Introduction to cryptography

ESISAR IR&C 2019/2020

Cyril Hugounenq

1 Playing with ECC

1. Init a prime number $p = randomprime(2^{100})$ and the elliptic curve $E : y^2 = x^3 + 2x + 3$ over $\mathbb{Z}/p\mathbb{Z}$ using the function *ellinit*
2. Draw a random point on the curve $P = random(E)$ and check that P is indeed on the curve using two methods
3. Draw a second point Q on the curve and check that $R = P + Q$ is also on the curve
4. Using the functions *ellcard* and *ellorder*, check that the order of P divides the cardinal of $E(F_p)$
5. Using the function *ellmul*, check that *ellorder* returns the order of a point.
6. Can $E(F_p)$ admit points of 2-torsion? Of 3-torsion?
7. Use the function $ellgenerators(E)$ to generate a point G. What is the order of G?
8. *Bonus:* For a fixed value of p prime and using *ellcard*, check empirically Hasse theorem on multiple curves. What is the empirical distribution of cardinals?

2 ECDSA

1. Using the notations given in the course, implement the functions $ECDSA{-}SHA256{-}sign(E, G, n, d_a, M)$ and $ECDSA - SHA256 - verify(E, G, n, Q_a, M, s, x_r)$

3 Rho-Pollard on ECC

1. Let E be an elliptic curve, G a point on E, and $P = aG$ for some unknown a. Write the function $rho - pollard - ECC(E, G, P)$ implementing the following algorithm
   - For a point $Q = (x, y)$ on E, we define
   $$f(Q) = \begin{cases} Q + P & if \quad x \bmod 3 = 0 \\ 2Q & if \quad x \bmod 3 = 1 \\ Q + G & if \quad x \bmod 3 = 2 \end{cases}$$
   - We define the sequences
   $$\begin{array}{ll} R_0 = P, & R_{i+1} = f(R_i) \\ S_0 = P, & S_{i+1} = f(f(S_i)) \end{array}$$
   - If $R_i = a_i P + b_i G$, what is the value of a_{i+1} and b_{i+1}?
   - Compute the sequences R_i and S_i until $R_i = S_i$.
   - Return a.
2. What is the empirical complexity of this attack with respect to the order of G?