	–	–	4	97	3	4	291	1	96	101	193	92	4	97	3	4	291	1	96	101	192	193	1
390	30	13	6	31	80	1	12	125	194	69	15	26	5	15	132	1	25	65	194	129	15	26	5	15	132	1	25	65	65	194	129
391	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
392	28	14	6	31	85	1	13	126	195	69	7	56	4	7	226	1	55	67	195	128	14	28	5	15	142	1	27	67	67	195	128
393	–	–	–	–	–	–	–	–	–	–	3	131	3	3	394	1	130	133	196	63	3	131	3	3	394	1	130	133	260	196	–
394	–	–	–	–	–	–	–	–	–	–	2	197	2	2	395	1	196	197	196	–	2	197	2	2	395	1	196	197	392	196	–
395	–	–	–	–	–	–	–	–	–	–	5	79	5	15	396	1	78	118	197	79	5	79	5	15	396	1	78	118	156	197	41
396	18	22	8	127	177	1	21	730	197	–	12	33	5	15	165	1	32	72	197	125	12	33	5	15	165	1	32	72	72	197	125
398	–	–	–	–	–	–	–	–	–	–	2	199	2	2	399	1	198	199	198	–	2	199	2	2	399	1	198	199	396	198	–
399	21	19	6	31	116	1	18	131	199	68	7	57	4	7	230	1	56	68	199	131	21	19	6	31	116	2	36	87	87	199	112
400	20	20	7	63	140	1	19	309	199	–	8	50	5	15	250	1	49	89	199	110	8	50	5	15	250	1	49	89	98	199	101
402	–	–	–	–	–	–	–	–	–	–	6	67	4	7	269	1	66	78	200	122	6	67	4	7	269	1	66	78	132	200	68
403	31	13	6	31	82	1	12	125	201	76	31	13	6	31	82	3	36	67	201	134	31	13	6	31	82	3	36	67	72	201	129
404	–	–	–	–	–	–	–	–	–	–	4	101	3	4	303	1	100	105	201	96	4	101	3	4	303	1	100	105	200	201	1
405	–	–	–	–	–	–	–	–	–	–	15	27	5	15	137	1	26	66	202	136	15	27	5	15	137	1	26	66	66	202	136

Results of our analysis, *continued*

	EG1										EG2										EG3										
N	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$	n	l	m	g	I	t	F	T	T_M	ρ	$D3$
406	—	—	—	—	—	—	—	—	—	—	14	29	5	15	147	1	28	68	202	134	14	29	5	15	147	1	28	68	68	202	134
407	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
408	24	17	7	63	119	1	16	306	203	—	12	34	5	15	170	1	33	73	203	130	12	34	5	15	170	1	33	73	73	203	130
410	—	—	—	—	—	—	—	—	—	—	5	82	5	15	411	1	81	121	204	83	10	41	6	31	247	1	40	153	153	204	51
411	—	—	—	—	—	—	—	—	—	—	3	137	3	3	412	1	136	139	205	66	3	137	3	3	412	1	136	139	272	205	—
412	—	—	—	—	—	—	—	—	—	—	4	103	3	4	309	1	102	107	205	98	4	103	3	4	309	1	102	107	204	205	1
413	—	—	—	—	—	—	—	—	—	—	7	59	4	7	238	1	58	70	206	136	7	59	4	7	238	1	58	70	116	206	90
414	18	23	8	127	185	1	22	731	206	—	6	69	4	7	277	1	68	80	206	126	6	69	4	7	277	1	68	80	136	206	70
415	—	—	—	—	—	—	—	—	—	—	5	83	5	15	416	1	82	122	207	85	5	83	5	15	416	1	82	122	164	207	43
416	—	—	—	—	—	—	—	—	—	—	8	52	5	15	260	1	51	91	207	116	8	52	5	15	260	1	51	91	102	207	105
417	—	—	—	—	—	—	—	—	—	—	3	139	3	3	418	1	138	141	208	67	3	139	3	3	418	1	138	141	276	208	—
418	—	—	—	—	—	—	—	—	—	—	2	209	2	2	419	1	208	209	208	—	2	209	2	2	419	1	208	209	416	208	—
420	60	7	7	63	50	3	18	103	209	106	15	28	5	15	142	1	27	67	209	142	15	28	5	15	142	1	27	67	67	209	142
422	—	—	—	—	—	—	—	—	—	—	2	211	2	2	423	1	210	211	210	—	2	211	2	2	423	1	210	211	420	210	—
423	—	—	—	—	—	—	—	—	—	—	3	141	3	3	424	1	140	143	211	68	9	47	7	63	330	2	92	229	229	211	—
424	—	—	—	—	—	—	—	—	—	—	8	53	5	15	265	1	52	92	211	119	8	53	5	15	265	1	52	92	104	211	107
425	85	5	9	255	49	5	22	315	212	—	5	85	5	15	426	1	84	124	212	88	85	5	9	255	49	15	70	143	143	212	69
426	—	—	—	—	—	—	—	—	—	—	6	71	4	7	285	1	70	82	212	130	6	71	4	7	285	1	70	82	140	212	72
427	—	—	—	—	—	—	—	—	—	—	7	61	4	7	246	1	60	72	213	141	7	61	4	7	246	1	60	72	120	213	93
428	—	—	—	—	—	—	—	—	—	—	4	107	3	4	321	1	106	111	213	102	4	107	3	4	321	1	106	111	212	213	1
429	—	—	—	—	—	—	—	—	—	—	3	143	3	3	430	1	142	145	214	69	3	143	3	3	430	1	142	145	284	214	—
430	—	—	—	—	—	—	—	—	—	—	5	86	5	15	431	1	85	125	214	89	10	43	6	31	259	1	42	155	155	214	59
432	24	18	7	63	126	1	17	307	215	—	12	36	5	15	180	1	35	75	215	140	12	36	5	15	180	1	35	75	75	215	140
434	62	7	7	63	53	3	18	103	216	113	14	31	5	15	157	1	30	70	216	146	14	31	5	15	157	1	30	70	70	216	146
435	—	—	—	—	—	—	—	—	—	—	15	29	5	15	147	1	28	68	217	149	15	29	5	15	147	1	28	68	68	217	149
436	—	—	—	—	—	—	—	—	—	—	4	109	3	4	327	1	108	113	217	104	4	109	3	4	327	1	108	113	216	217	1
437	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
438	146	3	11	1023	37	9	23	859	218	—	6	73	4	7	293	1	72	84	218	134	6	73	4	7	293	1	72	84	144	218	74

Results of our analysis, *continued*

	EG1										EG2										EG3										
N	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$	n	l	m	g	I	t	F	T	T_M	ρ	$D3$
440	20	22	7	63	154	1	21	311	219	—	8	55	5	15	275	1	54	94	219	125	8	55	5	15	275	1	54	94	108	219	111
441	63	7	7	63	53	3	18	103	220	117	63	7	7	63	53	6	38	72	220	148	63	7	7	63	53	5	32	75	75	220	145
442	—	—	—	—	—	—	—	—	—	—	2	221	2	2	443	1	220	221	220	—	2	221	2	2	443	1	220	221	440	220	—
444	—	—	—	—	—	—	—	—	—	—	12	37	5	15	185	1	36	76	221	145	12	37	5	15	185	1	36	76	76	221	145
445	—	—	—	—	—	—	—	—	—	—	5	89	5	15	446	1	88	128	222	94	5	89	5	15	446	1	88	128	176	222	46
446	—	—	—	—	—	—	—	—	—	—	2	223	2	2	447	1	222	223	222	—	2	223	2	2	447	1	222	223	444	222	—
447	—	—	—	—	—	—	—	—	—	—	3	149	3	3	448	1	148	151	223	72	3	149	3	3	448	1	148	151	296	223	—
448	28	16	6	31	97	1	15	128	223	95	14	32	5	15	162	1	31	71	223	152	14	32	5	15	162	1	31	71	71	223	152
450	30	15	6	31	92	1	14	127	224	97	15	30	5	15	152	1	29	69	224	155	15	30	5	15	152	1	29	69	69	224	155
451	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
452	—	—	—	—	—	—	—	—	—	—	4	113	3	4	339	1	112	117	225	108	4	113	3	4	339	1	112	117	224	225	1
453	—	—	—	—	—	—	—	—	—	—	3	151	3	3	454	1	150	153	226	73	3	151	3	3	454	1	150	153	300	226	—
454	—	—	—	—	—	—	—	—	—	—	2	227	2	2	455	1	226	227	226	—	2	227	2	2	455	1	226	227	452	226	—
455	35	13	8	127	106	1	12	721	227	—	7	65	4	7	262	1	64	76	227	151	7	65	4	7	262	1	64	76	128	227	99
456	24	19	7	63	133	1	18	308	227	—	12	38	5	15	190	1	37	77	227	150	12	38	5	15	190	1	37	77	77	227	150
458	—	—	—	—	—	—	—	—	—	—	2	229	2	2	459	1	228	229	228	—	2	229	2	2	459	1	228	229	456	228	—
459	51	9	9	255	84	2	16	835	229	—	3	153	3	3	460	1	152	155	229	74	51	9	9	255	84	11	95	204	204	229	25
460	20	23	7	63	161	1	22	312	229	—	4	115	3	4	345	1	114	119	229	110	20	23	7	63	161	3	66	151	151	229	78
462	21	22	6	31	134	1	21	134	230	96	14	33	5	15	167	1	32	72	230	158	14	33	5	15	167	1	32	72	72	230	158
464	—	—	—	—	—	—	—	—	—	—	8	58	5	15	290	1	57	97	231	134	8	58	5	15	290	1	57	97	114	231	117
465	465	1	10	511	14	28	23	105	232	127	15	31	5	15	157	1	30	70	232	162	15	31	5	15	157	1	30	70	70	232	162
466	—	—	—	—	—	—	—	—	—	—	2	233	2	2	467	1	232	233	232	—	2	233	2	2	467	1	232	233	464	232	—
468	36	13	9	255	117	1	12	1688	233	—	12	39	5	15	195	1	38	78	233	155	12	39	5	15	195	1	38	78	78	233	155
469	—	—	—	—	—	—	—	—	—	—	7	67	4	7	270	1	66	78	234	156	7	67	4	7	270	1	66	78	132	234	102
470	—	—	—	—	—	—	—	—	—	—	5	94	5	15	471	1	93	133	234	101	10	47	6	31	283	1	46	159	159	234	75
471	—	—	—	—	—	—	—	—	—	—	3	157	3	3	472	1	156	159	235	76	3	157	3	3	472	1	156	159	312	235	—
472	—	—	—	—	—	—	—	—	—	—	8	59	5	15	295	1	58	98	235	137	8	59	5	15	295	1	58	98	116	235	119
473	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—

Results of our analysis, *continued*

N	EG1 n	l	m	g	I	t	F	T	ρ	D1	EG2 n	l	m	g	I	t	F	T	ρ	D2	EG3 n	l	m	g	I	t	F	T	T_M	ρ	D3
474	—	—	—	—	—	—	—	—	—	—	6	79	4	7	317	1	78	90	236	146	6	79	4	7	317	1	78	90	156	236	80
475	—	—	—	—	—	—	—	—	—	—	5	95	5	15	476	1	94	134	237	103	5	95	5	15	476	1	94	134	188	237	49
476	28	17	6	31	103	1	16	129	237	108	14	34	5	15	172	1	33	73	237	164	14	34	5	15	172	1	33	73	73	237	164
477	—	—	—	—	—	—	—	—	—	—	3	159	3	3	478	1	158	161	238	77	9	53	7	63	372	2	104	241	241	238	—
478	—	—	—	—	—	—	—	—	—	—	2	239	2	2	479	1	238	239	238	—	2	239	2	2	479	1	238	239	476	238	—
480	60	8	7	63	57	3	21	106	239	133	15	32	5	15	162	1	31	71	239	168	15	32	5	15	162	1	31	71	71	239	168
481	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
482	—	—	—	—	—	—	—	—	—	—	2	241	2	2	483	1	240	241	240	—	2	241	2	2	483	1	240	241	480	240	—
483	21	23	6	31	140	1	22	135	241	106	7	69	4	7	278	1	68	80	241	161	21	23	6	31	140	2	44	95	95	241	146
484	—	—	—	—	—	—	—	—	—	—	4	121	3	4	363	1	120	125	241	116	4	121	3	4	363	1	120	125	240	241	1
485	—	—	—	—	—	—	—	—	—	—	5	97	5	15	486	1	96	136	242	106	5	97	5	15	486	1	96	136	192	242	50
486	—	—	—	—	—	—	—	—	—	—	6	81	4	7	325	1	80	92	242	150	6	81	4	7	325	1	80	92	160	242	82
488	—	—	—	—	—	—	—	—	—	—	8	61	5	15	305	1	60	100	243	143	8	61	5	15	305	1	60	100	120	243	123
489	—	—	—	—	—	—	—	—	—	—	3	163	3	3	490	1	162	165	244	79	3	163	3	3	490	1	162	165	324	244	—
490	70	7	9	255	65	3	18	545	244	—	14	35	5	15	177	1	34	74	244	170	14	35	5	15	177	1	34	74	74	244	170
492	—	—	—	—	—	—	—	—	—	—	12	41	5	15	205	1	40	80	245	165	12	41	5	15	205	1	40	80	80	245	165
493	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
494	—	—	—	—	—	—	—	—	—	—	2	247	2	2	495	1	246	247	246	—	2	247	2	2	495	1	246	247	492	246	—
495	—	—	—	—	—	—	—	—	—	—	15	33	5	15	167	1	32	72	247	175	15	33	5	15	167	1	32	72	72	247	175
496	62	8	7	63	60	3	21	106	247	141	31	16	6	31	100	3	45	76	247	171	62	8	7	63	60	5	37	80	80	247	167
497	—	—	—	—	—	—	—	—	—	—	7	71	4	7	286	1	70	82	248	166	7	71	4	7	286	1	70	82	140	248	108
498	—	—	—	—	—	—	—	—	—	—	6	83	4	7	333	1	82	94	248	154	6	83	4	7	333	1	82	94	164	248	84
500	—	—	—	—	—	—	—	—	—	—	4	125	3	4	375	1	124	129	249	120	20	25	7	63	175	3	72	157	157	249	92
501	—	—	—	—	—	—	—	—	—	—	3	167	3	3	502	1	166	169	250	81	3	167	3	3	502	1	166	169	332	250	—
502	—	—	—	—	—	—	—	—	—	—	2	251	2	2	503	1	250	251	250	—	2	251	2	2	503	1	250	251	500	250	—
504	63	8	7	63	60	3	21	106	251	145	14	36	5	15	182	1	35	75	251	176	14	36	5	15	182	1	35	75	75	251	176
505	—	—	—	—	—	—	—	—	—	—	5	101	5	15	506	1	100	140	252	112	5	101	5	15	506	1	100	140	200	252	52
506	—	—	—	—	—	—	—	—	—	—	2	253	2	2	507	1	252	253	252	—	2	253	2	2	507	1	252	253	504	252	—

Results of our analysis, *continued*

N	EG1										EG2										EG3										
	n	l	m	g	I	t	F	T	ρ	D1	n	l	m	g	I	t	F	T	ρ	D2	n	l	m	g	I	t	F	T	T_M	ρ	D3
507	—	—	—	—	—	—	—	—	—	—	3	169	3	3	508	1	168	171	253	82	3	169	3	3	508	1	168	171	336	253	—
508	508	1	10	511	13	28	23	105	253	148	127	4	8	127	37	13	47	80	253	173	127	4	8	127	37	11	40	81	81	253	172
510	510	1	10	511	14	28	23	105	254	149	15	34	5	15	172	1	33	73	254	181	15	34	5	15	172	1	33	73	73	254	181
511	511	1	10	511	17	28	23	105	255	150	511	1	10	511	17	52	46	80	255	175	511	1	10	511	17	46	41	81	82	255	173
512	—	—	—	—	—	—	—	—	—	—	8	64	5	15	320	1	63	103	255	152	8	64	5	15	320	1	63	103	126	255	129
513	—	—	—	—	—	—	—	—	—	—	3	171	3	3	514	1	170	173	256	83	9	57	7	63	400	2	112	249	249	256	7
514	—	—	—	—	—	—	—	—	—	—	2	257	2	2	515	1	256	257	256	—	2	257	2	2	515	1	256	257	512	256	—
515	—	—	—	—	—	—	—	—	—	—	5	103	5	15	516	1	102	142	257	115	5	103	5	15	516	1	102	142	204	257	53
516	—	—	—	—	—	—	—	—	—	—	12	43	5	15	215	1	42	82	257	175	12	43	5	15	215	1	42	82	84	257	173
517	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
518	—	—	—	—	—	—	—	—	—	—	14	37	5	15	187	1	36	76	258	182	14	37	5	15	187	1	36	76	76	258	182
519	—	—	—	—	—	—	—	—	—	—	3	173	3	3	520	1	172	175	259	84	3	173	3	3	520	1	172	175	344	259	—
520	40	13	9	255	117	1	12	1688	259	—	8	65	5	15	325	1	64	104	259	155	8	65	5	15	325	1	64	104	128	259	131
522	—	—	—	—	—	—	—	—	—	—	6	87	4	7	349	1	86	98	260	162	6	87	4	7	349	1	86	98	172	260	88
524	—	—	—	—	—	—	—	—	—	—	4	131	3	4	393	1	130	135	261	126	4	131	3	4	393	1	130	135	260	261	1
525	105	5	8	127	43	5	22	139	262	123	15	35	5	15	177	1	34	74	262	188	15	35	5	15	177	1	34	74	74	262	188
526	—	—	—	—	—	—	—	—	—	—	2	263	2	2	527	1	262	263	262	—	2	263	2	2	527	1	262	263	524	262	—
527	31	17	6	31	106	1	16	129	263	134	31	17	6	31	106	3	48	79	263	184	31	17	6	31	106	2	32	83	83	263	180
528	24	22	7	63	154	1	21	311	263	—	12	44	5	15	220	1	43	83	263	180	12	44	5	15	220	1	43	83	86	263	177
529	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
530	—	—	—	—	—	—	—	—	—	—	5	106	5	15	531	1	105	145	264	119	10	53	6	31	319	1	52	165	165	264	99
531	—	—	—	—	—	—	—	—	—	—	3	177	3	3	532	1	176	179	265	86	9	59	7	63	414	2	116	253	253	265	12
532	28	19	6	31	115	1	18	131	265	134	14	38	5	15	192	1	37	77	265	188	14	38	5	15	192	1	37	77	77	265	188
533	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
534	—	—	—	—	—	—	—	—	—	—	6	89	4	7	357	1	88	100	266	166	6	89	4	7	357	1	88	100	176	266	90
535	—	—	—	—	—	—	—	—	—	—	5	107	5	15	536	1	106	146	267	121	5	107	5	15	536	1	106	146	212	267	55
536	—	—	—	—	—	—	—	—	—	—	8	67	5	15	335	1	66	106	267	161	8	67	5	15	335	1	66	106	132	267	135
537	—	—	—	—	—	—	—	—	—	—	3	179	3	3	538	1	178	181	268	87	3	179	3	3	538	1	178	181	356	268	—

Results of our analysis, *continued*

N	EG1										EG2										EG3										
	n	*l*	*m*	*g*	*I*	*t*	*F*	*T*	*ρ*	*D1*	*n*	*l*	*m*	*g*	*I*	*t*	*F*	*T*	*ρ*	*D2*	*n*	*l*	*m*	*g*	*I*	*t*	*F*	*T*	*T_M*	*ρ*	*D3*
538	—	—	—	—	—	—	—	—	—	—	2	269	2	2	539	1	268	269	268	—	2	269	2	2	539	1	268	269	536	268	—
539	—	—	—	—	—	—	—	—	—	—	7	77	4	7	310	1	76	88	269	181	7	77	4	7	310	1	76	88	152	269	117
540	30	18	6	31	110	1	17	130	269	139	15	36	5	15	182	1	35	75	269	194	15	36	5	15	182	1	35	75	75	269	194
542	—	—	—	—	—	—	—	—	—	—	2	271	2	2	543	1	270	271	270	—	2	271	2	2	543	1	270	271	540	270	—
543	—	—	—	—	—	—	—	—	—	—	3	181	3	3	544	1	180	183	271	88	3	181	3	3	544	1	180	183	360	271	—
544	—	—	—	—	—	—	—	—	—	—	8	68	5	15	340	1	67	107	271	164	8	68	5	15	340	1	67	107	134	271	137
545	—	—	—	—	—	—	—	—	—	—	5	109	5	15	546	1	108	148	272	124	5	109	5	15	546	1	108	148	216	272	56
546	42	13	7	63	93	1	12	302	272	—	14	39	5	15	197	1	38	78	272	194	14	39	5	15	197	1	38	78	78	272	194
548	—	—	—	—	—	—	—	—	—	—	4	137	3	4	411	1	136	141	273	132	4	137	3	4	411	1	136	141	272	273	1
549	—	—	—	—	—	—	—	—	—	—	3	183	3	3	550	1	182	185	274	89	9	61	7	63	428	2	120	257	257	274	17
550	—	—	—	—	—	—	—	—	—	—	5	110	5	15	551	1	109	149	274	125	10	55	6	31	331	1	54	167	167	274	107
551	—										—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
552	24	23	7	63	161	1	22	312	275	—	12	46	5	15	230	1	45	85	275	190	12	46	5	15	230	1	45	85	90	275	185
553	—	—	—	—	—	—	—	—	—	—	7	79	4	7	318	1	78	90	276	186	7	79	4	7	318	1	78	90	156	276	120
554	—	—	—	—	—	—	—	—	—	—	2	277	2	2	555	1	276	277	276	—	2	277	2	2	555	1	276	277	552	276	—
555	—	—	—	—	—	—	—	—	—	—	15	37	5	15	187	1	36	76	277	201	15	37	5	15	187	1	36	76	76	277	201
556	—	—	—	—	—	—	—	—	—	—	4	139	3	4	417	1	138	143	277	134	4	139	3	4	417	1	138	143	276	277	1
558	31	18	6	31	112	1	17	130	278	148	31	18	6	31	112	3	51	82	278	196	31	18	6	31	112	2	34	85	85	278	193
559	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—
560	28	20	6	31	121	1	19	132	279	147	14	40	5	15	202	1	39	79	279	200	14	40	5	15	202	1	39	79	79	279	200
561	51	11	9	255	102	2	20	839	280	—	3	187	3	3	562	1	186	189	280	91	51	11	9	255	102	10	106	230	230	280	50
562	—	—	—	—	—	—	—	—	—	—	2	281	2	2	563	1	280	281	280	—	2	281	2	2	563	1	280	281	560	280	—
564	—	—	—	—	—	—	—	—	—	—	12	47	5	15	235	1	46	86	281	195	12	47	5	15	235	1	46	86	92	281	189
565	—	—	—	—	—	—	—	—	—	—	5	113	5	15	566	1	112	152	282	130	5	113	5	15	566	1	112	152	224	282	58
566	—	—	—	—	—	—	—	—	—	—	2	283	2	2	567	1	282	283	282	—	2	283	2	2	567	1	282	283	564	282	—
567	63	9	7	63	67	2	16	153	283	130	63	9	7	63	67	6	50	84	283	199	63	9	7	63	67	5	42	85	85	283	198
568	—	—	—	—	—	—	—	—	—	—	8	71	5	15	355	1	70	110	283	173	8	71	5	15	355	1	70	110	140	283	143
570	30	19	6	31	116	1	18	131	284	153	15	38	5	15	192	1	37	77	284	207	15	38	5	15	192	1	37	77	77	284	207

Results of our analysis, *continued*

N	\multicolumn{10}{c}{EG1}										\multicolumn{10}{c}{EG2}										\multicolumn{11}{c}{EG3}										
	n	l	m	g	I	t	F	T	ρ	$D1$	n	l	m	g	I	t	F	T	ρ	$D2$	n	l	m	g	I	t	F	T	T_M	ρ	$D3$
572	−	−	−	−	−	−	−	−	−	−	4	143	3	4	429	1	142	147	285	138	4	143	3	4	429	1	142	147	284	285	1
573	−	−	−	−	−	−	−	−	−	−	3	191	3	3	574	1	190	193	286	93	3	191	3	3	574	1	190	193	380	286	−
574	−	−	−	−	−	−	−	−	−	−	14	41	5	15	207	1	40	80	286	206	14	41	5	15	207	1	40	80	80	286	206
575	−	−	−	−	−	−	−	−	−	−	5	115	5	15	576	1	114	154	287	133	5	115	5	15	576	1	114	154	228	287	59
576	24	24	7	63	168	1	23	313	287	−	12	48	5	15	240	1	47	87	287	200	12	48	5	15	240	1	47	87	94	287	193
578	−	−	−	−	−	−	−	−	−	−	2	289	2	2	579	1	288	289	288	−	2	289	2	2	579	1	288	289	576	288	−
579	−	−	−	−	−	−	−	−	−	−	3	193	3	3	580	1	192	195	289	94	3	193	3	3	580	1	192	195	384	289	−
580	−	−	−	−	−	−	−	−	−	−	4	145	3	4	435	1	144	149	289	140	20	29	7	63	203	3	84	169	169	289	120
581	−	−	−	−	−	−	−	−	−	−	7	83	4	7	334	1	82	94	290	196	7	83	4	7	334	1	82	94	164	290	126
582	−	−	−	−	−	−	−	−	−	−	6	97	4	7	389	1	96	108	290	182	6	97	4	7	389	1	96	108	192	290	98
583	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−	−
584	73	8	10	511	84	3	21	1260	291	−	8	73	5	15	365	1	72	112	291	179	8	73	5	15	365	1	72	112	144	291	147
585	585	1	13	4095	19	28	23	1208	292	−	15	39	5	15	197	1	38	78	292	214	15	39	5	15	197	1	38	78	78	292	214
586	−	−	−	−	−	−	−	−	−	−	2	293	2	2	587	1	292	293	292	−	2	293	2	2	587	1	292	293	584	292	−
588	28	21	6	31	127	1	20	133	293	160	14	42	5	15	212	1	41	81	293	212	14	42	5	15	212	1	41	81	82	293	211
589	31	19	6	31	118	1	18	131	294	163	31	19	6	31	118	3	54	85	294	209	31	19	6	31	118	2	36	87	87	294	207
590	−	−	−	−	−	−	−	−	−	−	5	118	5	15	591	1	117	157	294	137	10	59	6	31	355	1	58	171	171	294	123
591	−	−	−	−	−	−	−	−	−	−	3	197	3	3	592	1	196	199	295	96	3	197	3	3	592	1	196	199	392	295	−
592	−	−	−	−	−	−	−	−	−	−	8	74	5	15	370	1	73	113	295	182	8	74	5	15	370	1	73	113	146	295	149
594	−	−	−	−	−	−	−	−	−	−	6	99	4	7	397	1	98	110	296	186	6	99	4	7	397	1	98	110	196	296	100
595	595	1	12	2047	17	28	23	529	297	−	7	85	4	7	342	1	84	96	297	201	7	85	4	7	342	1	84	96	168	297	129
596	−	−	−	−	−	−	−	−	−	−	4	149	3	4	447	1	148	153	297	144	4	149	3	4	447	1	148	153	296	297	1
597	−	−	−	−	−	−	−	−	−	−	3	199	3	3	598	1	198	201	298	97	3	199	3	3	598	1	198	201	396	298	−
598	−	−	−	−	−	−	−	−	−	−	2	299	2	2	599	1	298	299	298	−	2	299	2	2	599	1	298	299	596	298	−
600	30	20	6	31	122	1	19	132	299	167	15	40	5	15	202	1	39	79	299	220	15	40	5	15	202	1	39	79	79	299	220

Appendix 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 greater than or equal to 2^{160} for which $\#E_b(\mathbb{F}_{2^{161}})$ is twice a prime. Finally, the elliptic curves E176 and E272 are taken from ANSI X9.62 [1].

Appendix B.1.   *Elliptic curve generation*

Let $n = 31$, and let $q = 2^6$. 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, $0 \leqslant i \leqslant s$, be the monic irreducible factors of $x^{31} - 1$ over $\mathbb{F}_2$ with $f_0(x) = x - 1$ (see Theorem 11). Let $\sigma : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ be the Frobenius map defined by $x \mapsto x^q$. Define

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

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

$$a = \mathtt{3D7D03F4CB539C5B728D256DAD2E5E8ADDB81B524F7D68D}, \text{ and}$$

$$b = \mathtt{35108742308B720FAABCFFB70D33E3840F8D93323635F7E}$$

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

$$r = \mathtt{2000000000000000000000000E5BED0151962E91F6CDF581}$$

is prime.

Appendix B.2.   *ECDLP instance generation*

We selected two points P and 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. (These two strings are commonly used as inputs to generate test vectors for hash functions; see [25, Table 9.6].) 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 greaater than or equal to 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 select one of the two possible y-coordinates to obtain two points P' and Q', and then we set $P = 2P'$ and $Q = 2Q'$. In this way, we derive the following two points of

order r:

$$P = (\texttt{6FE4D23FBAFBAF66317050A0D102E23075572174ADC304},$$
$$\texttt{24E2CB9E1DAF261EA25FD0413F85CF067DB5FE50F4849B2});$$
$$Q = (\texttt{EFD00F993676085F97D9BB9117E00A34F6185104629F42},$$
$$\texttt{1EBBB1F436A53B00B4C74A93CF6E613F3C60D566BDB9653}).$$

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 by us a priori.

Appendix B.3. *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:

$$R = (\texttt{3A9EE09AEC0996B46F3680D80835FF3081D795A93AB58FF},$$
$$\texttt{FC867E29309F63717894B647A611E743919B511E204862}).$$

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 $J_{C186}(\mathbb{F}_{2^6})$. 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

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

The divisors D_1, D_2 and D_3 are:

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

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

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

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

Appendix C. *ECDLP challenge parameters*

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

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

$b = $ `1102A36EE3EEE95C1DDA26A51A954391733728D22`

$r = $ `FFFFFFFFFFFFFFFFFFFFFFFD03F975D827A7D20F89`

$P = ($ `1CBF654BEEF0AE9F525F8E9F5FA1DED1D10C7D781`,

`175984F97695A39291B94B6D9BD89860C9AF5DF80`$)$

$Q = ($ `AE24976AE483ED2E33A77FD48F78DAE06ED0F54E`,

`186EBA8B979ADAA320D47C7763CFF8EF810A970EB`$)$

$R = ($ `1E7958EF1FA48A2B92889B442DADE6E9A6A7C173`,

`4EE6671B1A5D69A5578EFE30C05704FA69C78345`$)$

C161, $q = 2^{23}$, $\mathbb{F}_{2^{23}} = \mathbb{F}_2[w]/(w^{23} + w^5 + 1)$

$f(u) = w^{6691705}u^{15} + w^{4316786}u^{14} + w^{4857716}u^{12} + w^{4289455}u^8 + w^{7257339}$

$h(u) = w^{7540156}u^7 + w^{4708240}u^6 + w^{2060647}u^4 + w^{7822973}$

$D_1 = \mathrm{div}(u^7+w^{111674}u^6+w^{6262987}u^5+w^{5507868}u^4+w^{5024071}u^3+w^{7360243}u^2$
$$+w^{4982988}u+w^{3476956},\ w^{7214579}u^6+w^{1039748}u^5+w^{5362902}u^4$$
$$+w^{5575575}u^3+w^{6046318}u^2+w^{783556}u+w^{7954483})$$

$D_2 = \mathrm{div}(u^7+w^{2418740}u^6+w^{6332447}u^5+w^{5288518}u^4+w^{6581623}u^3+w^{3461659}u^2$
$$+w^{663714}u+w^{2094946},\ w^{5819570}u^6+w^{5789770}u^5+w^{3853008}u^4$$
$$+w^{3628267}u^3+w^{4786898}u^2+w^{3463517}u+w^{2504145})$$

$D_3 = \mathrm{div}(u^7+w^{7595037}u^6+w^{6492024}u^5+w^{5128797}u^4+w^{1479702}u^3+w^{3764869}u^2$
$$+w^{2973617}u+w^{3579984},\ w^{5819570}u^6+w^{5789770}u^5+w^{3853008}u^4$$
$$+w^{3628267}u^3+w^{4786898}u^2+w^{3463517}u+w^{2504145})$$

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

$a = $ B3C8B5AF89342D73C9D12F1F5ACDD36011626BBC675C1

$b = $ 990D04982994434CB4C14DB21204025865B40069225B2

$r = $ 800000000000000000000023ABAE178BD70C3E01FDC31

$P = $ (EE4AB1D7C359522ED9CABE52021DAD0EAF613C1ECE8CB,

670775621CD859D56079BB52298C0A509AB4E689593F9)

$Q = $ (7F13258D03372C8A571E8C199DD9416A7642DDA05C515,

1182432B1B3C6C1856D47B139B28E003B6D9F440574FF)

$R = $ (BAD2E0D1D655559AF62E346BE2090135E40AEC22EE5C3,

B5B71A32C4498B8CF0DF6BB90911D91CC16F506D508C5)

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

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

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

$D_1 = \text{div}(u^{15} + w^{913}u^{14} + w^{120}u^{13} + w^{1222}u^{12} + w^{717}u^{11} + w^{1158}u^{10} + w^{406}u^9$

$\qquad + w^{3864}u^8 + w^{3391}u^7 + w^{3302}u^6 + w^{906}u^5 + w^{2528}u^4 + w^{3620}u^3 + w^{1164}u^2$

$\qquad + w^{119}u + w^{68},\ w^{3862}u^{14} + w^{1139}u^{13} + w^{4055}u^{12} + w^{3324}u^{11} + w^{1436}u^{10}$

$\qquad + w^{1968}u^9 + w^{1488}u^8 + w^{22}u^7 + w^{3071}u^6 + w^{1736}u^5 + w^{394}u^4 + w^{1892}u^3$

$\qquad + w^{3461}u^2 + w^{923}u + w^{2371})$

$D_2 = \text{div}(u^{15} + w^{2828}u^{14} + w^{2507}u^{13} + w^{2845}u^{12} + w^{3821}u^{11} + w^{550}u^{10} + w^{837}u^9$

$\qquad + w^{3146}u^8 + w^{1040}u^7 + w^{1551}u^6 + w^{2806}u^5 + w^{2321}u^4 + w^{251}u^3 + w^{3983}u^2$

$\qquad + w^{1482}u + w^{1796},\ w^{2370}u^{14} + w^{3993}u^{13} + w^{2270}u^{12} + w^{3787}u^{11} + w^{2128}u^{10}$

$\qquad + w^{2948}u^9 + w^{72}u^8 + w^{27}u^7 + w^{1515}u^6 + w^{1684}u^5 + w^{385}u^4 + w^{3635}u^3$

$\qquad + w^{1076}u^2 + w^{1654}u + w^{3081})$

$D_3 = \text{div}(u^{15} + w^{2485}u^{14} + w^{1754}u^{13} + w^{1638}u^{12} + w^{2078}u^{11} + w^{4039}u^{10} + w^{2857}u^9$

$\qquad + w^{2716}u^8 + w^{230}u^7 + w^{1139}u^6 + w^{1330}u^5 + w^{851}u^4 + w^{1926}u^3 + w^{428}u^2$

$\qquad + w^{2628}u + w^{2729},\ w^{2543}u^{14} + w^{998}u^{13} + w^{37}u^{12} + w^{1097}u^{11} + w^{2830}u^{10}$

$\qquad + w^{770}u^9 + w^{2604}u^8 + w^{3011}u^7 + w^{2334}u^6 + w^{863}u^5 + w^{1952}u^4 + w^{1777}u^3$

$\qquad + w^{1122}u^2 + w^{1754}u + w^{3677})$

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

$a = $ 3D7D03F4CB539C5B728D256DAD2E5E8ADDB81B524F7D68D

$b = $ 35108742308B720FAABCFFB70D33E3840F8D93323635F7E

$r = $ 2000000000000000000000000E5BED0151962E91F6CDF581

$P = $ (6FE4D23FBAFBAF66317050A0D102E23075572174ADC304,
    24E2CB9E1DAF261EA25FD0413F85CF067DB5FE50F4849B2)

$Q = $ (EFD00F993676085F97D9BB9117E00A34F6185104629F42,
    1EBBB1F436A53B00B4C74A93CF6E613F3C60D566BDB9653)

$R = $ (3A9EE09AEC0996B46F3680D80835FF3081D795A93AB58FF,
    FC867E29309F63717894B647A611E743919B511E204862)

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

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

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

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

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

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

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

$b = $ `11E8F97F344082577BB4D782D3F433FBE30D8F3D65684AE499694BA`

$r = $ `10000000000000000000000000000000598FB15077594E7069CED749A1`

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

$\quad a = $ C65B1B2B48E3A7B2BC69C365B4CAE385CE3F023A9742C0EF16
$\qquad$ C40E1D62ADA2

$\quad b = $ 1649390E2C5BBA8206486E33D3273AE269EE568F91AC46BC86
$\qquad$ A6A792CF6CEA

$\quad r = $ 8000000000000000000000000000000004B55AAB05CC2C4EE2E6
$\qquad$ 973D0C247E01

$\quad P = $ (4AF353C030AADA55B6FAED2BBF314EBC28C8B6FB1DFC09272
$\qquad$ 8A28E70F0E73F, 168FADD57DC3046C69A0121310D284A04C
$\qquad$ 145E0ECB88B91BAD8BE25F58CBE9)

$\quad Q = $ (62231B26EEF12154100D6257F7148AC78C5A61FC129532449
$\qquad$ 4368A42CA9FD5, 403910538623DE3633D0FD6690E12F4D81
$\qquad$ D1915D3728C5617CD6A65B92AA41)

$\quad R = $ (D69A12AFCF86A8CF9F30051B8C655D050B238A215C19C8512
$\qquad$ D41B547C1ADE2, A3FDA75DB34F93EF657FAAB2163AE05E0C
$\qquad$ C1241175CE1E880841F77A369B8B)

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

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

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

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

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

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

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

$a = $ 8F8EEC356CB05D6FC50A73F3639AB70C19A18E5234A172276EE
631E42A6A2CE5A28250424E4

$b = $ 44808A33D47780EC13CC721C66605252A082008AC5910272188
6382368CCB415802A4E95ACE

$r = $ 7FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF09A007BD63597
47C0A7181FC6DA9704EFB0C1

$P = ($ 9F080369EA917727D1E1C709CC5BF2674AA7C79A2DFA5E5B44
7F364F61690CD6DBAC05F5EFD, 558B8FB728CECBB9D0AA367
687E17D6E97793769C71645AA168EEDCA3E2AE03D642B722572$)$

$Q = ($ F93C3685D5E9AB2A0F7C7BD7F687A9C4E42C10C94BD477F419
E5C25B6E643B919F51CB3730B, 4C11A5F31FAD729F839F98D
34FB59D279C70A3126FFC3D5C1611F949340EEE12474A66263AC$)$

$R = ($ FF00541676FD0036D12C0FEC3A1B8D8C692627F4E8DB62F45B
708D9431C2E99F299984FD406, 37E09E68926A8157861A512
A86696A4A78A0F0C15F9EAC4AECF8BF6D2B818284E8C3F5853BD$)$

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

$a = 1$

$b = 1000000000000000000000000000000000000000062$

$r = \text{FFFFFFFFFFFFFFFFFFFFFD5D528D29B3677A6BF15}$

$P = (\text{1590236CF8BCADEA57D2ABABDC7C918CD991F7FD1},$
$\quad\ \text{16019BB593140463E7C859426E4AD76188D4EA3C8})$

$Q = (\text{ACA7F2D366101B27A6043551C0B0D8C60A32ED98},$
$\quad\ \text{C15307FE705B5A5D638B40DF023D202E434D7D75})$

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

$a = \text{E4E6DB2995065C407D9D39B8D0967B96704BA8E9C90B}$

$b = \text{5DDA470ABE6414DE8EC133AE28E9BBD7FCEC0AE0FFF2}$

$r = \text{10092537397ECA4F6145799D62B0A19CE06FE26AD}$

$P = (\text{96E2498B189AAD455FC2431323B24E0603155C4EEE24},$
$\quad\ \text{2056F497331B645ACAB8519F3F71099A71EBDD7E2D06})$

$Q = (\text{8CE8805EA1D92A77975F69988FF0B2C99A3C344D469D},$
$\quad\ \text{27A65C20DA08E0732D6327CF41E3C4B27AB9DB63706A})$

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

$a = \text{91A091F03B5FBA4AB2CCF49C4EDD220FB028712D42BE752B2C4}$
$\quad\ \text{0094DBACDB586FB20}$

$b = \text{7167EFC92BB2E3CE7C8AAAFF34E12A9C557003D7C73A6FAF003}$
$\quad\ \text{F99F6CC8482E540F7}$

$r = \text{100FAF51354E0E39E4892DF6E319C72C8161603FA45AA7B998A}$
$\quad\ \text{167B8F1E629521}$

$P = (\text{DE9DE5CD3B90447A206BEFE8167505CB7A28616DADABC639B42}$
$\quad\ \text{1DF763F961D689DA9}, \text{49831637686123445336FE8B59FF791C7}$
$\quad\ \text{1CF455823A4C375280A148B043DE7ECF17F})$

$Q = (\text{C9189420F828C242771E2D64768930089AB56BA7E6D3A1DB294}$
$\quad\ \text{AEDAD60BAC9591E65}, \text{EB0123561D81715B23575A5DF3B13A771}$
$\quad\ \text{C8521523C4EA853C0C4DF3294F70BF65AAA})$

References

1. ANSI X9.62, *Public key cryptography for the financial services industry: the elliptic curve digital signature algorithm* (*ECDSA*), 1999. 140, 164

2. S. ARITA, 'Weil descent of elliptic curves over finite fields of characteristic three', *Advances in Cryptology – Asiacrypt 2000*, Lecture Notes in Comput. Sci. 1976 (Springer, 2000) 248–259. 146

3. E. ARTIN, 'Quadratische Körper im Gebiete der höheren Kongruenzen', *Math. Z.* 19 (1924) 207–246. 129

4. D. CANTOR, 'Computing in the jacobian of a hyperelliptic curve', *Math. Comp.* 48 (1987) 95–101. 129

5. D. COPPERSMITH, A. ODLYZKO and R. SCHROEPPEL, 'Discrete logarithms in $GF(p)$', *Algorithmica*, 1 (1986) 1–15. 134

6. M. DABERKOW, C. FIEKER, J. KLÜNERS, M. POHST, K. ROEGNER, M. SCHÖRNIG and K. WILDANGER, 'KANT V4', *J. Symbolic Comput.* 24 (1997) 267–283. 131

7. C. DIEM, 'A study on theoretical and practical aspects of Weil-restrictions of varieties', Ph.D. thesis, University of Essen, 2001. 146, 146

8. A. ENGE and P. GAUDRY, 'A general framework for subexponential discrete logarithm algorithms', *Acta Arith.* 102 (2002) 83–103. 133

9. M. FOUQUET, P. GAUDRY and R. HARLEY, 'An extension of Satoh's algorithm and its implementation', *J. Ramanujan Math. Soc.* 15 (2000) 281–318. 140

10. G. FREY, 'Applications of arithmetical geometry to cryptographic constructions', *Proceedings of the Fifth International Conference on Finite Fields and Applications* (Springer, 2001) 128–161. 127

11. G. FREY and H. RÜCK, 'A remark concerning m-divisibility', *Math. Comp.* 62 (1994) 865–874. 127

12. S. GALBRAITH, 'Constructing isogenies between elliptic curves over finite fields', *LMS J. Comput. Math.* 2 (1999) 118–138; http://www.lms.ac.uk/jcm/2/lms1998-010. 140

13. S. GALBRAITH and N. SMART, 'A cryptographic application of Weil descent', *Codes and cryptography*, Lecture Notes in Comput. Sci. 1746 (Springer, 1999) 191–200. 127

14. S. GALBRAITH, F. HESS and N. SMART, 'Extending the GHS Weil descent attack', *Advances in Cryptology – Eurocrypt 2002*, Lecture Notes in Comput. Sci. 2332 (Springer, 2002) 29–44. 140, 144, 148, 148

15. R. GALLANT, R. LAMBERT and S. VANSTONE, 'Improving the parallelized Pollard lambda search on anomalous binary curves', *Math. Comp.* 69 (2000) 1699–1705. 133, 142

16. P. GAUDRY, 'An algorithm for solving the discrete log problem on hyperelliptic curves', *Advances in Cryptology – Eurocrypt 2000*, Lecture Notes in Comput. Sci. 1807 (Springer, 2000) 19–34. 133

17. P. GAUDRY, F. HESS and N. SMART, 'Constructive and destructive facets of Weil descent on elliptic curves', *J. Cryptology* 15 (2002) 19–46. 127, 128, 130, 130, 130, 130, 131, 131, 131, 135, 142, 142

18. F. Hess, KASH program for performing the GHS attack, 2000. http://www.cs.bris.ac.uk/~nigel/weil_descent.html. 131, 146, 164, 165

19. Internet Engineering Task Force, 'The OAKLEY key determination protocol', IETF RFC 2412, November 1998; http://www.ietf.org/rfc/rfc2412. 139

20. M. Jacobson, A. Menezes and A. Stein, 'Solving elliptic curve discrete logarithm problems using Weil descent', *J. Ramanujan Math. Soc.* 16 (2001) 231–260. 134, 134, 146, 146, 146

21. A. Joux and R. Lercier, 'Improvements on the general number field sieve for discrete logarithms in finite fields. A comparison with the Gaussian integer method', *Math. Comp.*, to appear. 135

22. N. Koblitz, 'Hyperelliptic cryptosystems', *J. Cryptology* 1 (1989) 139–150. 129

23. A. Menezes and M. Qu, 'Analysis of the Weil descent attack of Gaudry, Hess and Smart', *Topics in Cryptology – CT-RSA 2001*, Lecture Notes in Comput. Sci. 2020 (Springer, 2001) 308–318. 128, 131, 131, 133

24. A. Menezes, T. Okamoto and S. Vanstone, 'Reducing elliptic curve logarithms to logarithms in a finite field', *IEEE Trans. Inform. Theory* 39 (1993) 1639–1646. 127

25. A. Menezes, P. van Oorschot and S. Vanstone, *Handbook of applied cryptography* (CRC Press, 1996). 164

26. P. van Oorschot and M. Wiener, 'Parallel collision search with cryptanalytic applications', *J. Cryptology* 12 (1999) 1–28. 127, 133

27. S. Paulus and H. Rück, 'Real and imaginary quadratic representations of hyperelliptic function fields', *Math. Comp.* 68 (1999) 1233–1241. 130

28. S. Pohlig and M. Hellman, 'An improved algorithm for computing logarithms over $GF(p)$ and its cryptographic significance', *IEEE Trans. Inform. Theory* 24 (1978) 106–110. 127

29. J. Pollard, 'Monte Carlo methods for index computation mod p', *Math. Comp.* 32 (1978) 918–924. 127, 133

30. T. Satoh, 'The canonical lift of an ordinary elliptic curve over a finite field and its point counting', *J. Ramanujan Math. Soc.* 15 (2000) 247–270. 140

31. N. Smart, 'How secure are elliptic curves over composite extension fields?', *Advances in Cryptology – Eurocrypt 2001*, Lecture Notes in Comput. Sci. 2045 (Springer, 2001).

32. E. Teske, 'Speeding up Pollard's rho method for computing discrete logarithms', *Algorithmic number theory*, Lecture Notes in Comput. Sci. 1423 (Springer, 1998) 541–554. 133

33. N. Thériault, 'Weil descent attack for Artin-Schreier curves', preprint, 2002. 131

34. M. Wiener and R. Zuccherato, 'Faster attacks on elliptic curve cryptosystems', *Selected areas in cryptography*, Lecture Notes in Comput. Sci. 1556 (Springer, 1999) 190–200. 133, 142

Markus Maurer

Alfred Menezes   ajmeneze@uwaterloo.ca

Edlyn Teske   eteske@uwaterloo.ca

Department of Combinatorics and Optimization

University of Waterloo, Canada