CRYPTOGRAPHIC IMPLICATIONS OF GAUDRY-HESS-SMART WEIL DESCENT

Alfred Menezes
University of Waterloo

ECC 2001
October 30, 2001

Outline

- Introduction
- Hyperelliptic Curve Discrete Logarithm Problem
- Weil Descent and the GHS Attack
- Analysis
- Extensions of Prime Degree
- Extensions of Composite Degree
- Increasing the Number of Susceptible Curves
- Conclusions

Introduction

- No subexponential-time algorithm known for the ECDLP.
- **Weil descent** is a technique introduced by Frey that can be used to reduce the ECDLP to the DLP in other algebraic varieties such as hyperelliptic curves for which there may be more efficient DLP solvers.
- Here we study the implications of the **GHS Weil descent attack** on the ECDLP for elliptic curves over **characteristic two finite fields**.

Hyperelliptic Curves

- A **hyperelliptic curve** of genus g over $k = \mathbb{F}_q$ is defined by:

$$v^2 + h(u)v = f(u),$$

  where $h, f \in k[u]$, $\deg f = 2g+1$, $\deg h \leq g$.
- The **jacobian** of C over $\mathbb{F}_q$ is $J_C(k) = D_k^0/\mathsf{Prin}_k$.
- $(\sqrt{q}-1)^{2g} \leq \#J_C(k) \leq (\sqrt{q}+1)^{2g}$, so $\#J_C(k) \approx q^g$.
- Each jacobian element can be uniquely represented in **reduced form** $D = \mathrm{div}(a, b)$, where $a, b \in k[u]$, a is monic, $\deg b < \deg a \leq g$, and $a|(b^2 + bh - f)$.
- **Cantor's algorithm:** efficient algorithm for adding two reduced divisors.

Hyperelliptic Curve Discrete Logarithm Problem

- **HCDLP**: Given C, $D_1 \in J_C(k)$, $r = \text{ord}(D_1)$, $D_2 \in \langle D_1 \rangle$, find $l \in [0, r-1]$ such that $D_2 = lD_1$.
- **Subexponential-time algorithms for HCDLP**: Adleman-DeMarrais-Huang (1994), Gaudry (2000), Enge-Gaudry (2000).
- **Prime divisor**: $D = \text{div}(a, b)$, where a is irreducible over k. The **degree** of D is $\deg a$.
- **Fact**: If $D = \text{div}(a, b) \in J_C(k)$ and $a = a_1^{e_1} a_2^{e_2} \cdots a_L^{e_L}$ over k, then $D = \Sigma_{i=1}^{L} e_i \text{div}(a_i, b_i)$, where $b_i = b \bmod a_i$, expresses D as a sum of prime divisors.
- D is ***t*-smooth** if max$\{\deg a_i\} \le t$.

Enge-Gaudry Algorithm

1. Select a **smoothness bound** $t \in [1, g]$.
2. **Factor base**: $S = \{P_1, P_2, \ldots, P_w\}$= all prime divisors of degree $\le t$.
3. Perform a **random walk** (á la Teske) in the set of reduced divisors equivalent to divisors of the form $\alpha D_1 + \beta D_2$. Store relations $\alpha_i D_1 + \beta_i D_2 \equiv R_i = \Sigma e_{ij} P_j$.
4. Collect $w + 1$ relations and then find by **linear algebra** modulo r: $\Sigma_{i=1}^{w+1} \gamma_i (e_{i1}, e_{i2}, \ldots, e_{iw}) = (0, 0, \ldots, 0)$.
5. Then $\log_{D_1} D_2 = -(\Sigma \gamma_i \alpha_i)/(\Sigma \gamma_i \beta_i) \bmod r$.

Asymptotic running time: $L_{q^g}[\sqrt{2}]$ for $g/\log q \to \infty$.

Weil Descent Attack

- Frey (1998); Galbraith & Smart (1999).
- $q = 2^l$, $N = ln$.
- $E/\mathbb{F}_{q^n} : y^2 + xy = x^3 + ax^2 + b \qquad (*)$
- Let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be a basis for $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$.
- Let $$\begin{aligned} a &= a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n, & a_i &\in \mathbb{F}_q. \\ b &= b_1\beta_1 + b_2\beta_2 + \cdots + b_n\beta_n, & b_i &\in \mathbb{F}_q. \\ x &= x_1\beta_1 + x_2\beta_2 + \cdots + x_n\beta_n, & x_i &\in \mathbb{F}_q. \\ y &= y_1\beta_1 + y_2\beta_2 + \cdots + y_n\beta_n, & y_i &\in \mathbb{F}_q. \end{aligned}$$
- Substitute into (*) and equate coefficients of β_i to get 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 find a curve C which lies on A:
  - Intersect A with $n-1$ hyperplanes and eliminate variables to obtain an **algebraic curve** C over $\mathbb{F}_q$.
- Hopefully, $J_C(\mathbb{F}_q) \cong$ subgroup of $E(\mathbb{F}_{q^n})$.

$$\begin{tikzcd}
 & & E(\mathbb{F}_{q^n}) \arrow[d] \\
C/\mathbb{F}_q \arrow[rr] \arrow[dr] & & A(\mathbb{F}_q) \\
 & J_C(\mathbb{F}_q) \arrow[ur] &
\end{tikzcd}$$

- Some questions:
  - What is the genus of C?
  - How to solve the DLP in $J_C(\mathbb{F}_q)$?
  - How to map points in $E(\mathbb{F}_{q^n})$ to divisors in $J_C(\mathbb{F}_q)$?

GHS Attack

- Gaudry, Hess and Smart (2000)
- Assume that n is odd, or $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(a) = 0$, or $m(b) = n$.
- For a special selection of hyperplanes:

(i) The curve C is **hyperelliptic**.

(ii) C has **genus** $g = 2^{m-1}$ or $2^{m-1} - 1$ where

$$m = m(b) = \mathsf{dim}_{\mathbb{F}_2}(\mathsf{Span}_{\mathbb{F}_2}\{(1, b_0^{1/2}), \ldots, (1, b_{n-1}^{1/2})\})$$

and $b_i = b^{q^i}$.

(iii) The defining **equation** of C can be efficiently obtained.

(iv) There is an efficient algorithm for mapping points in $E(\mathbb{F}_{q^n})$ to divisors in $J_C(\mathbb{F}_q)$.

Note: Florian Hess has a KASH program for (iii) and (iv).

Surprising Nature of the Results

- The **moduli space M_g** over an algebraically closed field F is an irreducible quasi-projective variety over F whose elements are in 1-1 correspondence with the isomorphism classes of genus-g curves over F.
- The dimension of M_g over F is $3g - 3$ for $g \geq 2$.
- The isomorphism classes of genus-g hyperelliptic curves over F correspond to an irreducible subvariety of M_g of dimension $2g - 1$.
- One would expect that the number of genus-g curves over a finite field $\mathbb{F}_q$ is $O(q^{3g-3})$, while the number of genus-g hyperelliptic curves over $\mathbb{F}_q$ is $O(q^{2g-1})$.
- Thus, for $g \geq 3$, it is extremely unlikely that a random genus-g curve over $\mathbb{F}_q$ is hyperelliptic.

Analysis of the GHS Attack

The genus of $C/\mathbb{F}_q$ is $g = 2^{m-1}$ or $2^{m-1} - 1$, where $m = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, b_0^{1/2}), \ldots, (1, b_{n-1}^{1/2})\})$ and $b_i = b^{q^i}$.

(i) $1 \leq m \leq n$, so $1 \leq g \leq 2^{n-1}$.

(ii) If $m = 1$, so $g = 1$, the reduction is useless.

Example: If E is defined over $\mathbb{F}_q$.

Special case: Elliptic curves defined over $\mathbb{F}_2$.

(iii) If $\#E(\mathbb{F}_{q^n})$ is almost prime, then the reduction is useless if $m < 1 + \log_2 n$.

(iv) If $m = n$ then $g = 2^{n-1}$.

Example: If $l = 1$, the reduction takes fully exponential time ($\#J_C(\mathbb{F}_q) \approx q^{2^{n-1}}$).

Analysis: n prime

- (M, Qu 2000) Let n be an odd prime, $t = \mathrm{ord}_n(2)$, $s = (n-1)/t$, $b \in \mathbb{F}_{q^n}$. Then
$$m(b) \in \{1, t+1, 2t+1, \ldots, st+1\}.$$
Moreover, the number of $b \in \mathbb{F}_{q^n}$ with $m(b) = it + 1$ is $q\binom{s}{i}(q^t - 1)^i$.
- **Non-Koblitz curves over $\mathbb{F}_{2^n}$, n prime**.
  - If $n \in [160, 600]$, then $m \geq 18$, so $g \geq 2^{17} \approx 128,000$.
  - So GHS attack fails for *all* elliptic curves over $\mathbb{F}_{2^n}$.
  - NIST FIPS 186-2 binary fields: $n = 163, 233, 283, 409, 571$.
  - If $\mathrm{ord}_n(2) = n - 1$ (e.g., $n = 163$), then $m = n$ for *all* non-Koblitz curves, so $g = 2^{n-1}$ or $2^{n-1} - 1$.

Elliptic Curves over $\mathbb{F}_{2^{155}}$

(a) $q = 2^{31}$, $n = 5$.

- $g = 1, 15$ or 16.
- HCDLP in a genus 15 curve over $\mathbb{F}_{2^{31}}$ is infeasible. (Smart, Eurocrypt 2001)

(b) $q = 2^5$, $n = 31$.

- $m = 6$ and $g = 31$ for a small fraction of elliptic curves over $\mathbb{F}_{2^5}$ (2^{33} out of 2^{156} curves).
- HCDLP in a genus 31 curve over $\mathbb{F}_{2^5}$ is feasible. (Jacobson, M, Stein, 2001)

Exact Analysis of Enge-Gaudry Algorithm for HCDLP

- For each $l \in [1, t]$, let A_l be the number of prime divisors of degree l in the factor base.
- The number of of t-smooth reduced divisors in $J_C(\mathbb{F}_q)$ is

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

  where $[\,]$ denotes the coefficient operator.
- This enables one to select the optimal value of t, and provide **exact** running time estimates for specific instances of the HCDLP.

Example: ECDLP over $\mathbb{F}_{2^{124}}$

- $\mathbb{F}_{2^{124}} = \mathbb{F}_2[z]/(z^{124} + z^{19} + 1)$
- $a = z^{105}$
- $b = z^{108}+z^{106}+z^{102}+z^{101}+z^{99}+z^{93}+z^{87}+z^{85}+z^{75}+z^{70}+z^{68}+z^{67}+z^{66}+ z^{64}+z^{62}+z^{59}+z^{58}+z^{56}+z^{55}+z^{54}+z^{53}+z^{51}+z^{50}+z^{49}+z^{48}+z^{46}+z^{45}+ z^{44}+z^{42}+z^{41}+z^{40}+z^{33}+z^{32}+z^{29}+z^{27}+z^{24}+z^{23}+z^{22}+z^{20}+z^{18}+z^{16}+ z^{15}+z^{14}+z^{9}+z^{8}+z^{7}+z^{6}+z^{3}+z^{2}+z$
- Consider $E/\mathbb{F}_{2^{124}}: \quad y^2 + xy = x^3 + ax^2 + b$.
- $\#E(\mathbb{F}_{2^{124}}) = 2r$ where $r = 10633823966279326985483775888689817121$ is prime.
- Let P, Q be randomly selected points of order r in $E(\mathbb{F}_{2^{124}})$.
- Pollard-rho for finding $\log_P Q$ is infeasible.

Reduction

- Hess's KASH program was used to reduce the ECDLP instance (E, P, Q) to an HCDLP instance (C, D_P, D_Q), where C is the following hyperelliptic curve of genus $g = 31$ over $\mathbb{F}_{2^4}$:
- $\mathbb{F}_{2^4} = \mathbb{F}_2[w]/(w^4 + w + 1)$.
- $f(u) = w^3u^{63} + w^7u^{60} + w^3u^{56} + w^3u^{48} + 1$
- $h(u) = w^9u^{31} + w^{12}u^{30} + w^8u^{28} + w^{13}u^{24} + w^6u^{16} + w^6$
- $C/\mathbb{F}_{2^4}: \quad v^2 + h(u)v = f(u)$.
- $\#J_C(\mathbb{F}_{2^4}) = 2r$.

Smoothness bound selection

t	$F(t)$	$E(t)$	$T(t)$
1	16	$1.15149568 \times 10^{32}$	$2.24181409 \times 10^{32}$
2	64	$6.48579145 \times 10^{15}$	$4.44751961 \times 10^{18}$
3	744	1781948118	1334679140141
4	8872	1498799	13304838571
5	113728	25876	2942900859
6	*1511468	2001	3024499495
7	*20685428	354	7320993345
8	*289116788	103	29880384177

$F(t)$ = factor base size

$E(t)$ = expected number of random walk steps to a smooth relation

$T(t)$ = expected total number of random walk steps

Solving the HCDLP instance

- Smoothness bound: $t = 5$
- Factor base size: 113,728
- Time to generate factor base (800 MHz PII): 12m, 3s
- Average # of iterations per relation: 25,576
- Total CPU time to generate all relations: 397d, 2h, 1m
- Time to solve linear system (800 MHz PII): 3d, 17h, 55m

ECDLP over $\mathbb{F}_{2^{155}}$

For the special class of 2^{34} elliptic curves over $\mathbb{F}_{2^{155}}$ having $m = 6$:

t	$F(t)$	$E(t)$	$T(t)$
1	16	$1.15149568 \times 10^{32}$	$2.24181409 \times 10^{32}$
2	256	4105255075208737	1071471574629480605
3	5712	1549820999	8860326649526
4	136528	1378374	188193560220
5	*3491968	24746	86410841791
6	*92967640	1945	180781004858
7	*2547234664	347	883799233900
8	*71266645874	102	7257807696673

Expected time for an ECDLP computation with $t = 4$ on a single 1GHz PIII workstation: 26,000 days.

Exhaustive search on DES key space: 110,000d on a single 450MHz PII.

Pollard-rho for ECC2-108K challenge: 200,000d on a single 450MHz PII.

Analysis: n composite

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

- Let $b \in \mathbb{F}_{q^n}$ have type $(j_0, j_1, \ldots, j_s)$.
  (i) Then $m(b) = \Sigma_{i=0}^{s} j_i d_i + c$, 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 $\Pi_{i=0, j_i \neq 0}^{s} (q^{j_i d_i} - q^{(j_i - 1) d_i})$.

ECDLP Instances Most Susceptible to GHS Attack

- Maurer, M, Teske (2001)

N	n	l	m	g	I	t	F	T	ρ	D
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	*4*	*41*	*3*	*4*	*123*	*1*	*40*	*45*	*81*	*36*
165	15	11	5	15	58	2	20	37	82	45
166	*2*	*83*	*2*	*2*	*167*	*1*	*82*	*83*	*82*	–
168	7	24	4	7	98	1	23	35	83	48
169	169	1	13	4095	14	28	23	1208	84	–

$E/\mathbb{F}_{2^N}$ is cryptographically interesting.
I: # isomorphism classes of elliptic curves with these GHS parameters.
F: $\log_2$ of factor base size; $F \leq 23$.
T: $\log_2$ of time for HCDLP solution.
ρ: $\log_2$ of time for Pollard-rho.
$D = \rho - T$.

Increasing the Number of Susceptible Curves

- Galbraith, Hess and Smart (2001)
- Two elliptic curves E/K and E'/K are **K-isogenous** if $\#E(K) = \#E'(K)$.
- Given E/K, test if E is K-isogenous to an elliptic curve E'/K having small m value.
- If so, an isogeny $\phi : E \rightarrow E'$ can be determined in expected time $O(q^{n/4+\epsilon})$.
- Then the ECDLP instance in $E(K)$ can be efficiently mapped to the ECDLP instance in $E'(K)$.

Example: Elliptic Curves Over $\mathbb{F}_{2^{155}}$

- $N = 155$, $n = 31$, $l = 5$.
- Let the set of **susceptible elliptic curves** over $\mathbb{F}_{2^{155}}$ be
$$SE(155) = \{E_{0,b},\ E_{1,b}\ :\ b \in \mathbb{F}_{2^{155}},\ m(b) = 6\}.$$
- Then $\#SE(155) \approx 2^{34}$.
- Let $\pi : \alpha \mapsto \alpha^2$. If $m(b) = 6$ then $m(\pi(b)) = 6$, and $\#E_{a,b}(\mathbb{F}_{2^{155}}) = \#E_{a,\pi(b)}(\mathbb{F}_{2^{155}})$. Assume that there are no other isogenous curves in $SE(155)$. Then the number of non-isogenous curves in $SE(155)$ is $\approx 2^{34}/155 \approx 2^{27}$.
- The number of elliptic curves isogenous to these is $\approx 2^{27} \cdot 2^{155/2} \approx 2^{104}$.
- Thus 2^{104} out of 2^{156} elliptic curves succumb to GHS.

Example: Elliptic Curves Over $\mathbb{F}_{2^{161}}$

- $N = 161$, $n = 7$, $l = 8$, $m = 4$, $g = 7$.
- $\#SE(161) \approx 2^{94}$.
- Since there are $2^{81.5}$ isogeny classes of elliptic curves over $\mathbb{F}_{2^{161}}$, we expect that **almost all** elliptic curves over $\mathbb{F}_{2^{161}}$ are isogenous to an elliptic curve in $SE(161)$.
- **Problem:** Given $E/\mathbb{F}_{2^{161}}$, how to find an elliptic curve in $SE(161)$ that is $\mathbb{F}_{2^{161}}$-isogenous to E?

ECDLP Challenges

- Maurer, M, Teske (2001)

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

- **Purpose:** Increase interest in design and implementations of algorithms for solving the HCDLP.
- No financial rewards!

Conclusions

- The GHS attack fails for **all** elliptic curves over $\mathbb{F}_{2^N}$, where $N \in [160, 600]$ is **prime**.
- The GHS attack succeeds for **some** elliptic curves over $\mathbb{F}_{2^N}$, where $N \in [160, 600]$ is **composite**. These curves can easily be avoided in practice.
- The GHS attack does not apply to elliptic curves over large prime fields.
- **Question:** Are there other useful curves which lie on the Weil restriction of E to $\mathbb{F}_q$ that were not constructed by the GHS attack?
- **Question:** Are there faster algorithms for the HCDLP?