5 slides on Hyperelliptic Curve Cryptography

Joppe Bos, Craig Costello, Huseyin Hisil, and Kristin Lauter

08 March 2013

Traditional groups: e.g. $\mathbb{Z}_p^*$

group operation: $\times$
field size:

2353884568174101991961613115178010832508216040221109935362585811062469502264450

1689737111580283468133427037796206988408596105286320454446154171372379418430644

9779948675315653861708351849863952266033726510910884379171199063410955505249134

6884480455921662959145631975109736553072922962586150069694376878665931969553438

2702680219630971939783298082768376844564606736823457380499989827619474833739543

8890624664287203356972484595202805503858242946337172362253768334911288070529098

0396353880887982848760154967269499881898103264662392833761500848784997180404116

0086788187207679626285735227161353815124866225653387970872514130319473619652559

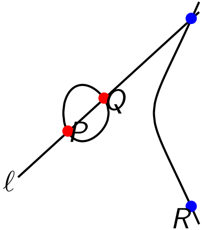
0802687437905250382025103426223952412139898023439071407928729147898155702930818

0833504071439251107602607490485110743498102403424373206651227056330069612780428

3253516701687175439820233927564153954517866423798470174861075615594323684476030

96305768507605419251266120624603573306634946918306258193 **(3072-bit)**

group operation:

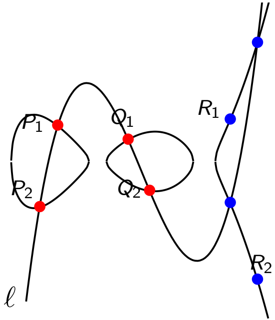


$$A = (Y_1 - X_1) * (Y_2 - X_2), \quad B = (Y_1 + X_1) * (Y_2 + X_2), \quad C = T_1 * k * T_2, \quad D = Z_1 * 2 * Z_2, E = B - A,$$
$$F = D - C, \quad G = D + C, \quad H = B + A, \quad X_3 = E * F, \quad Y_3 = G * H, \quad T_3 = E * H, \quad Z_3 = F * G.$$

field size:

115792089237316195423570985008687907853269984665640564039457584007913129639747 **(256-bit)**

group operation:

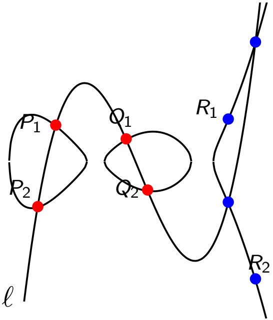


group operation:

$P = u_1 * Z,\quad R = u_0 * Z,\quad n_{01} = v0 * Z,\quad n_{02} = V0 * z,\quad n_{01} = n_{01} - n_{02},\quad n_{02} = U_0 * z,\quad n_{03} = U_1 * z,$
$n_{04} = n_{03} * n_{02},\quad n_{02} = n_{02} - R,\quad n_{05} = P - n_{03},\quad n_{06} = P * R,\quad n_{04} = n_{04} - n_{06},\quad n_{06} = V_1 * z,$
$W = z * Z,\quad n_{07} = v_1 * Z,\quad n_{08} = n_{07} - n_{06},\quad n_{06} = n_{07} + n_{06},\quad n_{09} = P^2,\quad n_{10} = W * n_{02},\quad n_{10} = n_{09} + n_{10},$
$n_{11} = n_{03}^2,\quad n_{03} = P + n_{03},\quad n_{12} = n_{10} - n_{11},\quad n_{11} = n_{09} + n_{11},\quad n_{09} = n_{04} * n_{08},\quad n_{04} = n_{04} * n_{05},$
$n_{05} = n_{01} * n_{05},\quad n_{01} = n_{01} * n_{12},\quad n_{08} = n_{02} * n_{08},\quad n_{02} = n_{02} * n_{12},\quad n_{01} = n_{09} + n_{01},\quad n_{05} = n_{05} + n_{08},$
$n_{02} = n_{02} - n_{04},\quad n_{04} = n_{05} * W,\quad n_{08} = n_{02} * n_{04},\quad n_{02} = n_{02}^2,\quad n_{05} = n_{05} * n_{04},\quad n_{04} = n_{01} * n_{04},$
$P = P * n_{05},\quad n_{09} = 2 * n_{04},\quad n_{09} = n_{09} - n_{02},\quad n_{12} = n_{05} * n_{03},\quad n_{09} = n_{09} - n_{12},\quad n_{02} = n_{09} - n_{02},$
$n_{02} = n_{02} * n_{03},\quad n_{11} = n_{05} * n_{11},\quad n_{02} = n_{02} + n_{11},\quad n_{02} = n_{02}/2,\quad n_{12} = W * n_{05},\quad R = R * n_{12},$
$n_{12} = n_{08} * n_{12},\quad n_{11} = Z * n_{12},\quad T = n_{11} * v_0,\quad S = n_{11} * v1,\quad n_{11} = n_{04} - n_{09},\quad n_{04} = P - n_{04},\quad n_{01} = n_{01}^2,$
$n_{06} = n_{08} * n_{06},\quad n_{01} = n_{01} * W,\quad n_{01} = n_{01} + n_{06},\quad n_{01} = n_{01} - n_{02},\quad n_{02} = n_{01} - R,\quad n_{05} = n_{02} * n_{05},$
$n_{02} = n_{09} * n_{11},\quad n_{11} = n_{01} * n_{11},\quad n_{06} = P * n_{04},\quad n_{06} = n_{06} + n_{02},\quad n_{05} = n_{06} + n_{05},\quad n_{04} = R * n_{04},$
$n_{11} = n_{04} + n_{11},\quad n_{09} = n_{09} * n_{08},\quad P = n_{09} * W,\quad R = n_{01} * n_{08},\quad n_{05} = n_{05} * W,\quad S = n_{05} - S,$
$T = n_{11} - T,\quad W = W * n_{12}.$

Hyperelliptic curves

group operation:



field size:

340282366920938463463374607431768211297 **(128-bit)**

Results for constant-time Diffie-Hellman at 128-bit security

Table: Intel Core i7-3520M (Ivy Bridge)

	cycles/scalar
previous best (elliptic)	139,000
ours (hyperelliptic)	117,000