\( P, Q \in E(\mathbb{F}_q), Q = nP \) \text{ (large prime order)} \text{ (ECDLP is given \( E, P, Q \), find \( n \)). Say } \exists \text{ hom'm } \phi : E(\mathbb{F}_q) \rightarrow G. \text{ Then } n(\phi(P)) = \phi(Q). \text{ Good if i) } \phi \text{ fast ii) } \phi(P) \neq 0, \text{ iii) the DLP in } G \text{ is easier.}

The GHS attack (Gaudry, Hess, Smart) does this (sometimes) when \( q = p^r \) with \( r \geq 2 \). Real life: \( q = 2^r, r \geq 163. \)

\text{(GHS attack involves hyperelliptic curves)}

Let \( K = \mathbb{F}_{2^r} \) 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 \( \infty \). \text{(Can have } \deg(f(x)) = 2g + 2). \text{ Called a hyperelliptic curve of genus } g. \text{ E.g. } y^2 + xy = x^5 + 1 \text{ over } \mathbb{F}_2 \text{ with genus 2. \text{ (Note an elliptic curve has genus 1. Lines and conic sections have genus 0.)}}

\text{(Group } G \text{ is Jacobian of hyperelliptic curve, involves divisors.)}

\( 3(1,1) - 2\infty \) has deg 1. End E.g.

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

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

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

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

Adleman, DeMarraisa, Huang: \text{ (imprecise)} \text{ Let } C \text{ be a hyper'c of large genus } g \text{ over a small } \mathbb{F}_q. \text{ Can solve DLP in } J(\mathbb{F}_q) \text{ in time}
subexponential in $\log(\# J(\mathbf{F}_q)) \approx \log(q^g)$ using an index calculus method where factor base consists of irreducible polynomials. Let $E$ be an elliptic curve with $\deg(D) = n << g$ (and $D$ is fixed by $\mathbf{F}_q$-Frobenius). E.g. Factor $[(0, 1) + (\alpha^3, 0) + \ldots + (\alpha^{12}, 0)]$ as $[(0, 1) - \infty] + [(\alpha^3, 0) + \ldots + (\alpha^{12}, 0) - 4\infty]$ End E.g. ((Note this doesn’t help with ECDLP for $E(\mathbf{F}_{2r})$ for $r \geq 163$ since genus small, finite field large.))

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

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

New E.g. Let $\alpha$ 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 $\alpha$)) Let $x_i, y_i \in \mathbf{F}_2$ 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 $(x_1 x_0^2 + x_1^2 x_0 + y_1 x_0 + y_0 x_1 + y_1 x_1 + y_1^2 + 1)\alpha + (x_0^3 + x_1^3 x_0 + y_0 x_0 + x_1^3 y_0 + y_0^2 + y_1^2) = 0$. Since $x_i, y_i \in \mathbf{F}_2$, that is 0 iff $(x_1 x_0^2 + x_1^2 x_0 + y_1 x_0 + y_0 x_1 + y_1 x_1 + y_1^2 + 1) = 0$ and $(x_0^3 + x_1^3 x_0 + y_0 x_0 + x_1^3 + y_1 x_1 + y_0^2 + y_1^2) = 0$. 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 $x_0 = 0, x_1 = 0, \ldots, x_{r-2} = 0$ ($(r - 1)$ 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 $\rho$ for ECDLP in $E(\mathbf{F}_{2r})$ in time exponential in $\log(2^r)$. Generically $g = O(2^r)$. Need $g \leq r^2$; sometimes happens.
Homomorphism: Need hom’s: \( \phi : E(F_{2^r}) \to J(C)(F_2) \). Well \( C \leftrightarrow W \to E \). Compose \( m : C \to E \).

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: \( E(F_{2^r}) \xrightarrow{P \to [P-0]} J(E)(F_{2^r}) \xrightarrow{m^{-1}} J(C)(F_{2^r}) \xrightarrow{\text{Trace}} J(C)(F_2) \). Induced by \( \text{Trace}(P) = \pi_0^0 P + \pi_2^1 P + \ldots + \pi_r^r P \).

E.g. Let \( C = W \cap (x = 0) \). Note \( (\alpha, 1) \in E(F_4) \leftrightarrow [(\alpha, 1) - 0] \in J(E)(F_4) \). Now \( \text{next apply } m^{-1} \), don’t know how on 0 so \( [(\alpha, 1) - 0] = [(\alpha, \alpha + 1) - (0, \alpha + 1)] \). (Have \( m : C \to E \) 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 \( y_0 + y_1^2 + y_1 + 1 = 0 \), \( y_0^2 + y_1 + 1 = 0 \). 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 \( y_1^2 + y_1 + 1 = 0 \). 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 \( E(F_4) \) to \( J(C)(F_4) \) 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 \( \phi((\alpha, 1)) = [2(0, 1, 1, 0) + 2(0, 1, 1, 1) + (0, 1, 0, \alpha) + (0, 1, 0, \alpha + 1) + (0, 1, 0, \alpha + 1) + (0, 1, 0, \alpha) - 8(0, 0, 1, 1)] \in J(C)(F_2) \). (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 \( Q = nP \in E(F_{2^r}) \) then \( E(F_{2^r}) \xrightarrow{\phi} J(C)(F_2) \) and \( n(\phi(P)) = \phi(Q) \). If \( g < r^2 \) then DLP faster in \( J(C)(F_2) \).