On the Weil descent attack on the Elliptic Curve Discrete Logarithm Problem

IPAM/UCLA, January 11, 2002

Edlyn Teske

C&O/CACR

University of Waterloo

Dept. of **C**ombinatorics and **O**ptimization
Centre for **A**pplied **C**ryptographic **R**esearch

E elliptic curve over $\mathbb{F}_{2^N}$.

$$E : y^2 + xy = x^3 + ax^2 + b \ , \qquad a, b \in \mathbb{F}_{2^N} \ .$$

Elliptic Curve Discrete Logarithm Problem (ECDLP):

Given E, $P \in E(2^N)$, $r = \mathrm{ord}(P)$ and $Q \in \langle P \rangle$, find $s \in [0, r-1]$ such that

$$Q = sP \ .$$

We write $s = \log_P Q$.

The apparent intractability of the ECDLP forms the basis for the security of elliptic curve cryptographic schemes.

The elliptic curve E over $\mathbb{F}_{2^N}$ is **cryptographically interesting** if

1. $\#E(\mathbb{F}_{2^N}) = rd$, r large prime and d small.
   (avoid Pohlig-Hellman & Pollard rho attacks).

2. $r \not| 2^{jN} - 1$, $j \in [1, J]$,
   J large enough so that DLP in $\mathbb{F}_{2^{JN}}^*$ is hard.
   (avoid Weil pairing and Tate pairing attacks).

For the ECDLP in cryptographically interesting curves, the best algorithm known to date is the parallelized Pollard rho attack.

This statement needs to be revised:

There are cryptographically interesting curves for which the best attack is better than Pollard rho. This attack is based on **Weil descent**.

Outline

- Introduction
- Weil Descent and GHS Attack
  - Weil Descent Methodology
  - GHS Attack (I)
  - Hyperelliptic Curves
  - GHS Attack (II)
- Analysis of the GHS Weil Descent Attack
  - Curves over $\mathbb{F}_{2^p}$, p prime
  - Index-Calculus Algorithm for the HCDLP
  - Curves over $\mathbb{F}_{2^N}$, N composite
- Extended Weil Descent Attack
- Weil Descent for F_{q^n}, q odd.
- Conclusion

Weil Descent Methodology

- First proposed by G. Frey in 1998.

- Idea: Reduce the ECDLP in $\mathbb{F}_{2^N}$ to a DLP in an abelian variety over a proper subfield of $\mathbb{F}_{2^N}$.

Let $N = nl$, $q = 2^l$. Then $\mathbb{F}_{2^N} = \mathbb{F}_{q^n}$. Consider

$$E/\mathbb{F}_{q^n} : y^2 + xy = x^3 + ax^2 + b \ . \qquad (*)$$

Let $\{\gamma_1, \ldots, \gamma_n\}$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
Let

$$\begin{aligned}
a &= a_1\gamma_1 + a_2\gamma_2 + \cdots + a_n\gamma_n \ , & a_i \in \mathbb{F}_q \ , \\
b &= b_1\gamma_1 + b_2\gamma_2 + \cdots + b_n\gamma_n \ , & b_i \in \mathbb{F}_q \ , \\
x &= x_1\gamma_1 + x_2\gamma_2 + \cdots + x_n\gamma_n \ , & x_i \in \mathbb{F}_q \ , \\
y &= y_1\gamma_1 + y_2\gamma_2 + \cdots + y_n\gamma_n \ , & y_i \in \mathbb{F}_q \ ,
\end{aligned}$$

Substitute into $(*)$ and **equate coefficients** of γ_i.

Result: n equations in $2n$ variables over $\mathbb{F}_q$:
an n-dimensional abelian variety A over $\mathbb{F}_q$ called the **Weil restriction** of E to $\mathbb{F}_q$.

Now, **intersect** A with $n-1$ hyperplanes and eliminate variables.
Result: Algebraic curve C over $\mathbb{F}_q$.

$$E(\mathbb{F}_{q^n})$$

$$C/\mathbb{F}_q \qquad\qquad A(\mathbb{F}_q)$$

$$J_C(\mathbb{F}_q)$$

Strategy to solve ECDLP:
Map points P, Q in $E(\mathbb{F}_{q^n})$ to divisors in $J_C(\mathbb{F}_q)$, the Jacobian of C, and solve the DLP in $J_C(\mathbb{F}_q)$.

$J_C(\mathbb{F}_q)$ = abelian variety of dimension g, the **genus** of the curve C.
(Elliptic curves have genus $g = 1$.)

The GHS Weil Descent Attack (I)

- P. **G**audry & F. **H**ess & N. **S**mart.

- Uses Frey's methodology
  (via special selection of hyperplanes)
  to reduce instance of ECDLP in $\mathbb{F}_{2^N} = \mathbb{F}_{q^n}$
  to instance of DLP in the Jacobian $J_C(\mathbb{F}_{2^l})$
  of a **hyperelliptic curve** over $\mathbb{F}_{2^l} = \mathbb{F}_q$.
  $\longrightarrow$ Explicit **HCDLP**
  = Hyperelliptic Curve Discrete Logarithm Problem.

For the HCDLP with high-genus curves, subexponential time algorithms are known.

Does this yield an attack that is better than Pollard's rho method?

Hyperelliptic Curves

- $k = \mathbb{F}_q$, finite field , $\#k = q$, $\mathrm{char}(k) = 2$.

- **Hyperelliptic curve** of genus g over k

$$C : \; v^2 + h(u)v = f(u) \; ,$$

  $h, f \in k[u]$, $\deg(f) = 2g + 1$, $\deg(h) \leq g$.

- **Jacobian** of C over k:

$$J_C(k) = D_k^0 / \mathrm{Prin}_k$$

  (degree zero divisors over principal divisors).

  - $J_C(k)$ is a finite abelian group.
  - Its elements: **divisor classes**.
  - Each divisor class has unique reduced representative: **reduced divisor**.
  - **Cantor's algorithm** to perform group operations.

– **HCDLP:**
Given C, $D_1 \in J_C(k)$, $r = \mathrm{ord}(D_1)$,
$D_2 \in \langle D_1 \rangle$,

find $s \in [0, r-1]$ such that

$$D_2 = sD_1 \ .$$

– **Hasse-Weil** and **Artin bounds** on $\#J_C(k)$,
Brauer-Siegel Theorem for function fields:

$$\#J_C(\mathbb{F}_q) \sim q^g \ .$$

The GHS Weil Descent Attack (II)

For

$$E/\mathbb{F}_{q^n} : y^2 + xy = x^3 + ax^2 + b$$

assume

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

Then the GHS attack constructs an **explicit group homomorphism**

$$\Phi : E(\mathbb{F}_{q^n}) \longrightarrow J_C(\mathbb{F}_q) \ ,$$

where C is a hyperelliptic curve over $\mathbb{F}_q$ of genus

$$g = 2^{m-1} \text{ or } g = 2^{m-1} - 1 \ .$$

Here, $m = m(b) =$ "magic number" $=$

$$\dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, b_0^{1/2}), \ldots, (1, b_{n-1}^{1/2})\}) \ ,$$

where $b_i = \sigma^i(b)$, for $0 \leq i \leq n-1$ and

$$\begin{array}{rl} \sigma : & \mathbb{F}_{q^n} \to \mathbb{F}_{q^n} \\ & \alpha \mapsto \alpha^q \end{array} \qquad \text{Frobenius automorphism.}$$

Consequence: ECDLP in $E(\mathbb{F}_{q^n})$ is **reduced** to HCDLP in the Jacobian $J_C(\mathbb{F}_q)$ of a hyperelliptic curve C of genus 2^{m-1} or $2^{m-1}-1$:

$P \in E(\mathbb{F}_{q^n})$, $\mathrm{ord}(P) = r$, $Q \in \langle P \rangle$:

$$\begin{array}{rcl} \Phi : E(\mathbb{F}_{q^n}) & \longrightarrow & J_C(\mathbb{F}_q) \\ P & \longrightarrow & \Phi(P) \\ Q & \longrightarrow & \Phi(Q) \end{array}$$

$$\log_P Q = \log_{\Phi(P)} \Phi(Q) \ .$$

The **condition** for this to work:

$\ker(\Phi)$ must not contain a subgroup of order r. (Otherwise, Φ maps P, Q to zero divisor of $J_C(\mathbb{F}_q)$.)

This condition is very likely to hold if $\#J_C(\mathbb{F}_q) \geq \#\langle P \rangle$ and r is a large prime.

Analysis of the GHS attack

Case 1: Prime extension degree

$E(\mathbb{F}_{2^N})$, N prime.
Then we (only) can reduce ECDLP to HCDLP in $J_C(\mathbb{F}_2)$.

Menezes & Qu (2001):

Let $t = \text{ord}(2)$ modulo N.
Then, for $b \in \mathbb{F}_{2^N}$,

$$m = m(b) \in \{1, t+1, 2t+1, \ldots, st+1\} ,$$

where $s = (N-1)/t$
(so $st + 1 = N$).

Recall: genus of C is $g = 2^{m-1}$ or $2^{m-1} - 1$.

Now, for each $N \in [100, 600]$, determine possible values for $m(b)$.

Result:
If $N \in [128, 600]$, prime, then $m = 1$ or $m \geq 16$.

- $m = 1$ if and only if E is defined over $\mathbb{F}_2$ ("Koblitz curve").
  Then $g = 1$,
  and $J_C(\mathbb{F}_2)$ is **too small** to contain subgroup of large prime order.

- If $m \geq 16$, then $g \geq 2^{15} \approx 33000$.
  So we'd have to work in Jacobian of size 2^{33000}.
  Infeasible.

Thus, GHS attack **fails for all elliptic curves** E/F_{2^N} when N prime, $128 \leq N \leq 600$.

Remark: Most current standards work with prime extension degree.
E.g.: NIST FIPS 186-2: $N = 163, 233, 283, 409, 571$.
If $N = 163$, then ord(2) modulo $N = 162$, so $m = 1$ or $m = 163$.

Case 2: Composite extension degree

$N = nl$, E/F_{q^n}, $J_C(\mathbb{F}_q)$, $q = 2^l$.

Menezes-Qu approach can be generalized.

Given an ECDLP for an elliptic curve E over $\mathbb{F}(q^n)$:

factorization of $x^n - 1$ over $\mathbb{F}_2$	admissible values of m
curve parameter b	specific m
$\#\langle P \rangle$ (P on E)	lower bound on m via $\#\langle P \rangle \leq \#J_C(\mathbb{F}_q) \approx q^g$, $g = 2^{m-1}$ or $g = 2^{m-1} - 1$.
running time of best algorithm for HCDLP	GHS attack is feasible /not feasible for given parameters (n, m, g).

Best algorithm to solve the HCDLP:
Enge-Gaudry Index-Calculus Algorithm (EG):

- Uses concept of **smooth divisors** to devise **Index-calculus** in Jacobian of hyperelliptic curves.

- **Subexponential** for high genus. Faster than Pollard's rho method for $g \geq 4$.

- Enge & Gaudry (2000): algorithm and asymptotic analysis.

- Jacobson & Menezes & Stein (2001): **Precise estimates** of expected # of hyperelliptic curve operations for a given *smoothness bound*.

Given $J_C(k)$, where C of genus g.

- Parameter: **Smoothness bound** t.
  $\longrightarrow$ Factor base of size $F(t)$.
- Precise estimate of number of t-smooth reduced divisors.
  $\longrightarrow$ Expected number of operations to find one *relation*.
- Need $F(t) + 5$ relations.
- Yields total expected number of operations.
- Neglect time for linear algebra step.

Note:

- t has to be optimized.
- Need $F(t) \leq 10^7 \approx 2^{23}$ for linear algebra step to be manageable.
  (Gaussian elimination followed by Lanczos, see Joux & Lercier (2000)).

Analysis for N composite
Maurer & Menezes & Teske (2001)

For each composite $N \in [100, 600]$:

- For each $n \mid N$, $n > 1$,
  - **factor** $x^n - 1$ over $\mathbb{F}_2$ and determine admissible values of $m = m(b)$
  - **find** m and $g = 2^{m-1} - 1$ (large enough), and smoothness bound t
    such that $T =$ expected number of hyperelliptic curve operations is **minimal**.

- Minimize over all $n \mid N$.

- Compare T with expected number ρ of elliptic curve operations in Pollard rho.

Example: $160 \leq N \leq 180$

EG1: factor base $\leq 10^7 = 2^{23.25}$										
N	n	l	m	g	log I	t	log F	log T	log ρ	log Δ
160	20	8	6	31	48	3	21	52	79	27
161	7	23	4	7	94	1	22	34	80	46
162	54	3	7	63	21	9	23	42	80	38
164	–	–	–	–	–	–	–	–	–	–
165	15	11	5	15	58	2	20	37	82	45
166	–	–	–	–	–	–	–	–	–	–
168	7	24	4	7	98	1	23	35	83	48
169	169	1	13	4095	14	28	23	1208	84	–
170	170	1	9	255	12	28	23	53	84	31
171	171	1	9	255	10	28	23	53	85	32
172	–	–	–	–	–	–	–	–	–	–
174	–	–	–	–	–	–	–	–	–	–
175	35	5	7	63	36	5	22	65	87	22
176	8	22	5	16	110	1	21	65	87	22
177	–	–	–	–	–	–	–	–	–	–
178	178	1	12	2047	15	28	23	529	88	–
180	15	12	5	15	63	2	22	39	89	50

Example: E161

$\mathbb{F}_{2^{161}} = \mathbb{F}_2[z]/(z^{161} + z^{18} + 1)$.

$E: y^2 + xy = x^3 + ax^2 + b$ with
$\#E(\mathbb{F}_{2^{161}}) = 2 \cdot r$, where

$a = 1$
$b =$ 1102A36EE3EEE95C1DDA26A51A954391733728D22
$r =$ FFFFFFFFFFFFFFFFFFFFFD03F975D827A7D20F89

ECDLP:

$$Q = sP \ ,$$

where

$P =$ (1CBF654BEEF0AE9F525F8E9F5FA1DED1D10C7D781,
175984F97695A39291B94B6D9BD89860C9AF5DF80)
$Q =$ (AE24976AE483ED2E33A77FD48F78DAE06ED0F54E,
186EBA8B979ADAA320D47C7763CFF8EF810A970EB)

P and Q are chosen **provably at random**.
(x-coordinates determined by
SHA-1 on input "" and "a".)

How to solve this ECDLP:

$161 = 23 \cdot 7$, thus $\mathbb{F}_{2^{161}} = \mathbb{F}_{(2^{23})^7}$.

GHS attack maps $E161$ into the Jacobian of the hyperelliptic curve

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

$C: \; v^2 + h(u)v = f(u)$, where

$$f(u) = w^{6691705}u^{15} + w^{4316786}u^{14} + w^{4857716}u^{12} + w^{4289455}u^8 + w^{7257339}$$
$$h(u) = w^{7540156}u^7 + w^{4708240}u^6 + w^{2060647}u^4 + w^{7822973}$$

C has genus $g = 7$.

The points $P + R$, $Q + R$ and an (arbitrarily chosen) auxiliary point R on $E161$,

$R =$ (1E7958EF1FA48A2B92889B442DADE6E9A6A7C173,
4EE6671B1A5D69A5578EFE30C05704FA69C78345)

are mapped to the reduced divisors in $J_C(\mathbb{F}_{2^{23}})$

$$D_P = \mathrm{div}(u^7 + w^{111674}u^6 + w^{6262987}u^5 + w^{5507868}u^4 + w^{5024071}u^3 + w^{7360243}u^2 + w^{4982988}$$
$$w^{7214579}u^6 + w^{1039748}u^5 + w^{5362902}u^4 + w^{5575575}u^3 + w^{6046318}u^2 + w^{783556}u + w$$
$$D_Q = \mathrm{div}(u^7 + w^{2418740}u^6 + w^{6332447}u^5 + w^{5288518}u^4 + w^{6581623}u^3 + w^{3461659}u^2 + w^{663714}$$
$$w^{5819570}u^6 + w^{5789770}u^5 + w^{3853008}u^4 + w^{3628267}u^3 + w^{4786898}u^2 + w^{3463517}u + w^{2504}$$
$$D_R = \mathrm{div}(u^7 + w^{7595037}u^6 + w^{6492024}u^5 + w^{5128797}u^4 + w^{1479702}u^3 + w^{3764869}u^2 + w^{297361}$$
$$w^{5819570}u^6 + w^{5789770}u^5 + w^{3853008}u^4 + w^{3628267}u^3 + w^{4786898}u^2 + w^{3463517}u + w^{2504}$$

Instead of ECDLP now **HCDLP:** find s such that

$$(D_Q - D_R) = s(D_P - D_R) \ .$$

C has genus $g = 7$, so $\#J_C(\mathbb{F}_{2^{23}}) \approx 2^{161}$.

Enge-Gaudry-Index-Calculus Algorithm:
optimized parameters for this HCDLP:
Factor basis $\approx 2^{22}$ reduced divisors
($\approx 4 \cdot 10^6$, feasible).

Expected: 2^{34} additions of reduced divisors in Jacobian.

25.000 days on a 1GHz PIII workstation.

To compare:
DES break using exhaustive search:
110.000 days on a 450MHz PII.
Pollard rho for 108-bit ECDLP:
200.000 days on 450MHz PII.
Pollard rho for E161: 2^{80} additions on E161.
10^{14} days on 500MHz Alpha workstation.

Remark:

- Over $\mathbb{F}_{2^{161}}$ there are approx. 2^{94} isomorphism classes of such insecure elliptic curves.

- There are ca. 2^{162} isomorphism classes over $\mathbb{F}_{2^{161}}$.

- Thus: Probability for GHS attack to be successfull for **randomly** chosen curve is **small**.

- Efficiency of attack is easy to check in advance:
  Genus g of hyperelliptic curve determined by curve parameter b from
  $E: y^2 + xy = x^3 + ax^2 + b$.

However: **Galbraith & Hess & Smart (2001):**

Extension of the GHS attack to **isogenous** curves.

$K = \mathbb{F}_{q^n}$.
Two elliptic curves E/K and E'/K are K-isogenous if $\#E(K) = \#E'(K)$.

An isogeny $\Psi : E \to E'$ can be determined in expected time $O(q^{n/4+\varepsilon})$.

Thus, if E/K is isogenous to a curve E'/K with small m-value, the ECDLP instance in $E(K)$ can be mapped to ECDLP instance in $E'(K)$ and solved over there.

Consequences for E161:

There are approx. $2^{82.5}$ isogeny classes of elliptic curves over $\mathbb{F}_{2^{161}}$.
There are approx. 2^{94} insecure isomorphism classes.
We thus expect that **every** isogeny class contains at least one insecure curve.

Study the following two **problems:**

Given a curve E_1,

- **Find** a curve E_2, isogenous with E_1, in one of the 2^{94} insecure isomorphism classes.
- Or: **Find** a curve E_3 in the isogeny class of E_1 that is insecure.
  We expect $2^{79.5}$ curves per isogeny class, out of which $2^{11.5}$ are insecure.

So far: exhaustive search is the only solution.
Not possible for either problem.

An efficient solution of one of these problems makes **all curves** over $\mathbb{F}_{2^{161}}$ **insecure**.

Weil Descent in Odd Characteristic

Diem (2001):

GHS Weil Descent attack can be generalized from fields of characteristic 2 to the case

E/F_{q^n}, $q = p^l$, p odd prime, $n \geq 3$ odd.

For $n = 5$ or $n = 7$ there exist examples of elliptic curves $E/\mathbb{F}_{q^n}$ for which the genus of the hyperelliptic curve is 5 or 7, respectively, so

$$\#J_C(\mathbb{F}_q) \approx \#E(\mathbb{F}_{q^n}) \ ,$$

and HCDLP in $J_C(\mathbb{F}_q)$ is possibly easier to solve than ECDLP in $E(\mathbb{F}_{q^n})$.

If $n \geq 11$, n prime, then $q^g \geq 2^{5000}$ for $q^n \geq 2^{160}$, so Jacobian is too large.

Conclusion

- Weil descent methodology – a new approach to solve the ECDLP.
- GHS Weil descent attack – the first (and only so far) concrete application for cryptographically interesting curves.
- GHS attack **fails** for all elliptic curves over $\mathbb{F}_{2^N}$, where $N \in [128, 600]$ is prime.
- GHS attack **successful** in specific cases when N is composite,
  e.g. for certain curves over F_{2^N} where
  $N = 161, 180, 186, 217, 248, 300$.
- GHS attack may apply in odd characteristic, if extension degree $n = 5, 7$. ($N = nl$.)
- GHS attack does **not** apply to elliptic curves over large **prime fields**.
- Need: study other possible ways to apply Weil descent.
- Need: further study of algorithms for the HCDLP.