$k = 18 prtz \#E() = p + 1 - trzss$
??????χ**?**
123**?**$1 \times 2 \to 3123$

$\alpha F_{p^k} pk embedding E(F_{p^k}) krp^k r \#E(F_p) \log_2 r \approx 256 \log_2 p^k \approx 30005000 \rho = (\log_2 p)/(\log_2 r) k1220$**?**$k = 18$**????**$2s21211$
$s(s-1)2pk\pi : (x,y) \mapsto (x^p, y^p) p(x,y) F_{p^k} tt = p + 1 - \#E(F_p)$**?**$z \equiv -3p + p^4 \bmod rzzrzszs$
?$E' 2' 2 F_{p^{18}} 2' F_{p^3} 22' 2 F_{p^{18}} z$
$k = 18$**?**

$4a^3 + 27b^2 \neq 0 a, b \in_c urveareknownasrationalpointsonthecurve.$
$E(p) \mathcal{O} E(F_p) \#E(F_p) E(F_p) L = (x_l, y_l) M = (x_m, y_m) N = L + M N = (x_n, y_n) L, M, N \in E() xyN$

λ

$\lambda O E(p) L \neq M L + M L = M L + M = 2 L s 0 \leq s < r r M [s] M (s-1) M$

$s = r r [r] M = \mathcal{O} [s] M = N s s M N$
?$F_{p^{18}}$

$b \neq 0 X, Y \in F_{p^{18}} ptrz$

$zz \equiv 1442 \rho = (\log_2 p / \log_2 r) 4/3 \#E(F_{p^{18}})$

$t_{18} = \alpha^{18} + \beta^{18} \alpha\beta\alpha + \beta = t \alpha\beta = p$**??**$prp = 511$
$E(F_{p^{18}})(x,y) E(F_{p^{18}}) \pi_p : (x,y) \mapsto (x^p, y^p) p F_{p^{18}}$**??**$k = 12$
$F_{p^{18}} F_{p^k} k$**??**
$F_{p^{18}}$**?**$(p-1)\theta$**?**$k = 18 F_{p^{18}}$

$\theta = 2$
$^2 - i),$
$p18 = p6[w]/(w^3 - v).$
(11)

?F_{p^3} *sextic twist*
$22123 Q \in 2 Q_r el2relation. Next, ascalarwillbeconsideredforscalarmultiplicationof. Afterthat, asFigure$**??**$, -adicre$
??$(t-1) s_a dic.eps-adicrepresentationofscalar.$
??$z s_a dic.eps-adicand-adicrepresentationofscalar.$
??$_s m.eps Multi - scalarmultiplicationofwithFrobeniusmapping.$
$1, 2 G_3$**?**123

$\alpha 1, 2 G_3 F_{p^{18}} r$
$Q \in 2 \subset E(p18) Q$