

$P, Q \in E(\mathbf{F}_q)$, $Q = nP$ ((large prime order) ((ECDLP is given E, P, Q , find n)). Say \exists hom'm $\phi : E(\mathbf{F}_q) \rightarrow G$. Then $n(\phi(P)) = \phi(Q)$. Good if i) ϕ fast ii) $\phi(P) \neq 0$, iii) the DLP in G is easier. The GHS attack (Gaudry, Hess, Smart) does this (sometimes) when $q = p^r$ with $r \geq 2$. Real life: $q = 2^r$, $r \geq 163$.

((GHS attack involves hyperelliptic curves))

Let $K = \mathbf{F}_{2^r}$ and $C/K : y^2 + h(x)y = f(x)$ with $\deg(f) = 2g+1$ and $\deg(h) \leq g$ and C non-sing away from ∞ . (Can have $\deg(f(x)) = 2g + 2$.)

Called a hyperelliptic curve of genus g . E.g. $y^2 + xy = x^5 + 1$ over \mathbf{F}_2 with genus 2. ((Note an elliptic curve has genus 1. Lines and conic sections have genus 0.))

((Group G is Jacobian of hyperelliptic curve, involves divisors.))
 $3(1, 1) - 2\infty$ has deg 1. End E.g.

$\text{Div}^0(C)$ is group of degree 0 divisors and $\text{Div}^0(C)(K)$, those fixed by $\pi_K = \pi_{2^r}$ (Frobenius). E.g. If $y=0$ get $0 = x^5 + 1 = (x + 1)(x^4 + x^3 + x^2 + x + 1)$. Let α gen $\mathbf{F}_{2^4}^*$, a cyclic group of order 15. Then $\{\alpha^{3i} \mid 0 \leq i \leq 4\}$ are the five elements of $\overline{\mathbf{F}}_2$ satisfying $x^5 + 1 = 0$. Note $\alpha^{15} = 1$. The divisor $(\alpha^3, 0) + (\alpha^6, 0) + (\alpha^9, 0) + (\alpha^{12}, 0) - 4\infty \in \text{Div}^0(C)(\mathbf{F}_2)$. End E.g.

A principal divisor (divisor of fcn) must have deg 0. E.g. $\text{div}(y/x) = (1, 0) + (\alpha^3, 0) + \dots + (\alpha^{12}, 0) - 2(0, 1) - 3\infty$. End E.g.

Let $J(C) = \text{Div}^0(C)/\text{Princ}(C)$ and
 $J(C)(K) = \text{Div}^0(C)(K)/\text{Princ}(C)(K)$.

Every divisor class in $J(K)$ can be represented $[P_1 + \dots + P_g - g\infty]$. E.g. $[2(1, 0) + (\alpha^3, 0) + \dots + (\alpha^{12}, 0) - (0, 1) - 5\infty] = [(0, 1) + (1, 0) - 2\infty]$ End E.g.

Adleman, DeMarrais, Huang: ((imprecise)) Let C be a hyper'c of large genus g over a small \mathbf{F}_q . Can solve DLP in $J(\mathbf{F}_q)$ in time

subexponential in $\log(\#J(\mathbf{F}_q)) \approx \log(q^g)$ using an index calculus method where factor base consists of irred $[D - n\infty]$ where $\deg(D) = n \ll g$ ((and D is fixed by \mathbf{F}_q -Frobenius)). E.g. Factor $[(0, 1) + (\alpha^3, 0) + \dots + (\alpha^{12}, 0) - 5\infty]$ as $[(0, 1) - \infty] + [(\alpha^3, 0) + \dots + (\alpha^{12}, 0) - 4\infty]$ End E.g. ((Note this doesn't help with ECDLP for $E(\mathbf{F}_{2^r})$ for $r \geq 163$ since genus small, finite field large.))

$E(\mathbf{F}_{2^r}) \rightarrow J(C)(\mathbf{F}_2)$. ((Write ECDLP below left)). How to get C for E .

Associate to E and $\mathbf{F}_{2^r}/\mathbf{F}_2$ the Weil restriction W over \mathbf{F}_2 of dimension r .

New E.g. Let α be a root of $x^2 + x + 1 = 0$ over \mathbf{F}_2 . So $\alpha \in \mathbf{F}_{2^2} = \{a_0 + a_1\alpha \mid a_i \in \mathbf{F}_2\}$. Define $E/\mathbf{F}_4 : y^2 + xy = x^3 + \alpha$. Note $(0 + 1\alpha, 1 + 1\alpha) \in E(\mathbf{F}_4)$. ((How to find points? Software doesn't like to deal with α)) A point $(x_0 + x_1\alpha, y_0 + y_1\alpha) \in E(\mathbf{F}_4)$ (for $x_i, y_i \in \mathbf{F}_2$) iff $(y_0 + y_1\alpha)^2 + (x_0 + x_1\alpha)(y_0 + y_1\alpha) = (x_0 + x_1\alpha)^3 + \alpha$ or $(x_1x_0^2 + x_1^2x_0 + y_1x_0 + y_0x_1 + y_1x_1 + y_1^2 + 1)\alpha + (x_0^3 + x_1^2x_0 + y_0x_0 + x_1^3 + y_1x_1 + y_0^2 + y_1^2) = 0$. Since $x_i, y_i \in \mathbf{F}_2$, that is 0 iff $(x_1x_0^2 + x_1^2x_0 + y_1x_0 + y_0x_1 + y_1x_1 + y_1^2 + 1) = 0$ and $(x_0^3 + x_1^2x_0 + y_0x_0 + x_1^3 + y_1x_1 + y_0^2 + y_1^2) = 0$. Let these two equations define W . Have bijection $W(\mathbf{F}_2) \rightarrow (E \setminus 0)(\mathbf{F}_4)$ sends $(0, 1, 1, 1) \mapsto (0 + 1\alpha, 1 + 1\alpha)$. ((These two equations define a variety of dimension 2 ($= r$).))

Intersect W with $x_0 = 0$, we get a hyper'c (non-obvious, isomorphic to $v^2 + (u^3 + 1)v = u^8 + u^4 + u^2 + u$) of genus 3. End E.g.

GHS: Intersect W with $x_0 = 0, x_1 = 0, \dots, x_{r-2} = 0$ ($(r - 1$ hyperplanes)) and get a hyper'c curve C of high genus g over \mathbf{F}_2 ((a small field)). So from ADH, there's algorithm to solve DLP in $J(C)(\mathbf{F}_2)$, subexponential in $\log(2^g)$, which may be faster than Pollard's ρ for ECDLP in $E(\mathbf{F}_{2^r})$ in time exponential in $\log(2^r)$. Generically $g = O(2^r)$. Need $g \leq r^2$; sometimes happens.

Homomorphism: Need hom'm: $\phi : E(\mathbf{F}_{2^r}) \rightarrow J(C)(\mathbf{F}_2)$. Well $C \hookrightarrow W \rightarrow E$. Compose $m : C \rightarrow E$.

E.g. $m(x_0, x_1, y_0, y_1) = (x_0 + x_1\alpha, y_0 + y_1\alpha) \in E \setminus 0$. End E.g.

Have hom's: $E(\mathbf{F}_{2^r}) \xrightarrow{P \mapsto [P-0]} J(E)(\mathbf{F}_{2^r}) \xrightarrow{m^{-1}} J(C)(\mathbf{F}_{2^r}) \xrightarrow{\text{Trace}} J(C)(\mathbf{F}_2)$.
Induced by $\text{Trace}(P) = \pi_2^0 P + \pi_2^1 P + \dots + \pi_2^{r-1} P$.

E.g. Let $C = W \cap (x_0 = 0)$. Note $(\alpha, 1) \in E(\mathbf{F}_4) \mapsto [(\alpha, 1) - 0] \in J(E)(\mathbf{F}_4)$. Now ((next apply m^{-1} , don't know how on 0 so)) $[(\alpha, 1) - 0] = [(\alpha, \alpha + 1) - (0, \alpha + 1)]$. ((Have $m : C \rightarrow E$ by $m(x_0, x_1, y_0, y_1) = (x_0 + x_1\alpha, y_0 + y_1\alpha)$.) Find $m^{-1}((\alpha, \alpha + 1))$. Need $x_0 + x_1\alpha = \alpha$ on C where $x_0 = 0$ so $x_1 = 1$. Get $y_0 + y_1^2 + y_1 + 1 = 0$, $y_0^2 + y_1^2 + y_1 + 1 = 0$. So $y_0^2 = y_0$, $0 = y_0^2 + y_0 = y_0(y_0 + 1)$ and $y_0 = 0$ or $y_0 = 1$. If $y_0 = 0$ then $0 = y_1^2 + y_1 + 1$. If $y_0 = 1$ then $0 = y_1^2 + y_1$ So $m^{-1}((\alpha, \alpha + 1)) = (0, 1, 0, \alpha) + (0, 1, 0, \alpha + 1) + (0, 1, 1, 0) + (0, 1, 1, 1)$. Find $m^{-1}((0, \alpha + 1))$. Need $x_0 + x_1\alpha = 0$ on C where $x_0 = 0$ so $x_1 = 0$. Get $0 = y_1^2 + 1 = (y_1 + 1)^2$ and $0 = y_0^2 + y_1^2 = (y_0 + 1)^2$. $m^{-1}(0, \alpha + 1) = 4(0, 0, 1, 1)$. Thus the homomorphism from $E(\mathbf{F}_4)$ to $J(C)(\mathbf{F}_4)$ sends $(\alpha, 1)$ to $[(0, 1, 1, 0) + (0, 1, 1, 1) + (0, 1, 0, \alpha) + (0, 1, 0, \alpha + 1) - 4(0, 0, 1, 1)]$. Now we apply the trace map and get $\phi((\alpha, 1)) = [2(0, 1, 1, 0) + 2(0, 1, 1, 1) + (0, 1, 0, \alpha) + (0, 1, 0, \alpha + 1) + (0, 1, 0, \alpha + 1) + (0, 1, 0, \alpha) - 8(0, 0, 1, 1)] \in J(C)(\mathbf{F}_2)$. ((Get into nice hyperelliptic form $[P_1 + P_2 + P_3 - 3\infty]$.)

Aside: ((Since P has large prime order)) $\phi(P) \neq 0$ usually.

So if have $Q = nP \in E(\mathbf{F}_{2^r})$ then $E(\mathbf{F}_{2^r}) \xrightarrow{\phi} J(C)(\mathbf{F}_2)$ and $n(\phi(P)) = \phi(Q)$. If $g < r^2$ then DLP faster in $J(C)(\mathbf{F}_2)$.