AN ELLIPTIC CURVE TRAPDOOR SYSTEM

EDLYN TESKE

ABSTRACT. We propose an elliptic curve trapdoor system which is of interest in key escrow applications. In this system, a pair (E_s, E_{pb}) of elliptic curves over $\mathbb{F}_{2^{161}}$ is constructed with the following properties: (i) the Gaudry-Hess-Smart Weil descent attack reduces the elliptic curve discrete logarithm problem (ECDLP) in $E_s(\mathbb{F}_{2^{161}})$ to a hyperelliptic curve DLP in the Jacobian of a curve of genus 7 or 8, which is computationally feasible, but by far not trivial; (ii) E_{pb} is isogenous to E_s; (iii) the best attack on the ECDLP in $E_{pb}(\mathbb{F}_{2^{161}})$ is the parallelized Pollard rho method.
The curve E_{pb} is used just as usual in elliptic curve cryptosystems. The curve $E_s$is submitted to a trusted authority for the purpose of key escrow. The crucial difference from other key escrow scenarios is that the trusted authority has to invest a considerable amount of computation to compromise a user's private key, which makes applications such as widespread wire-tapping impossible.

1. Introduction

For an elliptic curve E over a finite field $\mathbb{F}_{2^N}$, the Gaudry-Hess-Smart (GHS) Weil descent attack [GHS02b] gives (under certain technical assumptions) an explicit group homomorphism $\Phi : \langle P \rangle \longrightarrow J_C(\mathbb{F}_{2^l})$ into the Jacobian of a hyperelliptic curve C over $\mathbb{F}_{2^l}$. Here, $\langle P \rangle$ denotes the cyclic group of prime order r generated by a given point P on E, and l is such that $N = nl$ for some positive integer n. By these means, unless $P \in \ker(\Phi)$, the elliptic curve discrete logarithm problem (ECDLP): given P and $Q \in \langle P \rangle$, find $\lambda \in [0, r-1]$ such that $Q = \lambda P$, can be reduced to a hyperelliptic curve discrete logarithm problem (HCDLP) of the form: given $\Phi(P) \in J_C(\mathbb{F}_{2^l})$ and $\Phi(Q) \in \langle \Phi(P) \rangle$, find $\lambda \in [0, r-1]$ such that $\Phi(Q) = \lambda\Phi(P)$. The hyperelliptic curve C is of genus $g = 2^{m-1}$ or $g = 2^{m-1} - 1$, where $m = m(n)$ is the *magic number for E relative to n*, which can be easily determined from the defining equation of the elliptic curve.

Given that for hyperelliptic curves we have the Enge-Gaudry index calculus method [EG02] that is faster than $O((\#J_C(\mathbb{F}_{2^l}))^{1/2})$ if $g > 5$, and subexponential in the size of $J_C(\mathbb{F}_{2^l})$ as $g/N \to \infty$, the GHS Weil descent attack may result in a faster algorithm for the ECDLP than Pollard's rho algorithm [Pol78, vOW99]. Indeed, while it was shown by Menezes and Qu [MQ01] that the GHS attack fails for all elliptic curves over $\mathbb{F}_{2^N}$ if $N \in [100, 600]$ is *prime* and $N \neq 127$, Maurer, Menezes and Teske [MMT02] have identified all elliptic curves defined over characteristic 2 fields of *composite* extension degree $N \in [100, 600]$ for which the GHS attack reduces the total running time to solve the ECDLP (compared to applying Pollard rho). In particular, if $N = 161$, there exists a set I_4 of approximately 2^{94} isomorphism classes of elliptic curves over $\mathbb{F}_{2^{161}}$ with the following property: For any elliptic curve E in I_4, the GHS Weil descent attack produces a hyperelliptic curve C over $\mathbb{F}_{2^{23}}$ of genus 7 or 8. That is, $m(7) = 4$ for all $E \in I_4$. If $g = 7$, the resulting HCDLP can be solved in estimated 25,000 days on a 1GHz PIII workstation, and it takes estimated 200,000 days if $g = 8$. This compares to an estimated 200,000 days on a 450MHz PII machine to solve the 108-bit ECDLP of the Certicom challenge [Cer] in April 2000. Thus, any instance of the ECDLP for any curve in

Date: March 31, 2003.
1991 *Mathematics Subject Classification.* 94A60.
Key words and phrases. Elliptic curve cryptography, Weil descent, Isogenies, Trapdoor functions, Key escrow.

I_4 can be considered feasible, *but not trivial*. Here we assume that the curve is cryptographically interesting, meaning that (i) $\#E(\mathbb{F}_{2^N}) = rd$ where r is prime and $d \in \{2, 4\}$ 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 $\mathbb{F}^*_{2^{NJ}}$. (The second requirement, which is almost always fulfilled for a random curve, is to avoid the Weil pairing and Tate pairing attacks, while the first requirement implies that the Pohlig-Hellman combined with the parallelized Pollard rho attack takes about 2^{80} elliptic curve operations.)

While the magic number m for an elliptic curve $E/\mathbb{F}_{q^n}$ $(q = 2^l)$ relative to n is an invariant of the *isomorphism* class of an elliptic curve, it is in general not invariant under *isogenies* between elliptic curves. In particular, given a curve $E/\mathbb{F}_{2^{161}}$ in I_4 an elliptic curve E' randomly chosen from the isogeny class of E has magic number 7 with respect to $n = 7$ with an estimated probability $\approx 1 - 2^{-68}$ (cf. Section 3.1). For such a curve E', the GHS attack fails: it yields a hyperelliptic curve over $\mathbb{F}_{2^{23}}$ of genus 63 or 64, whose Jacobian has approximately 2^{1450} elements. Solving the HCDLP in this Jacobian with index-calculus methods is a task much more expensive than using the Pollard rho method in $E'(\mathbb{F}_{2^{161}})$.

In this paper, we use the set I_4 of elliptic curves over $\mathbb{F}_{2^{161}} = \mathbb{F}_{(2^{23})^7}$ with $m(7) = 4$ to design a trapdoor system. Using techniques from [MQ01], Trent generates a cryptographically interesting elliptic curve E_{s} over $\mathbb{F}_{2^{161}}$ with $m(7) = 4$. Then, using techniques from [GHS02a], Trent computes a curve E_{pb} isogenous to E_{s} with magic number 7, and an isogeny Ψ from E_{pb} to E_{s}. The curve E_{pb} is given to the user, Alice, while E_{s} and Ψ form the trapdoor, and Trent keeps them secret. E_{pb} is cryptographically interesting, and can be used, for example, to execute an elliptic curve based Diffie-Hellman key exchange protocol. Our trapdoor system has the following properties:

(1) Trent can solve any instance of an ECDLP on E_{pb}, but needs a non-trivial amount of computing power to do so.
(2) Any attacker not knowing E_{s} and the way E_{pb} was constructed cannot recover either information any faster than applying Pollard rho in $E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$.
(3) Finding another curve $E \in I_4$ (and thus as susceptible to the GHS attack as E_{s}) that is isogenous to $E_{\mathrm{pb}}/\mathbb{F}_{2^{161}}$ is equally infeasible.

Consequently, against an attacker who lacks the trapdoor information, E_{pb} provides the same per-bit-security as any other cryptographically interesting curve over $\mathbb{F}_{2^{161}}$ The first property crucially distinguishes our new system from traditional trapdoor systems such as RSA, where knowledge of the trapdoor yields a polynomial time algorithm to recover the secret key. This makes our trapdoor system attractive for key escrow applications where the key escrow agency (Trent) wants to be able to control encrypted communication, but the user's privacy should be somewhat protected in the sense that only a small number of keys can be recovered by Trent.

Having this key escrow application in mind, in this paper we prefer to present our trapdoor system in the following scenario: Alice generates a random curve $E_{\mathrm{s}} \in I_4$ herself, and a curve E_{pb} isogenous to E_{s}. She uses E_{pb} as her public curve, and submits E_{s} (and possibly information of how E_{pb} was obtained from E_{s}) to Trent.

For details on the GHS Weil descent attack we refer the interested reader to [GHS02b]. In the following, we just give those details of immediate interest for our exposition, which involves magic numbers, GHS attack data, and isogenies (Section 2). In Section 3 we do a little detour on how magic numbers behave under isogenies, and present an important assumption on how I_4 distributes over the isogeny classes of curves over $\mathbb{F}_{2^{161}}$. The set-up of our trapdoor system is given in Section 4, while its security is analyzed in Section 5, and its efficiency in Section 6. Finally, we discuss which finite fields other than $\mathbb{F}_{2^{161}}$ can possibly be used for similar trapdoor system constructions

(Section 7). In the Appendix, we give an instance of the trapdoor system, and a challenge to attack it.

For a set S we denote by $s \in_R S$ that s is chosen uniformly at random from S.

2. Magic Numbers, GHS Weil Descent and Isogenies

Throughout this paper, let $E : y^2 + xy = x^3 + ax^2 + b$ be a cryptographically interesting elliptic curve over $\mathbb{F}_{2^N}$, and let P be a point on E of large prime order r. We often specialize to the case $N = 161$. Other possible choices for N are discussed in Section 7.

2.1. Magic Numbers.

Let $N = 161 = 7 \cdot 23$ and $q = 2^{23}$, then we can write $\mathbb{F}_{2^{161}} = \mathbb{F}_{q^7}$. By [MQ01, Lemma 4], $\mathbb{F}_{2^{161}}$ can be decomposed into a direct sum of subspaces:

$$\mathbb{F}_{2^{161}} = W_0 \oplus W_1 \oplus W_2 \ ,$$

where

$$\begin{aligned} W_0 &= \{c : \sigma(c) + c = 0\} = \{c : c^{2^{23}} = c\} = \mathbb{F}_{2^{23}} \ , \\ W_1 &= \{c : \sigma^3(c) + \sigma^2(c) + c = 0\} = \{c : c^{2^{69}} + c^{2^{46}} + c = 0\} \ , \\ W_2 &= \{c : \sigma^3(c) + \sigma(c) + c = 0\} = \{c : c^{2^{69}} + c^{2^{23}} + c = 0\} \ , \end{aligned}$$

and $\sigma : \mathbb{F}_{2^{161}} \to \mathbb{F}_{2^{161}}$ is the Frobenius endomorphism defined by $\alpha \mapsto \alpha^q$. Then $|W_0| = 2^{23}$ and $|W_1| = |W_2| = 2^{69}$. An elliptic curve $E = E_{a,b}$ over $\mathbb{F}_{2^{161}}$ has magic number $m(7) = 1$ if and only if $b \in W_0 \setminus \{0\}$, and $m(7) = 4$ if and only if b is an element of

$$S := (W_0 \oplus (W_1 \setminus \{0\})) \cup (W_0 \oplus (W_2 \setminus \{0\})) \ ,$$

and $m(7) = 7$ otherwise. Note that we have $|S| = 2 \cdot 2^{23} \cdot (2^{69} - 1) \approx 2^{93}$. We let

$$I_4 = \{E_{a,b}/\mathbb{F}_{2^{161}} \ : \ a \in \{0,1\}, b \in S\} \ ,$$

the set of representatives of the isomorphism classes of elliptic curves over $\mathbb{F}_{2^{161}}$ with magic number $m(7) = 4$. Clearly, $|I_4| \approx 2^{94}$.

It is easy to compute bases (over $\mathbb{F}_2$) of the three subspaces W_0, W_1 and W_2, so that using the above representation for S we can quickly generate random curves $E_{a,b}$ ($a \in_R \{0,1\}$) over $\mathbb{F}_{2^{161}}$ with $m(7) = 4$. Moreover, this allows us to implement an exhaustive search through the set S.

2.2. GHS Weil Descent Attack Data.

Let $E \in I_4$ and cryptographically interesting. Then, any ECDLP in the large prime-order subgroup of order r takes expected $2^{79.8}$ or $2^{79.3}$, respectively, elliptic curve operations using the parallelized Pollard rho method (see Section 7). On the other hand, the GHS Weil descent attack maps any such ECDLP to a HCDLP in the Jacobian of a hyperelliptic curve C of genus $g = 7$ or 8. If $g = 7$, this HCDLP can be solved in expected 2^{34} hyperelliptic curve operations using the Enge-Gaudry index calculus algorithm [Gau00, EG02]. If $g = 8$, it takes expected 2^{37} operations in the Jacobian. With Stein's analysis of the Jacobian arithmetic [Ste01], this translates into at most $1.2 \cdot 2^{44}$ operations in $\mathbb{F}_{2^{23}}$ if $g = 7$, and at most $1.5 \cdot 2^{47}$ operations in $\mathbb{F}_{2^{23}}$ if $g = 8$. In either case, a factor base containing 2^{22} prime divisors of degree 1 is used, so that about 2^{44} bit operations in the final linear algebra step are required. Based on timings from [JMS01], we estimate that if $g = 7$, the computational effort for the entire computation corresponds to about 25,000 days on a 1GHz PIII workstation. However, only about 2^{70} values $b \in S$ result in a genus 7 curve, while the vast majority of b-values yields a genus 8 curve. In fact, we have the following theorem.

Theorem 2.1. *Let $E_{a,b}$ be an elliptic curve over $\mathbb{F}_{2^{161}}$ with $m(7) = 4$. Then the GHS Weil descent attack produces a hyperelliptic curve of genus 7 if and only if $b \in W_1 \setminus \{0\}$ or $b \in W_2 \setminus \{0\}$.*

Proof. By [Hes, Corollary 13], $g = 7$ if and only if $\mathrm{Tr}_{\mathbb{F}_{q^7}/\mathbb{F}_q}(b^{1/2}) = 0$, which is the case if and only if $\mathrm{Tr}_{\mathbb{F}_{q^7}/\mathbb{F}_q}(b) = 0$. Let

$$t(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \ .$$

Then $\mathrm{Tr}_{\mathbb{F}_{q^7}/\mathbb{F}_q}(b) = t(\sigma)(b)$. As in [MQ01], let $\mathrm{Ord}_b(x)$ denote the unique monic polynomial $f \in \mathbb{F}_2[x]$ of least degree such that $f(\sigma)(b) = 0$. Now we can write

$$t(x) = g(x)\mathrm{Ord}_b(x) + r(x) \ ,$$

where $g(x), r(x) \in \mathbb{F}_2[x]$ and $r(x) = 0$ or $\deg(r(x)) < \deg(\mathrm{Ord}_b(x))$. Then

$$\mathrm{Tr}_{\mathbb{F}_{q^7}/\mathbb{F}_q}(b) = g(\sigma)(b)\mathrm{Ord}_b(\sigma)(b) + r(\sigma)(b) \ .$$

Hence, $\mathrm{Tr}_{\mathbb{F}_{q^7}/\mathbb{F}_q}(b) = 0$ if and only if $\mathrm{Ord}_b(x) \,|\, t(x)$. Now, $m(7) = 4$ if and only if $\mathrm{Ord}_b(x) = (x+1)^{j_0}(x^3+x^2+1)^{j_1}(x^3+x+1)^{j_2}$ with $j_0, j_1, j_2 \in \{0,1\}$ and $j_1 + j_2 = 1$. Therefore, $\mathrm{Ord}_b(x) \,|\, t(x)$ for $b \in S$ if and only if $j_0 = 0$ and exactly one of $j_1, j_2 = 1$, which is the case if and only if $b \in (W_1 \setminus \{0\}) \cup (W_2 \setminus \{0\})$. $\square$

2.3. **Isogenies, and Class Groups.** For background material, the reader may wish to consult [Koh96] and [Gal99] on isogenies, and [Coh93, Chapt. 5] and [Cox89] on class groups.

An isogeny between two elliptic curves E and E' over a field K is a non-constant morphism $\Psi : E \to E'$ such that $\Psi(\mathcal{O}_E) = \mathcal{O}_{E'}$, where $\mathcal{O}_E$ and $\mathcal{O}_{E'}$ denote the zero elements of the corresponding elliptic curve groups. E and E' are called isogenous over K if Ψ is defined over K; we write $E \sim E'$. In the case of a finite field, $E \sim E'$ if and only if $\#E(K) = \#E'(K)$. The equivalence classes with respect to isogeny are called isogeny classes.

Let E be an elliptic curve over $\mathbb{F}_{2^N}$ and $t = 2^N + 1 - \#E(\mathbb{F}_{2^N})$ its trace and $\Delta = t^2 - 4 \cdot 2^N$ its discriminant. Then the endomorphism ring $\mathrm{End}(E)$ can be viewed as an order in the maximal order $\mathcal{O}_\Delta$ of the quadratic number field $\mathbb{Q}(\sqrt{\Delta})$. In fact,

$$\mathbb{Z}[\pi] \subseteq \mathrm{End}(E) \subseteq \mathcal{O}_\Delta \ ,$$

where $\pi : E(\overline{\mathbb{F}_{2^N}}) \to E(\overline{\mathbb{F}_{2^N}})$ is the 2^N-th power Frobenius map on E, whose characteristic polynomial is $T^2 - tT + 2^N$.

Theorem 2.2. *If $E/\mathbb{F}_{2^N}$ is an elliptic curve with $\mathrm{End}(E) \cong \mathcal{O}_\Delta$, then there is a bijection*

$$\mathrm{Cl}_\Delta \longleftrightarrow \mathrm{Ell}(\mathcal{O}_\Delta) \ ,$$

where Cl_Δ denotes the class group of $\mathcal{O}_\Delta$, and $\mathrm{Ell}(\mathcal{O}_\Delta)$ denotes the isomorphism classes of curves isogenous to E whose endomorphism ring is isomorphic to $\mathcal{O}_\Delta$.

This is proved in [Sil94, Proposition II.1.2] for elliptic curves over the complex numbers, and via Deuring's lifting extends to finite fields (cf. [Lan87]).

In the following, we conveniently identify an isomorphism class of a curve over $\mathbb{F}_{2^{161}}$ with its representative $E_{a,b}$ where $a \in \{0,1\}$ and $b \in \mathbb{F}_{2^{161}} \setminus \{0\}$, and we identify an ideal class in Cl_Δ with its unique reduced representative. Sometimes, however, we will find it appropriate to use $\mathrm{Red}(\mathfrak{a})$ to indicate the reduced ideal equivalent to the $\mathcal{O}_\Delta$-ideal $\mathfrak{a}$. By h_Δ we denote the class number, $\#\mathrm{Cl}_\Delta$.

In our trapdoor system we restrict ourselves to elliptic curves over $\mathbb{F}_{2^{161}}$ with squarefree discriminant Δ. For such a curve E, $\mathbb{Z}[\pi] \cong \mathcal{O}_\Delta$ and thus $\mathrm{End}(E') \cong \mathcal{O}_\Delta$ for any curve $E' \sim E$. The set $\mathrm{Ell}(\mathcal{O}_\Delta)$ includes *all* isomorphism classes of curves in the isogeny class of E, and all isogenies are "horizontal" in the sense of [Koh96]. Since Δ is fundamental, we have that, on average, h_Δ behaves as $c\sqrt{|\Delta|}$, where $c \approx 0.46$ and the average is taken over all fundamental negative discriminants up to Δ. Also, $h_\Delta < \sqrt{|\Delta|}\ln|\Delta|/\pi$, and, under the Extended Riemann Hypothesis, $h_\Delta > (1+o(1))\sqrt{|\Delta|}/(c\ln\ln|\Delta|)$ where $c \approx 6.8$ [Lit28]. Thus, the isogeny class of an elliptic curve of a k-bit squarefree discriminant Δ contains *roughly* $2^{k/2}$ isomorphism classes of elliptic curves over the same field.

Now let $E_{a,b}$ be an elliptic curve over $\mathbb{F}_{2^N}$, let $j(E) = b^{-1}$ denote its j-invariant, and let l be a prime that splits in $\mathcal{O}_\Delta$ (i.e., $\left(\frac{\Delta}{l}\right) = 1$). Then the modular polynomial $\Phi_l(j(E), X)$ has two roots j_1 and j_2 in $\mathbb{F}_{2^N}$, which define two elliptic curves E_{a,b_1} and E_{a,b_2} isogenous to E, where $b_i = j_i^{-1}$. These roots can be computed by a probabilistic algorithm using $O(l^2N)$ operations in $\mathbb{F}_{2^N}$. In the one-to-one correspondence between Cl_Δ and $\mathrm{Ell}(\mathcal{O}_\Delta)$, the two isogenies $\Psi_1 : E \to E_{a,b_1}$ and $\Psi_2 : E \to E_{a,b_2}$ correspond to the multiplication of a fixed ideal, for example $\mathcal{O}_\Delta$, by the two prime ideals $\mathfrak{l}_1$ and $\mathfrak{l}_2$ lying over l. In the case of a ramified prime l (i.e. $l \mid \Delta$), $\Phi_l(j(E), X)$ has just one root, yielding one isogenous curve E', and the respective isogeny corresponds to multiplication by an ideal (class) of order two. For our purpose, we leave these ambiguous ideal classes aside and restrict ourselves to split primes (which are sufficient to generate the class group).

We have an efficient method to move around in the isogeny class of an elliptic curve $E = E_{a,b}$ of squarefree discriminant Δ in a pseudo-random way:

Algorithm 2.1. *A pseudo-random walk in the isogeny class.*
Input: $E = E_{a,b}$ over $\mathbb{F}_{2^N}$, a positive integer K, repository of modular polynomials $\Phi_l(X, Y)$, $3 \le l < 2000$.
Output: A chain of length K of isogenous curves.

(1) Let $E_1 = E$ and $b_1 = b$.
(2) Choose $L \le 2000$.
(3) Compute $\mathcal{L} := \{3 \le l \le L, l \text{ prime}, \left(\frac{\Delta}{l}\right) = 1\}$.
(4) For $i = 2$ to K do the following:
  (a) Choose $l \in_R \mathcal{L}$.
  (b) For $j := b_{i-1}^{-1}$, compute the two roots in $\mathbb{F}_{2^N}$ of $\Phi_l(j, X)$, and randomly select one of them, say j'.
  (c) Let $b_i := (j')^{-1}$ and $E_i := E_{a,b'}$,
(5) Return $E_1, E_2, \ldots, E_K$.

Remark 2.1. We cannot readily apply the results from [Tes01] stating that in a group of prime order, if 16 or more pairwise distinct "multipliers" (in our application: 16 or more primes l) are used, a random walk in $\mathrm{Ell}(\mathcal{O}_\Delta)$ can be efficiently simulated. In our application, the corresponding multipliers (via the correspondence between isogenies and ideal classes) are ideals of small norm l rather than randomly chosen elements of Cl_Δ. Moreover, the groups in which we work are not necessarily of prime order, and sometimes they are not even cyclic. Nevertheless, extensive experiments suggest that $L = 300$ (which yields, on average, 30 distinct pairs of prime ideals lying over the split primes $l \le L$) is indeed sufficient for 160-bit discriminants to pseudo-randomly generate a chain $(E_1, \ldots, E_K) \subset \mathrm{Ell}(\mathcal{O}_\Delta)$.

3. Magic numbers and isogenies

The magic number of E with respect to a fixed $n|N$ is invariant under the power-2 Frobenius map – this follows directly from the definition of the magic number in [GHS02b].

Proposition 3.1. *The isomorphism classes of an elliptic curve E over $\mathbb{F}_{2^N}$ that are obtained by repeatedly applying the 2-isogeny stemming from $\Phi_2(X,Y)$ are exactly those (up to ordering) obtained by repeatedly applying the 2-power Frobenius to E.*

Proof. We compute two chains of curves isogenous to $E_{a,b}$. For the first chain, let $J = j(E)$, and let j be a root of the modular polynomial (modulo 2)

$$\Phi_2(J,X) = X^3 + X^2J^2 + XJ + J^3 \ .$$

Then $E' := E_{a,j^{-1}} \sim E$. The next curve is obtained from a root of the polynomial $\Phi_2(j,X)$, and so forth. For the second chain, repeated application of the power-2 Frobenius to E produces elliptic curves with j-invariants $J, J^2, J^{2^2}, \dots, J^{2^{k-1}}$, for some $k|N$. Noting that for any $j \in \mathbb{F}_{2^N}$ with the property that $j^2 = J$ we have $\Phi(J,j) = 0$ gives the desired result. □

Moreover, isogenies stemming from the multiplication-by-l map yield just the same curves that are obtained by repeated applications of the power-2 Frobenius map. But also for l-isogenies associated with $\Phi_l(J,X)$ for random odd primes l we may find strong patterns in the magic numbers, depending on the field $\mathbb{F}_{2^N} = \mathbb{F}_{(2^l)^n}$. This is detailed in the following theorem.

Theorem 3.1. *Let $N = nl$. Let $f_0,\dots,f_s$ be irreducible polynomials over $\mathbb{F}_2$ and $j_0,\dots,j_s \in \mathbb{N}$ such that*

$$x^n - 1 = f_0^{j_0} f_1^{j_1} \cdots f_s^{j_s} \ .$$

Let $q = 2^l$ and let $E : y^2 = x^3 + ax^2 + b$ be an elliptic curve over $\mathbb{F}_{q^n}$ with magic number $m = m(n)$. Let

$$f = f_0^{i_0} f_1^{i_1} \cdots f_s^{i_s} \ , \qquad 0 \le i_v \le j_v, \ v = 1, \dots s \ ,$$

be the unique polynomial of least degree such that $f(\sigma)(b) = 0$, where σ is the q-th power Frobenius. Let U_f be the set of roots of f in its splitting field. Let $\overline{U_f}$ be the subgroup of n-th roots of unity generated by U_f, and let $\overline{f} \,|\, (x^n - 1)$ be the annihilating polynomial of $\overline{U_f}$. Let $B \subset \mathbb{F}_{2^N}$ be the set of roots of $\overline{f}(\sigma)$. Then, for any elliptic curve $E_{a,b'}$ generated by Algorithm 2.1 we have $b' \in B$. The corresponding magic number, m', satisfies $m' \le \deg(\overline{f})$. In particular, if $U_f \cup \{1\} = \overline{U_f}$, then $m' \le m$.

Proof. We first note that in the language of [MQ01], b is of type $(i_0, i_1, \dots, i_s)$ and $m = \deg(f)$ if $i_0 > 0$ and $m = \deg(f) + 1$ if $i_0 = 0$. Now, the group $\overline{U_f}$ is the group of k-th roots of unity, for some $k \,|\, n$, and $\overline{f} = x^k - 1$. Thus, for $b \in B$ we have $\sigma^k(b) - b = 0$, or $b^{q^k} = b$, which implies $B \subset \mathbb{F}_{q^k}$. Conversely, $\mathbb{F}_{q^k} \subset B$, so that $B = \mathbb{F}_{q^k}$. Now, also $j := j(E_{a,b}) \in \mathbb{F}_{q^k}$ for any $b \in B$. Therefore, for any modular polynomial $\Phi_l(X,Y)$, the two roots j_1, j_2 of $\Phi_l(j,X)$ that are in $\mathbb{F}_{q^n}$ are indeed in $\mathbb{F}_{q^k}$. Consequently, $b_1 := j_1^{-1}$ and $b_2 := j_2^{-1}$ are also elements of $B = \mathbb{F}_{q^k}$. For the magic numbers m_1 and m_2 of the corresponding isogenous curves E_{a,b_1} and E_{a,b_2}, this implies $m_i \le k$.
Finally, if $\overline{U_f} = U_f \cup \{1\}$, then $f(x) = x^k - 1$ or $f(x) = (x^k - 1)/(x - 1)$ for some $k \,|\, n$, and $m = k$ by [MQ01, Theorem 6], and thus $m_i \le m$. □

Remark 3.1. In the notation of the above theorem, by [MQ01, Theorem 5] there exist $\prod_{v=0, j_v \ne 0}^{s} (q^{i_v d_v} - q^{(i_v - 1)d_v})$ elements $b \in \mathbb{F}_{2^N}$ for which $f(\sigma)(b) = 0$; here, $d_v = \deg(f_v)$. From this it is immediate that if $U_f \cup \{1\} = \overline{U_f}$, then the most likely case is $m' = m$. We thus can say that the magic number m is "almost invariant" under isogenies. Of course, this includes the trivial situation that $k = n$. Table 3 shows some parameters for non-trivial applications of Theorem 3.1.

n	m	$f(x)$	m'
$3u$	3	$(x+1)^j(x^2+x+1)$	$1,3$
$5u$	5	$(x+1)^j(x^4+x^3+x^2+x+1)$	$1,5$
$9u$	9	$(x+1)^j(x^2+x+1)(x^6+x^3+1)$	$1,3,7,9$
$33u$	11	$(x^{11}-1)/(x+1)^j$	$1,11$
$65u$	13	$(x^{13}-1)/(x+1)^j$	$1,13$
$129u$	43	$(x^{43}-1)/(x+1)^j$	$1,43$

TABLE 1. Non-trivial instances $(N,n,m) = (nw,n,m)$ for Theorem 3.1 ($j \in \{0,1\}$, and $u,w \in \mathbb{N}$).

Remark 3.2. It is easy to see that for all non-trivial instances of Theorem 3.1 where the GHS Weil descent attack applies, the elliptic curve $E_{a,b}$ is necessarily defined over a proper subfield $\mathbb{F}_{q^k}$ of $\mathbb{F}_{q^n}$, and thus not cryptographically interesting, with the exception of Koblitz curves where $q=2$ and $k=1$. However, Koblitz curves (just as curves defined over other small subfields $\mathbb{F}_{q^k}$) never have a squarefree discriminant.

3.1. **The case $\mathbb{F}_{2^{161}}$.** Theorem 3.1 does not yield any non-trivial instances for $(N,n) = (161,7)$: If $m=4$, then $\overline{U_f}$ is the set of seventh roots of unity and $B = \mathbb{F}_{2^{161}}$. On the contrary, we make the following heuristic assumption:

Assumption A. *The set I_4 of (isomorphism classes of) elliptic curves over $\mathbb{F}_{2^{161}}$ with magic number $m(7)=4$ is randomly distributed over the isogeny classes in the following sense: An elliptic curve over $\mathbb{F}_{2^{161}}$ that is randomly chosen from a fixed isogeny class has magic number $m(7)=4$ with probability $|I_4|/2^{162}$.*

Thus, under Assumption A a random curve over $\mathbb{F}_{2^{161}}$ in a given isogeny class has magic number 4 with probability $\approx 2^{-68}$, and magic number 7 with probability $\approx 1-2^{-68}$. Moreover, in any given isogeny class of squarefree discriminant Δ, we expect to find $h_\Delta/2^{68}$ isomorphism classes of curves with magic number 4.

Remark 3.3. Assumption A is *not* true for small values of N of the form $N=7l$. This is due to the fact that for any given curve $E/\mathbb{F}_{2^N}$ of magic number $m(7)=4$ there exist up to N curves with magic number 4 that stem from repeated applications of the power-2 Frobenius. For example, if $N=21$ and E has magic number $m(7)=4$, there exist (up to) 20 curves isogenous to E with magic number 4, which prevents I_4 from equally distributing over all isogeny classes. In fact, experimentally we found that while $|I_4| \approx 2^{14}$, only $2^{9.33\cdots}$ out of the $2^{11.5}$ isogeny classes over $\mathbb{F}_{2^{21}}$ contain curves with $m(7)=4$ – which roughly matches what we expect when taking the effect of the power-2 Frobenius into account ($2^{14}/21 = 2^{9.60\cdots}$). But as N increases, this distortion rapidly becomes insignificant, as has been verified in extensive experiments.

4. A Trapdoor System for Elliptic Curves over $\mathbb{F}_{2^{161}}$

4.1. **Constructing the secret trapdoor curve.** The trusted authority, or the user herself, does the following steps to construct a cryptographically interesting trapdoor curve:

Algorithm 4.1. *Construction of the secret trapdoor curve.*
Input: Bases of W_0, W_1, W_2.
Output: Cryptographically interesting curve $E/\mathbb{F}_{2^{161}}$ with $m(7)=4$.

(1) Choose $b \in_R S$.
(2) Check if $E_{0,b}$ or its twist $E_{1,b}$ is cryptographically interesting and denote the resulting curve by E. Otherwise, go back to Step (1).
(3) Let Δ be the discriminant of E, and check the following:
  (a) Δ is squarefree,
  (b) $|\Delta| \geq 2^{157}$,
  (c) $2^{76} \leq h_\Delta < 2^{83}$,
  (d) The odd, cyclic part of Cl_Δ has cardinality $\geq 2^{68}$.

  If so, return E. Otherwise, go back to Step (1).

There are 2^{93} pairs $(E_{0,b}, E_{1,b})$ to choose from in Step (1) of Algorithm 4.1. Their group orders are of the form $2m$ and $4m'$, where m is a 161-bit number and m' is a 160-bit number. Assuming $2m$ and $4m'$ are randomly distributed over the even integers and the integers $\equiv 0 \mod 4$ in the Hasse-interval, respectively, we know by the Prime Number Theorem that m or m' is prime with probability about $1/\ln 2^{160}$ so that there should exist some 2^{87} cryptographically interesting elliptic curves in I_4. Now, we find experimentally that 90 to 95 out of any 100 random elliptic curves over $\mathbb{F}_{2^{161}}$ in I_4 have a squarefree discriminant. A curve passes Step (3b) if $\#E(\mathbb{F}_{2^{161}})$ is not too close to the edges of the Hasse interval. More precisely, $|\Delta| \geq 2^{157}$ whenever $\#E(\mathbb{F}_{2^{161}})$ does not lie in the outermost 0.5%-ranges of the Hasse interval, which is true for the vast majority of curves. Given the reasoning in Section 2.3, a curve that passes (3b) is highly likely to pass the much more expensive to verify next step. The lower bound in Step (3c) ensures that the (up to) 160 (isomorphism classes of) curves isogenous to E with $m(7) = 4$ that stem from the power-2 Frobenius do not lead to a violation of Assumption A (note: $2^{76}/161 > 2^{68}$), while the upper bound is to make finding another isogenous curve I_4 difficult enough (cf. Section 5.3). Criterion (3d) guarantees that the problem of reconstructing the trapdoor curve from the public curve is hard enough (cf. Section 5.2). Note that the vast majority of curves over $\mathbb{F}_{2^{161}}$ have 162- or 163-bit discriminants, and the vast majority of such class groups have cardinality $> 2^{80}$.

Experimentally, we found that out of 3000 randomly chosen pairs of elliptic curves in I_4, 58, or 1.93%, have order or twisted order twice or four times a prime, 2782 (92.73%) have a squarefree discriminant, 54 satisfy both criteria, 2998 have $|\Delta| \geq 2^{157}$ while 2999 curves have $2^{76} \leq h_\Delta < 2^{83}$. In 2987 out of 3000 cases (99.57%) we find that the odd cyclic part of Cl_Δ has cardinality $\geq 2^{68}$. Altogether, 54 out of 3000 curves (1.8%) passed all criteria. Extrapolating, this translates into expected $2^{87.2}$ suitable trapdoor curves, so there is plenty to choose from. Steps (1) and (2) are executed expected 52 times, while Step (3) most likely has to be executed just once.

4.2. **Constructing public curves.** We next need to construct a curve E_{pb} isogenous to the trapdoor curve E. Apart from the group order, E_{pb} must not leak information about E in the sense that given E_{pb}, it should not be any easier to recover E than to find any other curve in I_4 isogenous to E_{pb}. While we have fast exponentiation methods to efficiently generate a random element in Cl_Δ from a set of generators, there is no such method known to us in $\mathrm{Ell}(\mathcal{O}_\Delta)$. We thus resort to a variant of Algorithm 2.1. Given a prime l with $\left(\frac{\Delta}{l}\right) = 1$, let $\mathfrak{l}(l), \mathfrak{l}'(l) \in \mathcal{O}_\Delta$ denote the two prime ideals lying over l. For a positive integer L let

$$\mathcal{P}(\Delta, L) = \{(\mathrm{Red}(\mathfrak{l}(l)), \mathrm{Red}(\mathfrak{l}'(l))) \ : \ 3 \leq l \leq L, l \text{ prime and } \left(\frac{\Delta}{l}\right) = 1\} \ .$$

Let $M := M(\Delta, L)$ denote the number of pairwise distinct pairs in $\mathcal{P}(\Delta, L)$, and let $\mathcal{L} = \{l_1, \ldots, l_M\}$ denote the corresponding primes.

Algorithm 4.2. *Algorithm to construct a public curve.*
Input: Cryptographically interesting curve $E_{a,b} \in I_4$, parameter L and B, repository of modular polynomials $\Phi_l(X,Y)$, $3 \le l \le L$.
Output: $E_{\mathrm{pb}}/\mathbb{F}_{2^{161}}$, isogenous to $E_{a,b}$.

(1) Determine $M = M(\Delta, L)$ and $\mathcal{L} = \{l_1, \ldots, l_M\}$ as defined above.
(2) Let $j' := j_- := b^{-1}$.
(3) For $i = 1, \ldots, M$ do the following:
   (a) Select $n_i \in_R \{0, 1, \ldots, B\}$.
   (b) *(Construct a chain of* n_i l*-isogenous curves.)*
      For $k = 1, \ldots, n_i$ do the following:
         (i) Compute the two roots j_1 and j_2 in $\mathbb{F}_{2^{161}}$ of $\Phi_{l_i}(j', X)$.
         (ii) If $j_1 \ne j_-$ then let $j_- = j'$ and $j' = j_1$,
            otherwise let $j_- = j'$ and $j' = j_2$.
(4) Let $b' = (j')^{-1}$ and return $E_{\mathrm{pb}} = E_{a,b'}$.

In Section 5.2 we will show that suitable choices for L and B are $(L, B) = (300, 11)$ or $(L, B) = (500, 3)$. Then $MB \approx 165$ for the first choice, and $MB \approx 70$ for the second choice, which is how often the for-loop (3b) is executed.

4.3. **Solving the ECDLP using the trapdoor curve.** We now discuss the computational effort for the key escrow agency (Trent) to recover a user's secret key, i.e., to solve an ECDLP on a user's public curve E_{pb} given the trapdoor curve $E_{\mathrm{s}} \in I_4$.

If, along with E_{s} as part of the trapdoor information, Alice has also submitted the sequence of j-invariants encountered while computing the public curve (j' in Step (3b,ii) of Algorithm 4.2), then Trent can compute the explicit chain of isogenies in time $O(L)$ using Vélu's formulae [Vél71]. This enables him to efficiently map any given ECDLP in $E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$ to an ECDLP on $E_{\mathrm{s}} \in I_4$, for which the GHS attack data given in Section 2.2 apply.

Should Trent know only the public and secret elliptic curves over $\mathbb{F}_{2^{161}}$, one needs to first construct a chain of isogenies of small degrees linking E_{pb} and E_{s}. This can be done using ideas of [GHS02a]: Starting from E_{pb} and E_{s}, two pseudo-random walks in the isogeny class of $E_{\mathrm{pb}}, E_{\mathrm{s}}$ are computed (similar as in Algorithm 2.1, but this time the walks have to be deterministic), where one keeps track of all l-values and j-variants encountered on the way. A distinguished point method [vOW99] is used to detect a collision between these two walks, which is expected to occur after $\sqrt{\pi h_\Delta}$ steps in the isogeny class.[1] This computation can be efficiently parallelized to run on k machines where one works with $k/2$ walks of both kinds.

5. Security Analysis

While our system is designed such that the ECDLP in $E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$ can be solved by the trusted party (such as the key escrow agency), this feature must not diminish the security against any outside attacker. The purpose of this section is to show that there is no faster method to solve the ECDLP in $E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$ than running a parallelized Pollard rho attack in its subgroup of large prime order. First note that E_{pb} is cryptographically interesting. Moreover, there is only one other possibility

[1] The expected number of steps is by a factor of $\sqrt{2}$ larger than usually in birthday paradox applications. This is because only a collision *between the two walks* – in the parallelized version: between a walk starting from E_{pb} and one starting from E_{s} – yields the desired result, while a collision *within one walk* – in the parallelized version: among walks originating at the same curve – is useless.

to do a GHS Weil descent, namely to map the ECDLP into the Jacobian of a hyperelliptic curve over $\mathbb{F}_{2^7}$. But it can readily be seen from [MQ01] that this results in curves of genus 1, 2047 or 2048, so that the Jacobians are either too small to yield any information on the ECDLP, or far too large (of size $\approx 2^{14329}$) to allow for an algorithm faster than Pollard rho. Thus, the only other possible attack is to find a curve $\overline{E} \in I_4$ isogenous to E_{pb} along with an isogeny $\Psi : E_{\mathrm{pb}} \to \overline{E}$, and to solve the corresponding ECDLP in $\overline{E}(\mathbb{F}_{2^{161}})$ via the GHS attack. We will argue that the following problem cannot be solved in time faster than 2^{80} elliptic curve operations.

Problem P: *Given $E_{\mathrm{pb}}/\mathbb{F}_{2^{161}}$ with $m(7) = 7$, find $\overline{E} \sim E_{\mathrm{pb}}$ with $m(7) = 4$.*

There are three possible approaches to solve this problem: (i) Search the isogeny class of E_{pb} for a curve $\overline{E} \in I_4$; (ii) Try to retrieve the trapdoor curve E knowing that E_{pb} was constructed via Algorithm 4.2; and (iii) Search the set I_4 for a curve $\overline{E}$ with $\#\overline{E}(\mathbb{F}_{2^{161}}) = \#E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$.

We first consider the cost for moving around in the isogeny class of E_{pb}. That is, we estimate the computational cost of stepping from one curve to the next (Step (4) of Algorithm 2.1, Step (3b) of Algorithm 4.2). The dominating cost is that for computing the roots in $\mathbb{F}_{2^{161}}$ of $\Phi_l(j, X)$ for a given j-invariant and a given prime $l \in \mathcal{L}$, which is $O(l^2 \cdot 161)$ operations in $\mathbb{F}_{2^{161}}$. Compared with the cost of an elliptic curve operation in E_{pb} (doubling or adding of points using projective coordinates), which is bounded below by 10 operations in $\mathbb{F}_{2^{161}}$ [IEE00], this means that one step in the isogeny class of E_{pb} using Φ_l is at least by a factor of $16 \cdot l^2$ more expensive than one elliptic curve operation.

5.1. **Searching the isogeny class of E_{pb} for a curve in I_4.** Using Algorithm 2.1, the attacker can perform a pseudo-random walk in the isogeny class of E_{pb}. Each elliptic curve encountered this way is checked for membership in I_4 by computing its magic number m with respect to $n = 7$. Under Assumption A, expected 2^{68} steps in the isogeny class have to be executed until an appropriate curve is found. This takes much longer than running a Pollard rho attack in $E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$: Each step in the isogeny class costs at least as much as $16l^2$ elliptic curve operations; here using all split primes l up to $L = 300$ is appropriate to properly simulate a random walk; working with only 8 pairwise distinct (pairs of) prime ideals of smallest norm l (l split) does not properly simulate a random walk and still would require, on average, to work with l-values up to 80. So we safely may assume that the average step of Algorithm 2.1 costs at least the equivalent of $16 \cdot 30^2$ elliptic curve operations. Now, $2^{68} \cdot 16 \cdot 30^2 > 2^{80}$.

5.2. **Reconstructing the trapdoor curve from the public curve.** By the correspondence between $\mathrm{Ell}(\mathcal{O}_\Delta)$ and Cl_Δ, the isogeny Ψ that maps the trapdoor curve E_{s} to the public curve E_{pb} can be represented by the ideal class of

$$\mathfrak{b} := \prod_{i=1}^{M} \mathfrak{l}_i^{n_i} ,$$

where $\mathfrak{l}_i$ is one of $\mathfrak{l}(l_i)$, $\mathfrak{l}'(l_i)$ and $n_i \in [0, B]$. If an attacker could find integers n_i' such that $\prod_{i=1}^{M} \mathfrak{l}_i^{n_i'} = \mathfrak{b}$, this would allow her (using a variant of Algorithm 4.2) to construct a chain of $\sum_{i=1}^{M} n_i'$ isogenies of small degree l_i that maps E_{pb} to E_{s}. The task would be feasible (using index-calculus techniques in Cl_Δ, cf. [GHS02a]) if $\mathfrak{b}$ was known; which it is not. Thus, all the attacker can do is to check for candidate tuples $(n_1', \ldots, n_M')$ if the resulting isogeny yields a curve in I_4. We estimate the number of candidate tuples that have to be tried in order to find E_{s} with non-negligible probability. By construction of the trapdoor curve, Cl_Δ has an odd cyclic part of cardinality $h_{\Delta,oc} \geq 2^{68}$. Having excluded the ramified primes $\leq L$, we expect that the large majority of the $\mathfrak{l}_i$, $(i = 1, \ldots, M)$ have an element order of order of magnitude 2^{68}. Now let $\{\mathfrak{g}_1, \ldots, \mathfrak{g}_d\}$ be a set of generators of Cl_Δ such that $\operatorname{ord}\mathfrak{g}_1 \,|\, \operatorname{ord}\mathfrak{g}_2 \,|\, \cdots \,|\, \operatorname{ord}\mathfrak{g}_d$. Note that $\operatorname{ord}\mathfrak{g}_d \geq 2^{68}$. For each $i = 1, \ldots, M$, let $0 \leq k_{ij} < \operatorname{ord}\mathfrak{g}_j$ such that $\mathfrak{l}_i = \prod_{j=1}^{d} \mathfrak{g}_j{}^{k_{ij}}$. Then

$$\mathfrak{b} = \prod_{j=1}^{d} \mathfrak{g}_j^{\sum_{i=1}^{M} k_{ij} n_i} \; .$$

An attacker now has to find n_i' such that for $s_j := \sum_{i=1}^{M} k_{ij} n_i' \mod (\operatorname{ord}\mathfrak{g}_j)$, $\mathfrak{b} = \prod_{j=1}^{d} \mathfrak{g}_j^{s_j}$. Here she may want to exploit the knowledge that a solution exists with $0 \leq n_i' \leq B$. So consider the mapping

$$[0, B]^M \ni (n_1, \ldots, n_M) \mapsto (s_1, \ldots, s_d) \; , \quad s_j = \sum_{i=1}^{M} k_{ij} n_i \mod (\operatorname{ord}\mathfrak{g}_i) \; .$$

The cardinality of the image of this mapping is bounded below by the number of possible choices for s_d, which is of the order of magnitude $\max\{(B+1)^M, \operatorname{ord}\mathfrak{g}_d\}$.

For sample values of L, in Table 2 we give the average (M_{ave}), minimum (M_{min}) and maximum (M_{max}) values $M(\Delta, L)$ (cf. Section 4.2); averages etc. are taken over 500 negative discriminants of the form $\Delta = t^2 - 4 \cdot 2^{161}$ with t a randomly chosen odd integer in the Hasse interval. In the columns for $B(\cdot)$ we indicate the least integer values B such that $(B+1)^M \geq 2^{68}$, for M_{ave}, M_{min}, and M_{max}.

L	M_{ave}	$B(M_{\mathrm{ave}})$	M_{min}	$B(M_{\mathrm{min}})$	M_{max}	$B(M_{\mathrm{max}})$
300	30.0	4	19	11	41	3
500	46.4	2	34	3	60	2
700	61.4	2	44	2	77	1
1000	82.5	1	65	2	108	1
2000	149.6	1	122	1	175	1

TABLE 2. Least values of B such that $(B+1)^M > 2^{68}$.

These data show that $L = 500$ and $B = 3$, or $L = 300$ and $B = 11$ are suitable choices for Algorithm 4.2 to effectively hide the trapdoor curve: An attacker is expected to have to try about $2^{68}/2$ candidates to retrieve E_{s}, where the cost of each trial is at least the cost of $16l^2$ elliptic curve operations, where $l = \max\{l_i \; : n_i' \neq 0\}$. Thus, this approach by far exceeds the cost of running a Pollard rho attack in $E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$.

5.3. **Searching I_4 for a curve isogenous to E_{pb}.** The only method currently known to find an elliptic curve over $\mathbb{F}_{2^{161}}$ with $m(7) = 4$ that has a given number of points is exhaustive search through I_4: loop through all elements $b \in S$ (cf. Section 2.1), count the number of points of $E_{0,b}$ over $\mathbb{F}_{2^{161}}$ and check if $E_{0,b}(\mathbb{F}_{2^{161}})$ or its twist has the desired cardinality.

Under Assumption A, there exist $h_\Delta/2^{68}$ elliptic curves in I_4 isogenous to E_{pb}. To find one such curve, the expected number of $b \in S$ that have to be considered is $2^{161}/h_\Delta$. With $h_\Delta < 2^{83}$, this number is bounded below by 2^{78}. Given that the cost of point counting over $\mathbb{F}_{2^{161}}$ [Gau02] still exceeds the cost of 4 elliptic curve operations in $\mathbb{F}_{2^{161}}$, finding a curve in I_4 isogenous to E_{pb} is at least as costly as performing 2^{80} elliptic curve operations.

6. Efficiency

Elliptic curve cryptosystems using curves over $\mathbb{F}_{2^{161}}$ that were constructed as in Section 4 are just as efficient as cryptosystems using a randomly chosen curve over the same field.

The only drawback of our system is that its set-up is somewhat more time-consuming than just randomly choosing a cryptographically interesting curve over $\mathbb{F}_{2^{161}}$. The dominant additional step in the construction of the trapdoor curve is the computation of $\#\mathrm{Cl}_\Delta$ for a 163-bit discriminant Δ. This computation, which usually has to be executed just once, takes a few minutes on a Sun Ultra 60 Workstation using Jacobson's subexponential-time algorithm [Jac99] (implemented in LiDIA). It is, however, infeasible on small devices. Secondly, the construction of the public curve from the trapdoor curve requires the computation of the roots over $\mathbb{F}_{2^{161}}$ of about 70 polynomials $\Phi_l(j, X)$ when $L = 500$, or about 165 polynomials $\Phi_l(j, X)$ when $L = 300$, each of which requires $O(161l^2)$ operations in $\mathbb{F}_{2^{161}}$. Using Magma on a Sun Ultra 60 Workstation, for each $\Phi_l(j, X)$ this takes between a few seconds and a couple of minutes for $3 \leq l \leq 500$. When $L = 300$, Algorithm 4.2 can be sped up by choosing B only after M is computed, such that $(B + 1)^M > 2^{68}$, which in most cases yields a significantly smaller value of B.

Open question: Is there an equivalent to the square-and-multiply algorithm to compute in the isogeny class of an elliptic curve? This would be a means to speed up the construction of public curves.

7. Other suitable parameter choices for trapdoor systems

We look for other fields $\mathbb{F}_{2^N}$ and GHS attack parameters that can be used in a trapdoor constructions. Let I denote a set of (isomorphism classes of) trapdoor curves over $\mathbb{F}_{2^N}$ for which the GHS attack reduces the ECDLP to a HCDLP in the Jacobian of a hyperelliptic curve of genus $g = 2^{m-1}(-1)$ over $\mathbb{F}_{2^l}$, that is feasible, or at least much faster to solve than the ECDLP and possibly feasible in the future. Let $n = N/l$. Let $J = \log_2(\#I)$. First we derive conditions on J such that the use of a public curve E_{pb} over $\mathbb{F}_{2^N}$ provides as much security as a randomly chosen cryptographically interesting curve over $\mathbb{F}_{2^N}$. For this, the following aspects enter the picture:

Running time of the Pollard rho method. Pollard's rho algorithm 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 (taking into account the speed-up by a factor of $\sqrt{2}$ due to the "inverse-point method" [GLV00, WZ98]). 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 $(\sqrt{\pi 2^{N-1}})/2 = 2^{N/2-0.67\ldots}$ to express the running time of Pollard's rho algorithm.

Validity of Assumption A. Assumption A generalized to $\mathbb{F}_{2^N}$ means that an elliptic curve over $\mathbb{F}_{2^N}$ randomly chosen from a given isogeny class has magic number m with probability $2^{J-(N+1)}$. Which can only be true if there is no distortion due to the N isomorphism classes of curves in I stemming from the power-2 Frobenius. That is, we require that $\#I \geq N \cdot \#ISOG$, where $\#ISOG$ denotes the number of isogeny classes over $\mathbb{F}_{2^N}$, which is $2^{N/2+1}$ (taking into account that $\#E(\mathbb{F}_{2^N})$ is always even). Thus, we need $J \geq N/2 + \log N + 1$ for the equivalent of Assumption A to hold.

Cost to find a curve in I that is isogenous to E_{pb}.
Case 1: Assumption A holds. Then we expect that I contains $h_\Delta \cdot 2^{J-(N+1)}$ curves isogenous (over $\mathbb{F}_{2^N}$) to any given curve with discriminant Δ. In other words, out of the $\#I/2$ elements $b \in S$ ($|S| = \#I$ if n even) we expect to need to check $2^N/h_\Delta$ of them until an isogenous curve is found. Each such check involves point counting for $E_{0,b}$ over $\mathbb{F}_{2^N}$ [Gau02], which we consider at least as

costly as 4 elliptic curve operations over $\mathbb{F}_{2^N}$. Then the expected cost to find a curve isogenous to E_{pb} in I exceeds the cost of the Pollard rho algorithm if $h_\Delta < 2^{(N+5)/2}$. This bound, which is almost a formality given that $\Delta \leq 2^{N+2}$ and $h_\Delta \sim \sqrt{\Delta}$, needs to be imposed when constructing the trapdoor curve. No condition on $\#I$ arises in this case.
Case 2: Assumption A does not hold. For the benefit of the attacker we assume that exhaustive search of I is possible, and that all $b \in S$ that have been tested can be stored along with their orbits under the power-2 Frobenius. Then for up to $\#I/(2N)$ b-values ($\#I/N$ if n even) one needs to determine $\#E_{0,b}(\mathbb{F}_2)$. This altogether requires the equivalent of about $4\#I/2N = 2^{J+1-\log N}$ elliptic curve operations. In order that this cost exceeds the cost of Pollard rho we require $J \geq N/2 + \log N - 1.67$, a bound only slightly lower than if we required Assumption A. Therefore will assume from now on that J be chosen such that Assumption A holds.

Cost to reconstruct the trapdoor curve from the public curve. As soon as I is large enough so that finding a curve in I isogenous to E_{pb} is no easier than solving the ECDLP in $E_{\text{pb}}(\mathbb{F}_{2^N})$, we always can choose $h_{\Delta,oc}$ (when constructing the trapdoor curve) and L, B (when constructing the public curve) large enough to guarantee the cost of reconstructing E_{s} from E_{pb} exceeds the cost of Pollard rho.

Cost to find a curve in the isogeny class of E_{pb} that also is in I. Under Assumption A, it takes expected 2^{N+1-J} random walk steps in the isogeny class of E_{pb} to encounter a curve $E' \in I$. Each such step requires $O(Nl^2)$ operations in $\mathbb{F}_{2^N}$, or the equivalent of at least $Nl^2/10$ elliptic curve operations in $E_{\text{pb}}(\mathbb{F}_{2^N})$, where $l \in \{3, \ldots, L\}$, and L is large enough so that Cl_Δ is generated by the split primes of norm $\leq L$ and that a random walk in the isogeny class is simulated. The average cost for each random walk step certainly exceeds $90N$ elliptic curve operations (substituting $l = 30$). Thus, a lower bound for the cost to find an isogenous curve that is in I is $2^{N+1-J+\log N+6.5}$, which exceeds the cost of Pollard rho if $J \leq N/2 + \log N + 8$.

Summing up, we obtain the following bounds on $J = \log \#I$:

$$N/2 + \log N + 1 \leq J \leq N/2 + \log N + 8\ . \tag{7.1}$$

(Note that the lower bound on $\#I$ also ensures that there are plenty of cryptographically interesting curves in I to choose from.) This leaves only a very small window for $\#I$. Also, only those values for N are suitable for which any other way of doing the GHS attack (that is, using a different decomposition $N = nl$) either fails, or yields an algorithm faster than Pollard rho only for a negligible proportion of elliptic curves over $\mathbb{F}_{2^N}$.

Now, Table 7 lists the GHS attack parameters for all finite fields $\mathbb{F}_{2^N}$ ($150 \leq N \leq 600$, N composite) that are possibly suitable for a trapdoor construction as presented in this paper. These data were obtained as follows: Given N, for all divisors n of N we determined those magic numbers m for which the Enge-Gaudry index calculus algorithm in the resulting Jacobian of $C/\mathbb{F}_{2^{N/n}}$ of genus $g = 2^{m-1}(-1)$ with optimally chosen smoothness bound yields a running time faster than Pollard rho for $E(\mathbb{F}_{2^N})$. (The smoothness bound t is the bound on the degree of the prime divisors that are included into the factor base). For each such m, we then determined the number $\#I$ of isomorphism classes of curves over $\mathbb{F}_{2^N}$ with magic number m with respect to n, and checked if (7.1) holds for $J = \log \#I$. In Table 7, J has been rounded to the nearest integer. Moreover, 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 hyperelliptic curve operations in the Enge-Gaudry algorithm, the maximum $T_M(t)$ of $T(t)$ and $L(t) = F(t)^2$ ($L(t)$ is a measure for the cost of the linear algebra step), and the number of elliptic curve operations in Pollard's rho method, respectively. D denotes the difference $\rho - T_M$.

N	n	l	m	g	J	t	F	T	T_M	ρ	D
154	7	22	4	7	90	1	21	33	42	76	34
161	7	23	4	7	94	1	22	34	44	80	36
182	7	26	4	7	106	1	25	37	50	90	40
189	7	27	4	7	110	1	26	38	52	94	42
196	7	28	4	7	114	1	27	39	54	97	43

TABLE 3. Extension degrees N suitable for the trapdoor construction of this paper.

Hence, only extension degrees N that are multiples of 7 seem to be suitable. But as N increases, the size of I grows faster than the running time for Pollard rho, and thus quickly the problem of finding an isogenous curve with magic number 4 becomes too easy.

8. Final remark

As a by-product of this work, the following statements are immediate: (i) Any algorithm to solve Problem P efficiently makes all curves over $\mathbb{F}_{2^{161}}$ insecure. (ii) Any algorithm to solve Problem P considerably faster than solving the ECDLP in $E_{\mathrm{pb}}(\mathbb{F}_{2^{161}})$ makes the field $\mathbb{F}_{2^{161}}$ uninteresting for cryptographic applications. (iii) Any elliptic curve over $\mathbb{F}_{2^{161}}$ that is given to a user of an elliptic curve cryptosystem and is not explicitly meant to be used in a trapdoor system must be generated provably at random, or otherwise is suspicious of being constructed by Algorithm 4.2 or a variant thereof.

Acknowledgements. My thanks go to Jason M Hinek, M.K. Low, and Matt Tucker for support with several of the numerous experiments conducted during this work, for which we used KASH, LiDIA, Magma and NTL. Further thanks go to David McKinnon, Mark Bauer and Alfred Menezes for many helpful discussions, as well as to Frederik Vercauteren for providing the modular polynomials Φ_l for $1 \leq l \leq 2000$.

References

[Cer] The Certicom ECC Challenge. `http://www.certicom.com/research/ecc_challenge.html`.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory.* Springer-Verlag, Berlin, 1993.

[Cox89] D.A. Cox. *Primes of the form $x^2 + ny^2$.* John Wiley & Sons, 1989.

[EG02] A. Enge and P. Gaudry. A general framework for subexponential discrete logarithm algorithms. *Acta Arithmetica*, 102:83–103, 2002.

[Gal99] S. Galbraith. Constructing isogenies between elliptic curves over finite fields. *LMS Journal of Computation and Mathematics*, 2:118–138, 1999.

[Gau00] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology – EUROCRYPT 2000*, volume 1807 of *Lecture Notes in Computer Science*, pages 19 – 34. Springer, 2000.

[Gau02] P. Gaudry. A comparison and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. In *Advances in Cryptology - ASIACRYPT 2002*, volume 2501 of *Lecture Notes in Computer Science*, pages 311–327. Springer-Verlag, 2002.

[GHS02a] S. Galbraith, F. Hess, and N. Smart. Extending the GHS Weil descent attack. In *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *Lecture Notes in Computer Science*, pages 29–44. Springer-Verlag, 2002.

[GHS02b] P. Gaudry, F. Hess, and N. Smart. Constructive and destructive facets of Weil descent on elliptic curves. *J. Cryptology*, 15:19–46, 2002.

[GLV00] R. Gallant, R. Lambert, and S. Vanstone. Improving the parallelized Pollard lambda search on binary anomalous curves. *Mathematics of Computation*, 69:1699–1705, 2000.

[Hes] F. Hess. The GHS attack revisited. In *Advances in Cryptology – EUROCRYPT 2003*, Lecture Notes in Computer Science. Springer-Verlag. To appear.

[IEE00] IEEE. IEEE-1363, Standard specifications for public-key cryptography, 2000.

[Jac99] M. J. Jacobson, Jr. Applying sieving to the computation of quadratic class groups. *Math. Comp.*, 68:859–867, 1999.

[JMS01] M. J. Jacobson, Jr., A. Menezes, and A. Stein. Solving elliptic curve discrete logarithm problems using Weil descent. *Journal of the Ramanujan Mathematical Society*, 16:231–260, 2001.

[Koh96] D. Kohel. *Endomorphism rings of elliptic curves over finite fields.* PhD thesis, University of California, Berkeley, 1996.

[Lan87] S. Lang. *Elliptic Functions.* Springer-Verlag, 1987.

[Lit28] J. E. Littlewood. On the class number of the corpus $p(\sqrt{-k})$. *Proceedings of the London Mathematical Society*, 27:358–372, 1928.

[MMT02] M. Maurer, A. Menezes, and E. Teske. Analysis of the GHS Weil descent attack on the ECDLP over characteristic two finite fields of composite degree. *LMS Journal of Computation and Mathematics*, 5:127–174, 2002.

[MQ01] A. Menezes and M. Qu. Analysis of the Weil descent attack of Gaudry, Hess and Smart. In *Topics in Cryptology – CT-RSA 2001*, volume 2020 of *Lecture Notes in Computer Science*, pages 308–318. Springer, 2001.

[Pol78] J. M. Pollard. Monte Carlo methods for index computation (mod p). *Mathematics of Computation*, 32(143):918–924, 1978.

[Sil94] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, 1994.

[Ste01] A. Stein. Sharp upper bounds for arithmetics in hyperelliptic function fields. *Journal of the Ramanujan Mathematical Society*, 16:1–86, 2001.

[Tes01] E. Teske. On random walks for Pollard's rho method. *Mathematics of Computation*, 70:809–825, 2001.

[Vél71] J. Vélu. Isogénies entre courbes elliptiques. *Compte Rendues Acad. Sci. Paris, Sér. A*, 273:238–241, 1971.

[vOW99] P. C. van Oorschot and M. J. Wiener. Parallel collision search with cryptanalytic applications. *Journal of Cryptology*, 12:1–28, 1999.

[WZ98] M. Wiener and R. Zuccherato. Faster attacks on elliptic curve cryptosystems. In *Proceedings of SAC – Workshop on Selected Areas in Cryptography*, volume 1556 of *Lecture Notes in Computer Science*, pages 190 – 200. Springer, 1998.

Appendix A. An example

Using Algorithm 4.1, we constructed the curve $E_{\mathrm{s},1} = E_{a,b}$ over $\mathbb{F}_{2^{161}} = \mathbb{F}_2[z]/(z^{161}+z^{18}+1)$ where $a = 0$ and $b = z^{152}+z^{143}+z^{139}+z^{136}+z^{135}+z^{133}+z^{130}+z^{125}+z^{124}+z^{122}+z^{120}+z^{119}+z^{118}+z^{117}+z^{116}+z^{114}+z^{113}+z^{112}+z^{110}+z^{109}+z^{106}+z^{105}+z^{103}+z^{102}+z^{101}+z^{99}+z^{97}+z^{96}+z^{92}+z^{91}+z^{88}+z^{87}+z^{86}+z^{85}+z^{81}+z^{78}+z^{77}+z^{76}+z^{75}+z^{73}+z^{71}+z^{69}+z^{68}+z^{67}+z^{66}+z^{63}+z^{59}+z^{58}+z^{53}+z^{51}+z^{50}+z^{49}+z^{48}+z^{46}+z^{45}+z^{44}+z^{42}+z^{38}+z^{34}+z^33+z^{32}+z^{31}+z^{29}+z^{27}+z^{26}+z^{24}+z^{23}+z^{22}+z^{21}+z^{20}+z^{19}+z^{18}+z^{17}+z^{16}+z^{15}+z^{14}+z^{13}+z^{12}+z^{10}+z^7+z^6+z^4+z^3+z^2$. This curve has magic number $m(7) = 4$, and on performing the GHS Weil descent attack we obtain a hyperelliptic curve of genus $g = 8$. It has $4r$ points over $\mathbb{F}_{2^{161}}$, with $r = 730750818665451459101841775429946272920385056109$ prime. Its discriminant Δ is squarefree, has 162 bits, and $\mathrm{Cl}_\Delta = [1215497015372525105759490]$, with an 80-bit odd cyclic part. Thus, $E_{\mathrm{s},1}$ is a valid trapdoor curve.

We then used Algorithm 4.2 with $L = 300$ and $B = 11$. We found $M = 28$, and constructed the public curve $E_{\mathrm{pb},1} = E_{a,b'}$ with $a = 0$ and $b' = z^{160}+z^{156}+z^{155}+z^{153}+z^{152}+z^{151}+z^{150}+z^{149}+z^{148}+z^{147}+z^{146}+z^{145}+z^{143}+z^{142}+z^{141}+z^{130}+z^{129}+z^{127}+z^{126}+z^{125}+z^{124}+z^{123}+z^{120}+z^{118}+z^{112}+z^{109}+z^{104}+z^{103}+z^{102}+z^{101}+z^{99}+z^{98}+z^{97}+z^{96}+z^{93}+z^{92}+z^{91}+z^{90}+z^{88}+z^{85}+z^{83}+z^{77}+z^{74}+z^{70}+z^{68}+z^{65}+z^{64}+z^{63}+z^{62}+z^{61}+z^{60}+z^{58}+z^{57}+z^{55}+z^{50}+z^{48}+z^{45}+z^{41}+z^{38}+z^{37}+z^{36}+z^{33}+z^{31}+z^{30}+z^{27}+z^{26}+z^{24}+z^{23}+z^{22}+z^{21}+z^{20}+z^{19}+z^{17}+z^{16}+z^{14}+z^{13}+z^{10}+z^8+z^7+z^4+z^3+z$.

Appendix B. A challenge

Alice uses the public curve $E_{\mathrm{pb},2} = E_{a,b}$ over $\mathbb{F}_{2^{161}} = \mathbb{F}_2[z]/(z^{161} + z^{18} + 1)$, where $a = 1$ and $b = z^{160} + z^{158} + z^{155} + z^{152} + z^{151} + z^{150} + z^{149} + z^{148} + z^{147} + z^{144} + z^{142} + z^{140} + z^{137} + z^{136} + z^{134} + z^{133} + z^{131} + z^{130} + z^{127} + z^{126} + z^{124} + z^{123} + z^{122} + z^{120} + z^{117} + z^{114} + z^{111} + z^{109} + z^{103} + z^{102} + z^{100} + z^{99} + z^{98} + z^{95} + z^{94} + z^{90} + z^{88} + z^{86} + z^{81} + z^{80} + z^{79} + z^{78} + z^{77} + z^{76} + z^{75} + z^{74} + z^{65} + z^{64} + z^{57} + z^{56} + z^{54} + z^{53} + z^{52} + z^{50} + z^{46} + z^{45} + z^{44} + z^{40} + z^{39} + z^{37} + z^{35} + z^{33} + z^{31} + z^{30} + z^{29} + z^{28} + z^{26} + z^{23} + z^{22} + z^{21} + z^{18} + z^{14} + z^{13} + z^{9} + z^{8} + z^{7} + z^{3} + z^{2} + 1$. This curve has been constructed from a curve in I_4 using Algorithm 4.2 with $L = 300$ and $B = 11$. $E_{\mathrm{pb},2}(\mathbb{F}_{2^{161}})$ has group order $2r$ where $r = 1461501637330902918203684418527084399771825396431$. Its discriminant Δ has 163 bits and is squarefree, and $\mathrm{Cl}_\Delta = [2\ 2\ 382272180083678181989678]$, with a 78-bit odd cyclic part. Challenge: find a curve in I_4 isogenous over $\mathbb{F}_{2^{161}}$ to $E_{\mathrm{pb},2}$.

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

E-mail address: eteske@math.uwaterloo.ca