The GHS Attack Revisited

ECC 2003

Florian Hess
University of Bristol

Overview

1. General attack philosophy
2. The new construction for elliptic curves in characteristic 2
3. Combination with isogenies
4. Conclusion

Curves and discrete logarithms

$q = p^r$, $k = \mathbb{F}_q$, C_0 algebraic curve over k of genus g.
Divisor class group $\mathrm{Pic}_k^0(C_0)$ contains DLP.

$\#\mathrm{Pic}_k^0(C_0) \approx q^g$.

If $g \geq 4$ the DLP can be solved faster using index calculus than with Pollard methods.

Index calculus:

- g fixed, $q \to \infty \Rightarrow$ time $\approx O(q^{2g/(g+1)})$,
- q fixed, $g \to \infty \Rightarrow$ time $\approx O(q^{\sqrt{g}})$.

Pollard: Time $\approx O(q^{g/2})$.

General attack philosophy

"Weil descent methodology" or "covering attacks".

$K = \mathbb{F}_{q^n}$, E elliptic curve (function field) over K.

$$\begin{tikzcd}
 & C \arrow[dl, no head] \arrow[dr, no head] & & {} \arrow[r, bend left] & {} & & \mathrm{Pic}^0_K(C) \arrow[dr, "\mathrm{N}"] & \\
E & & C_0 & & & \mathrm{Pic}^0_K(E) \arrow[ur, "\mathrm{Con}"] & & \mathrm{Pic}^0_k(C_0)
\end{tikzcd}$$

C extension of E,

U automorphism group with Frobenius, $C_0 = C^U$ fixed field,

$\phi : \mathrm{Pic}^0_K(E) \to \mathrm{Pic}^0_k(C_0)$, $\phi(x) = \mathrm{N}_{C/C_0}(\mathrm{Con}_{C/E}(x))$.

$Q = \lambda P \Rightarrow \phi(Q) = \lambda\phi(P)$.

General attack philosophy

Questions:

1. How construct C and U?
2. ϕ preserves the DLP?
3. Genus of $C_0 = C^U$ small?

Ad 1: Obtain C as splitting field of $E/k(x)$, $x \in E$.

- Use Artin-Schreier extensions, $(p = 2)$
- Use Kummer extensions. $(p > 2)$

Ad 2, 3: Some general statements in the paper.

Basic GHS attack: Uses Artin-Schreier extensions, yields hyperelliptic C_0.

The new construction

$p = 2, \;\; f = \gamma/x + \alpha + \beta x \; \in K(x)$.

Use normalisation $\alpha \in \{0, \omega\}$ with $\mathrm{Tr}_{K/\mathbb{F}_2}(\omega) = 1$.

Artin-Schreier equation $E_f : y^2 + y = f = \gamma/x + \alpha + \beta x$.
Associated $E : Y^2 + XY = X^3 + aX^2 + b$ with $a = \alpha$ and $b = (\gamma\beta)^2$.

Take $C = K(x, y_0, \ldots, y_{n-1})$ where $y_i^2 + y_i = \gamma^{q^i}/x + \alpha^{q^i} + \beta^{q^i} x$.

Using the y_i is necessary in order to have a Frobenius automorphism on C fixing x.

C_0 is then the fixed field of this Frobenius automorphism.

The new construction

$m_z = \sum_{i=0}^{m} \lambda_i t^i \in \mathbb{F}_2[t]$ of minimal degree such that $\sum_{i=0}^{m} \lambda_i z^{q^i} = 0$.

$$m_f = \begin{cases} \mathrm{lcm}(m_\gamma, m_\beta) & \mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0, \\ \mathrm{lcm}(m_\gamma, m_\beta, t+1) & \text{otherwise.} \end{cases}$$

Then $m_f \mid (t^n + 1)$.

Construction works $\Leftrightarrow$ $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$ or $\mathrm{Tr}_{K/k}(\gamma) \neq 0$ or $\mathrm{Tr}_{K/k}(\beta) \neq 0$.

1. $g_{C_0} = 2^{\deg(m_f)} - 2^{\deg(m_f) - \deg(m_\gamma)} - 2^{\deg(m_f) - \deg(m_\beta)} + 1$.
2. If $K = k(\gamma, \beta)$ then DLP is preserved, $2^{\deg(m_f)-1} \ker(\phi) = 0$.
3. If $\gamma \in k$ or $\beta \in k$ then C_0 hyperelliptic.
4. Formula for characteristic polynomial of Frobenius.

Example

$q := 2^5$, $n := 31$. $\mathbb{F}_q = \mathbb{F}_2[u]/(1+u^2+u^5)$, $\mathbb{F}_{q^n} = \mathbb{F}_2[w]/(1+w^{62}+w^{155})$.

$$E_f : y^2 + y = 1/x + \begin{pmatrix} w^{148}+w^{141}+w^{140}+w^{136}+w^{134}+w^{132}+w^{129}+w^{128}+w^{117}+w^{113}+ \\ w^{111}+w^{109}+w^{102}+w^{101}+w^{98}+w^{97}+w^{95}+w^{86}+w^{82}+w^{80}+w^{70}+ \\ w^{67}+w^{66}+w^{65}+w^{64}+w^{51}+w^{47}+w^{43}+w^{41}+w^{37}+w^{18}+w^{10}+w^{8} \end{pmatrix} x,$$

$\Rightarrow \deg(m_\gamma) = 1$, $\deg(m_\beta) = 15$, $m_f = m_\gamma m_\beta$, $g_{C_0} = 2^{16} - 2^{15} - 2^1 + 1 = 32767$.

$$x \mapsto x / \begin{pmatrix} w^{132}+w^{128}+w^{125}+w^{101}+w^{97}+w^{66}+ \\ w^{64}+w^{63}+w^{39}+w^{35}+w^{33}+w^{8}+w^{4}+w^{2} \end{pmatrix} :$$

$$E_f' : y^2 + y = \begin{pmatrix} w^{132}+w^{128}+w^{125}+w^{101}+w^{97}+w^{66}+ \\ w^{64}+w^{63}+w^{39}+w^{35}+w^{33}+w^{8}+w^{4}+w^{2} \end{pmatrix} / x + \begin{pmatrix} w^{140}+w^{132}+w^{128}+w^{125}+w^{101}+w^{94}+ \\ w^{78}+w^{70}+w^{64}+w^{63}+w^{47}+w^{39}+w^{35} \end{pmatrix} x$$

$\Rightarrow m_f = m_\gamma = m_\beta$, $\deg(m_f) = 5$, $g_{C_0} = 2^5 - 2^0 - 2^0 + 1 = 31$.

$$C_0 : y^{32} + u^{22}y^{16} + u^{28}y^8 + u^{18}y^4 + y^2 + u^{16}y + (x^{32} + x^{24} + u^{10}x^{20} + u^{28}x^{18} + u^9x^{17} + u^{17}x^{15} + u^3x^{14} + u^{17}x^{12} + u^{20}x^8 + u^{28})/x^{16} = 0.$$

Remarks

Possible m_γ, m_β correspond to divisors of $t^n - 1 \bmod 2$.
If n prime then degrees of m_γ, m_β often $\geq n-1$.

Basic GHS is the subcase $\gamma = 1$.

Number of E subject to attack is roughly the square of the previously attackable E.

C_0 is not necessarily hyperelliptic anymore ...

There is a program to compute C_0 efficiently.

The characteristic polynomial of Frobenius can be used for the smoothness estimations in index calculus.

Applying the new construction

Assume n odd prime.

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

Number of β with $m_\beta = f_i$ for some i is $s(q^d - 1)$. Similarly for γ.

Number of β with $m_\beta = (t-1) f_i$ for some i is $s(q-1)(q^d-1)$.

g_{C_0}	$\approx \#\{\gamma\beta\}$	α	m_γ	m_β
$2^d - 1$	$\min\{q^n, sq^{2d-1}/2\}^\dagger$	0	f_i	f_i
$2^d - 1$	sq^d	$0, \omega$	$t-1$	f_i
2^d	$s(q-1)q^d$	$0, \omega$	$t-1$	$(t-1) f_i$

† = heuristically expected,

$(\gamma, \beta) \mapsto \gamma\beta$ is $\geq 2(q-1)$-to-1 map. $(\gamma\beta = \beta\gamma,\ (\lambda\gamma)(\lambda^{-1}\beta) = \gamma\beta$ for $\lambda \in k^\times$.)

Applying the new construction

Given E, how can we find a suitable decomposition $b = \gamma\beta$?

1) n odd prime.

If $f_i = t^{r_1} + t^{r_2} + 1$ then γ, β with $m_\gamma = m_\beta = f_i$ can be found efficiently:

- Solve for ρ such that $b^{q^{r_1}} + b^{q^{r_2}}(\rho+1)/\rho + b(\rho+1) = 0$.
- Compute $\tau = \rho^\lambda$ where $\lambda(q^{r_2}-1)/(q-1) \equiv 1 \bmod q^n - 1$.
- Solve for γ such that $\gamma^{q-1} = \tau$ using Lagrange's resolvent.

No or $2(q-1)$ solutions for $m_b \nmid f_i$.

Example: $n = 7$, $t^n - 1 = (t-1)(t^3+t+1)(t^3+t^2+1)$, $d = 3$, $s = 2$.
A proportion of about q^{-2} of all E with $\alpha = 0$ leads to $g_{C_0} = 7$.

Applying the new construction

2) n composite, $n = n_1 n_2$ and $\mathrm{Tr}_{K/K_1}(b) \neq 0$ where $K_1 = \mathbb{F}_{q^{n_1}}$.

Observations:

i) $\gamma = \mathrm{Tr}_{K/K_1}(b)$, $\beta = b/\gamma$. Then $m_\gamma \,|\, (t^{n_1} - 1)$ and $m_\beta \,|\, (t-1)(t^n - 1)/(t^{n_1} - 1)$.

ii) $m_1 \,|\, (t^{n_1} - 1)$ and $m_2 \,|\, (t-1)(t^n - 1)/(t^{n_1} - 1)$.

Then $\#\{\gamma\beta \,|\, m_\gamma = m_1$ and $m_\beta = m_2\} = \mathrm{Phi}(m_1)\mathrm{Phi}(m_2)/(q-1)$.

iii) $k(b) = k(\gamma, \beta)$, and $\mathrm{Tr}_{K/k}(\beta) \neq 0$ iff n_1 odd.

Example (cf. Menezes-Teske-Weng): $n = 6$, $n_1 = 3$, $n_2 = 2$.

Every E over $\mathbb{F}_{q^6}$ with $\mathrm{Tr}_{\mathbb{F}_{q^6}/\mathbb{F}_{q^3}}(b) \neq 0$ leads to $g_{C_0} \in \{8, 9, 11, 12, 14\}$.

Using isogenies

An isogeny $\psi : E \longrightarrow E_1$ maps $P = \lambda Q$ to $\psi(P) = \lambda\,\psi(Q)$.
Use E_1 in place of E in the attack ...

Problems: Does ”weak” E_1 exist? How find ψ?

Strategy 1:
Create all E_f and ”weak” E_1. Check $\#E_1(K) = \#E(K)$. Compute ψ.
Time $\approx \#\{E_1\} + O(q^{n/4+\varepsilon})$ (on average).

Strategy 2:
Random walk in isogeny class of E, yields some E_1 and ψ. Check whether E_1 is ”weak”.

Using isogenies

View from other perspective:

If E_1 is ”weak” then all E isogenous to E_1 ”weak” too.

Number of isogeny classes $\approx 2q^{n/2}$.

Expect that random E lies in isogeny class of some given ”weak” E_1 with probability $\approx 1/(q^{n/2}nr)$.

$q = 2^r$, n odd prime. $t^n - 1 = (t-1)f_1 \cdots f_s$, $\deg(f_i) = d$.

A proportion of $\min\{1, sq^{2d-1}/(2q^{n/2}nr)\}$ among all E with $\alpha = 0$ is expected to lead to C_0 with $g_{C_0} = 2^d - 1$ and equivalent DLP.

Using isogenies

Example:

$n = 31$, $r = 5$: IPSec curve with $\alpha = 0$ in $\mathbb{F}_{2^{155}}$.

Here $d = 5$, $s = 6$ and $g_{C_0} = 31$.

Success probability $\approx 2^{-37}$. Time using strategy 1 is $\approx 2^{40}$.

Previous success probability: $sq^{d+1}/(q^{n/2}nr) \approx 2^{-52}$.

Example:

$n = 7$, $d = 3$, $s = 2$. Expect that using strategy 2 and a random walk of length $\approx q^2$ yields a ”weak” E_1 and $g_{C_0} = 7$.

Further Observations

Using a different rational function $f = \gamma/x + \alpha + \beta x$ is possible but gives worse genera.

Iterative descent: $n = n_1 n_2$, $n_1 \approx n_2$.
Descent for n_1 and then n_2 yields subexponential genus $\approx 2^{(2+o(1))\sqrt{n}}$.
Apparently no practical implications.

Consider subfields of $C_0 = C^U$ or bigger U. We do not expect improvements but there could be isolated cases ...

Different constructions?

Conclusions

We have generalised the basic construction of the GHS attack
so that it applies to more curves.

Some composite field extensions are considerably weakened.

We have not found further useful generalisations of the construction
but we have not proven that they do not exist.

Curves over $\mathbb{F}_{2^p}$ and $\mathbb{F}_p$ are not susceptible.