An extension of the GHS attack

ECC 2001

F. Hess
University of Bristol

joint work with

S. Galbraith and N. P. Smart
Royal Holloway, London
University of Bristol

Overview

1. Review of the basic GHS attack

2. The extended GHS attack

3. Implications and observations

GHS attack

Let $q = 2^r$ and $E : y^2 + xy = x^3 + ax^2 + b$ with $a, b \in \mathbb{F}_{q^n}$.

GHS attack produces

a hyperelliptic curve $H : y^2 + f(x)y = h(x)$ with $f(x), h(x) \in \mathbb{F}_q[x]$ of genus $g = 2^{m-1}$ or $g = 2^{m-1} - 1$, where m depends on b and $1 \leq m \leq n$.

a homomorphism

$$\phi : E(\mathbb{F}_{q^n}) \longrightarrow \mathrm{Jac}(H)(\mathbb{F}_q).$$

Try to solve $\phi(P) = \lambda\phi(Q)$ instead of $P = \lambda Q$.

Applicability

Does not work

- if m is too small ($b \in$ intermediate field),
- if m is large ($\Rightarrow g$ is too large).

Usually $m = n$, especially for $q = 2$ and n prime.
The value of m is too large for all primes $\in [160, 600]$.
[Men-Qu]

Example:

n	$\approx$ *Prob* small m	g	
7	$4q^{-3}$	7	(+1)
31	$12q^{-25}$	31	(+1)
127	$36q^{-119}$	127	(+1)

Applicability

If m is small, H and images under ϕ can be computed very fast.

Using index calculus algorithms for solving the discrete logarithm in $\mathrm{Jac}(H)(\mathbb{F}_q)$:

- for $n \geq 4$ and $q \to \infty$ an upper time bound is $O(q^{2+\varepsilon})$,
- for q fixed and $n \to \infty$ a “lower bound” is $O(\exp(c\sqrt{\log(q) \cdot n\log(n)}))$.

Construction

U := all possible sums of $x^{-1} + a^{q^i} + b^{q^i/2}x$, $i = 1, \ldots, n$.

$f(x) \in U$: $F_{f(x)} := \mathbb{F}_{q^n}(x, y)$ where $y^2 + y = f(x)$.

$\mathbb{F}_{q^n}(E) \cong F_{x^{-1}+a+b^{1/2}x}$.

Combine all $F_{f(x)}$ to one F_U.

F_U is a hyperelliptic function field of genus 2^{m-1} or $2^{m-1} - 1$, $m = \dim \operatorname{span}_{\mathbb{F}_2}\{(1, b^{q^i}) : i = 1, \ldots, n\}$.

n odd, $n = m$ or $\mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_2}(a) = 0$
$\Rightarrow F_U \cong \mathbb{F}_{q^n}(H)$ for a hyperelliptic curve H defined over $\mathbb{F}_q$.

Construction

$E(\mathbb{F}_{q^n}) \cong \mathrm{Cl}^0(\mathbb{F}_{q^n}(E)),\ \mathrm{Jac}(H)(\mathbb{F}_q) \cong \mathrm{Cl}^0(\mathbb{F}_q(H)).$

More general $f(x) \in U$:

$$\begin{array}{rcl} \phi_{f(x)} : \mathrm{Cl}^0(F_{f(x)}) & \longrightarrow & \mathrm{Cl}^0(\mathbb{F}_q(H)), \\ D & \longmapsto & N_{\mathbb{F}_{q^n}(H)/\mathbb{F}_q(H)}(Con_{\mathbb{F}_{q^n}(H)/F_{f(x)}}(D)) \end{array}$$

Example:

$q = 2,\ n = 127.\ \mathbb{F}_{q^n} = \mathbb{F}_2[w]/(1 + w + w^{127}).$

$E : y^2 + xy = x^3 + w$

$\Rightarrow H : y^2 + (x^{128} + x^{64} + x)y + x^{128} + x^{64} + x = 0.$

$m = 8,\ g = 127.$

Some new formulas

$\sigma :=$ q-th power Frobenius on $\mathbb{F}_{q^n}(H)$.

$f(x) = x^{-1} + \alpha + \beta x \in U$: $s_{f(x)} := \min\{s \geq 1 \mid \sigma^s(\beta) = \beta\}$.

$\Rightarrow$ $\sigma^{s_{f(x)}}$ Frobenius automorphism of $F_{f(x)}$.

Let $U' := (U / U \cap \mathbb{F}_{q^n}) // \langle\sigma\rangle$ (representatives).

$$\boxed{\chi_{\sigma \mid \mathbb{F}_q(H)}(t) = \prod_{\overline{f(x)} \in U'} \chi_{\sigma^{s_{f(x)}} \mid F_{f(x)}}(t^{s_{f(x)}}).}$$

$\boxed{g = 2^{m-1} - 1 \;\Leftrightarrow\; \mathrm{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_{q^u}}(b) = 0}$ where $u = 2^{v_2(n)}$.

$$\boxed{\ker(\phi_{f(x)}) \subseteq N^{-1}_{F_{f(x)}/Fix(\sigma^{s_{f(x)}}|F_{f(x)})}(\mathrm{Cl}^0(Fix(\sigma^{s_{f(x)}}|F_{f(x)}))[2^m]).}$$

$\Rightarrow$ $b \notin$ intermediate field then kernel small.

Extending the GHS attack

An isogeny $\psi : E \longrightarrow E_1$ maps

$$P = \lambda Q \quad \text{to} \quad \psi(P) = \lambda\,\psi(Q).$$

<u>Basic idea:</u>

> If E is not well suited for the GHS attack, maybe E_1 is.

Example I

$q := 2^5$, $n := 31$. $\mathbb{F}_q = \mathbb{F}_2[u]/(1+u^2+u^5)$,

$$\mathbb{F}_{q^n} = \mathbb{F}_2[w]/(1+w^{62}+w^{155}).$$

$$E : y^2+xy = x^3 + \left(\begin{array}{l} w^{154}+w^{152}+w^{149}+w^{147}+w^{145}+w^{144}+w^{141}+w^{140}+w^{136}+ \\ w^{135}+w^{133}+w^{132}+w^{129}+w^{126}+w^{119}+w^{117}+w^{113}+w^{110}+ \\ w^{109}+w^{105}+w^{101}+w^{98}+w^{97}+w^{96}+w^{93}+w^{90}+w^{85}+w^{84}+ \\ w^{82}+w^{81}+w^{80}+w^{78}+w^{77}+w^{76}+w^{74}+w^{73}+w^{72}+w^{66}+ \\ w^{65}+w^{61}+w^{56}+w^{55}+w^{52}+w^{50}+w^{46}+w^{45}+w^{43}+w^{42}+ \\ w^{38}+w^{36}+w^{35}+w^{34}+w^{33}+w^{30}+w^{28}+w^{26}+w^{24}+w^{22}+ \\ w^{19}+w^{18}+w^{17}+w^{16}+w^{15}+w^{11}+w^{10}+w^{8}+w^{5}+w^{3}+w^{2}+1 \end{array}\right),$$

GHS $\Rightarrow$ $m = 31$ and $g = 2^{m-1} - 1 = 1073741823$.

$$E_1 : y^2+xy = x^3 + (w^{140}+w^{109}+w^{95}+w^{78}+w^{70}+w^{64}+w^{47}+w^{35}+w^{33}+w^{8}+w^{4}),$$

$E_1 \cong_7 E$ and GHS $\Rightarrow$ $m = 6$, $g = 2^{m-1} - 1 = 31$.

$$\begin{aligned} H :\ & y^2+(u^{22}x^{31}+u^{13}x^{30}+u^{12}x^{28}+u^{18}x^{24}+u^{8}x^{16}+u^{25})y+ \\ & u^{13}x^{63}+u^{4}x^{62}+u^{3}x^{60}+u^{9}x^{56}+u^{30}x^{48}+u^{16}x^{32} = 0. \end{aligned}$$

Example II

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

$E : y^2 + xy = x^3 + 1 \Rightarrow$ GHS does not work.

$E_1 : y^2 + xy = x^3 + w^7$,
$E_1 \cong E$ and GHS $\Rightarrow m = 4$, $g = 2^{m-1} = 8$.

$H : y^2 + (x^8 + x^4 + x)\,y + x^{17} + x^{13} + x^8 + x = 0.$

$\chi_{\sigma^n|\mathbb{F}_{q^n}(E_1)}(t) = t^2 - 13t + 128,$
$\chi_{\sigma|\mathbb{F}_q(H)}(t) = (t^2 + t + 2)(t^{14} - 13t^7 + 128).$

Strategy

Input: $E,\ N$

Output: E_1 and $\psi : E \to E_1$, or failure.

1. Check whether suitably small m can be obtained.
   Find N elliptic curves E_1 with small m-value.

2. Check whether $\#E_1(\mathbb{F}_{q^n}) = \#E(\mathbb{F}_{q^n})$ for some E_1.

3. Determine the isogeny $\psi : E \to E_1$.

Finding small m

From now on r, n odd and n prime.

Over $\mathbb{F}_2$ we have $x^n - 1 = (x-1)f_1 \cdots f_s$ and $\deg(f_i) = t$.

Let

$\alpha \in \mathbb{F}_{q^n}$ be a normal basis element over $\mathbb{F}_2$,

$\sigma : x \mapsto x^q$,

$g_i(x) = (x^n - 1)/((x-1)f_i)$,

$\alpha_i = g_i(\sigma)\alpha$,

$B_i = \{u(\sigma)\alpha_i : u(x) \in \mathbb{F}_q[x], \deg(u(x)) \leq t+1\}$,

$B = \bigcup_{i=1}^{s} B_i \backslash \mathbb{F}_q$.

Then $N \leq \#B = qs(q^t - 1)$ and E has $m = t+1$ iff $b \in B$.

Finding small m

Improvements:

For $b \in B$ don't use conjugates b^{2^i}
$\Rightarrow \approx sq^{t+1}/(nr)$ small m elements.
$\Rightarrow N = O(sq^{t+1}/(nr))$.

Testing of the elliptic curves E_1 can be done in parallel.

Finding the isogeny

Building on earlier work of [Gal], uses ideas of [Koh, Cou, Ler].

Input: Isogenous E_1, E_2

Output: $\psi : E_1 \to E_2$

1. Find isogenous E_i' such that $O = \mathrm{End}(E_i')$ is the maximal order in $\mathrm{End}(E_i) \otimes \mathbb{Q}$. Find an isogeny $\psi_i : E_i \longrightarrow E_i'$. [Koh]

2. Use a random walk on j-invariants resp. in $\mathrm{Pic}(O)$ to determine an ideal $\mathfrak{a}$ of O corresponding to an isogeny $E_1' \longrightarrow E_2'$.

Finding the isogeny

3. Smooth the ideal modulo principal ideals, using ideas from index calculus.

4. Determine the isogeny $\psi' : E_1' \longrightarrow E_2'$ from the smooth ideal. Return $\psi_1 \psi' \hat{\psi}_2 : E_1 \longrightarrow E_2$.

Complexity:

- Average case time $O(q^{n/4+\varepsilon})$,
- average case space $O(\exp(c\sqrt{\log(q^n)\log(\log(q^n))}))$.
- Worst case time $O(q^{3n/2+\varepsilon})$.

Running time

Step 1: Finding N small m elements
takes time $N = O(sq^{(n-1)/s+1}/(nr))$.

Step 2: $N = O(sq^{(n-1)/s+1}/(nr))$ "point countings"
on elliptic curves over $\mathbb{F}_{q^n}$ (only check that
random point on E_1 has order $\#E(\mathbb{F}_{q^n})$ ...).

Step 3: Finding the isogeny on average $O(q^{n/4+\varepsilon})$.

$\Rightarrow \boxed{T_{\mathrm{ext}}(N) = N + O(q^{n/4+\varepsilon})}$ "operations".

$\Rightarrow \boxed{T_{\mathrm{ext}}^{\max} = O(sq^{(n-1)/s+1}/(nr) + q^{n/4+\varepsilon})}$ "operations".

Success probability

What is the probability $Pr_{ext}(N)$ that there is one out of N non-conjugate small m curves E_1 in the isogeny class of any given curve E?

Number of isogeny classes $\approx 2q^{n/2}$.
Assume " $N \lll\ggg 2q^{n/2}$ ".

<u>Heuristic assumption:</u> Small m curves E_1 distribute over isogeny classes like arbitrary curves E.

$$\Rightarrow \quad \boxed{Pr_{\text{ext}}(N) \approx \min\{\, 1, N/(2q^{n/2})\,\}}$$

$$\Rightarrow \quad \boxed{Pr_{\text{ext}}^{\max} \approx \min\{\, 1, sq^{(n-1)/s+1-n/2}/(nr)\,\}}$$

Implications

Values $n = st + 1$ for n prime ($g = 2^t, 2^t - 1$).

n	t	s	n	t	s	n	t	s
5	4	1	43	14	3	101	100	1
7	**3**	**2**	47	23	2	103	51	2
11	10	1	53	52	1	107	106	1
13	12	1	59	58	1	109	36	3
17	**8**	**2**	61	60	1	113	28	4
19	18	1	67	66	1	**127**	**7**	**18**
23	**11**	**2**	71	35	2	131	130	1
29	28	1	**73**	**9**	**8**	137	68	2
31	**5**	**6**	83	82	1	139	138	1
37	36	1	**89**	**11**	**8**	149	148	1
41	20	2	97	48	2	151	15	10

Implications

$\boxed{s = 1:}$ $Pr_{\text{ext}}^{\max} = 1$.

$\boxed{s = 2:}$ $Pr_{\text{ext}}^{\max} \approx \min\{\,1,\, q^{1/2}/(nr)\,\} \to 1$ for $q \to \infty$.

$\boxed{s = 2,\ n = 7:}$ Gaudrys algorithm on genus 7 or 8 is practical and runs in time $O(q^{2+\varepsilon})$!

$n = 7$	q	2	2^2	2^3	2^4	2^5	$\ldots$	2^{10}	2^{11}
Formula $Pr_{\text{ext}}^{\max}$		0.404	0.286	0.269	0.286	0.323	$\ldots$	0.914	1.0
Actual $Pr_{\text{ext}}^{\max}$		0.470	0.290	0.280	≈ 0.285	≈ 0.331	–	–	–

Implications

$\boxed{s \geq 3:}$ $Pr_{\text{ext}}^{\max} \to 0$ with $q \to \infty$.

Number of curves $\approx 2q^n$.

Basic GHS: $Pr_{\text{basic}} = sq^{(n-1)/s+1-n}$

Extended GHS: $Pr_{\text{ext}}^{max} = sq^{(n-1)/s+1-n/2}/(nr)$

$\Rightarrow$ Probability improved by $\boxed{Pr_{\text{ext}}^{\max}/Pr_{\text{basic}} = q^{n/2}/(nr).}$

$\boxed{s = 6,\ n = 31,\ q = 2^5:}$ Feasible parameters according to [Jac, Men, Ste]. $Pr_{\text{basic}} \approx 2^{-122}$, $Pr_{\text{ext}}^{\max} \approx 2^{-52}$

31 days on 500 Mhz Pentium $\Rightarrow$ IPSEC curve not subject to extended GHS attack.

Observation I

Extended GHS works with high probability for subfield curves E if isogenous to non subfield curve E_1.

Replace $\mathbb{F}_{q^n}$ by $\mathbb{F}_{q^{nl}}$ $\Rightarrow$ more small m elements.

n	m	$\#b$	l	m	new $\#b$
17	9	$2q(q^8-1)$	15	9	$28q(q^8-1)$
31	6	$6q(q^5-1)$	11	11	$30q(q^{10}-1)$
73	10	$8q(q^9-1)$	7	10	$48q(q^9-1)$

Try upstairs to find isogenous curve.

Observation II

$|I|$:= cardinality of the isogeny class I of E.
$\#b$:= number of small m elements.

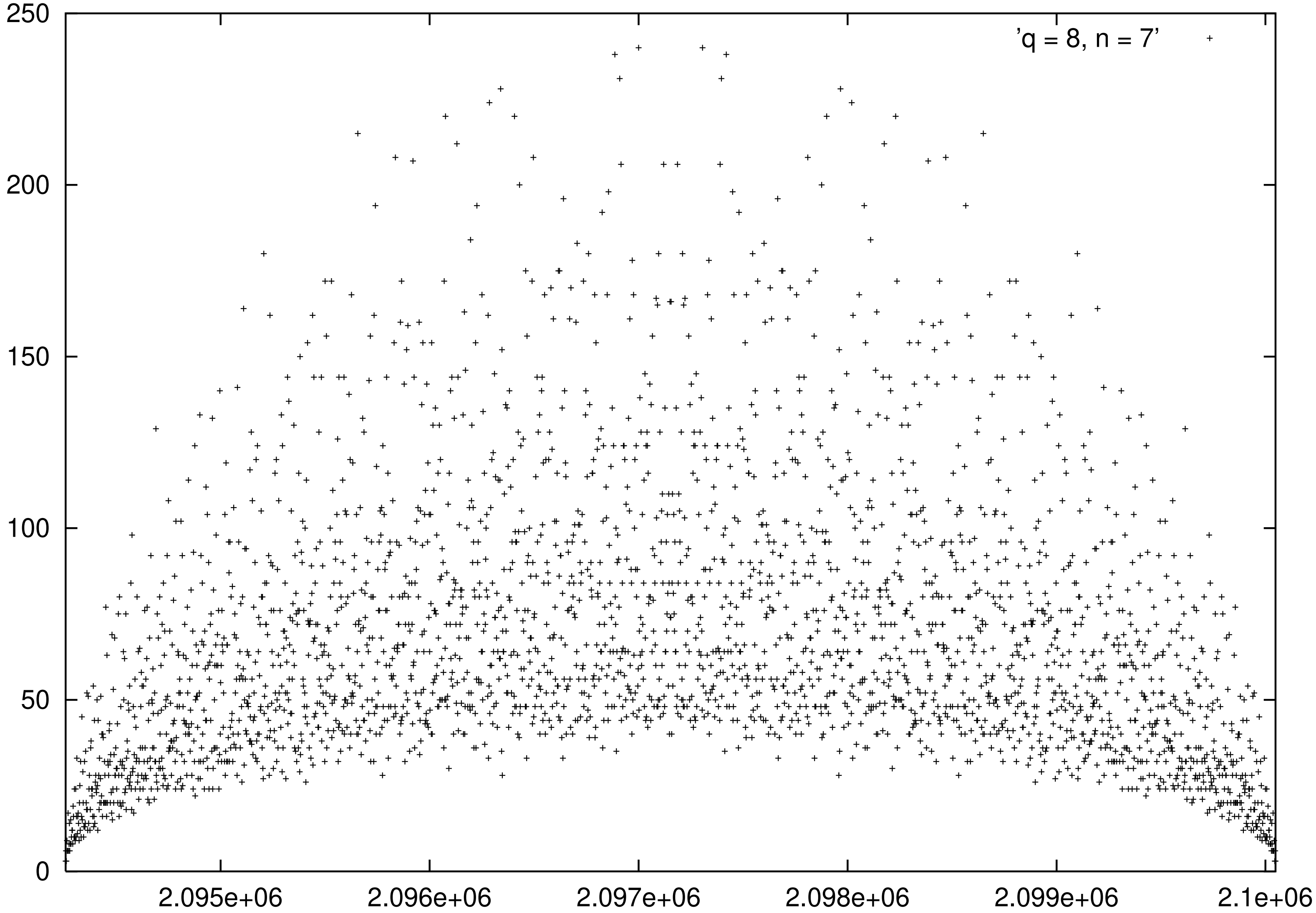
$\#b$ can be very large (ANSI X.962 E176: $\approx 2^{110}$) ...

If $|I| < \#b$ then it could be better to compute all isogenous curves and test for a small m curve.

Are there exceptionally small isogeny classes?
Not really ...

x-axis: isogeny classes I,
y-axis: cardinality $|I|$ scaled by constant factor.

Distribution



Conclusions

We have given some new formulas for the basic GHS attack.

We have extended the basic GHS attack so that the success probability is heuristically considerably higher at added cost.

We have discussed some implications.

We have mentioned further possible improvements.

Curves over $\mathbb{F}_{2^p}$ and $\mathbb{F}_p$ are immune.