Cryptography, exercise sheet 3 for 17 Sep 2024

1. Write 20210914 in binary and compute the coefficients of the presentation with window width $w = 3$.

2. Take the doubling formulas for twisted Edwards curves from exercise sheet 2 and turn them into projective formulas using as few multiplications as possible.

3. Test your understanding of the Montgomery ladder by writing out the intermediate values for P_0 and P_1 encountered in computing $19P$. We did a small example in class for computing $5P$.

4. For this exercise you may (and should) use a computer algebra system like sage for doing the elliptic curve computations. Think about how to document your work so that others can verify it.

   The elliptic curve
   $$y^2 = x^3 + x + 3 \text{ over } \mathbb{F}_{43}$$
   has 47 points. The point $P = (19, 42)$ has order 47. The point $P_A = (28, 15)$ is a multiple of P. Use the BSGS method to compute the discrete logarithm $a = \log_P(P_A)$ of P_A with base P.
   Verify your result.
   Each point that you compute should be documented, i.e., all baby steps and all the giant steps until you find a match. You do not need to document the arithmetic steps taken in computing the elliptic-curve additions.

5. Use the schoolbook version of Pollard rho and Floyd's cycle-finding algorithm to solve the DLP from exercise 4 using starting point $S_0 = F_0 = W_0 = 5P_A = (36, 30)$ and the step function
   $$W \leftarrow \begin{cases} W + P \\ W + P_A \\ 2W \end{cases}, \quad b \leftarrow \begin{cases} b + 1 \\ b \\ 2b \end{cases}, \quad c \leftarrow \begin{cases} c \\ c + 1 \\ 2c \end{cases}, \text{ for } s(W) = \begin{cases} 0 \\ 1 \\ 2 \end{cases}.$$
   The base point $P = (19, 42)$ has order 47, the target point is $P_A = (28, 15)$.

6. Discuss how you can document the work you did in exercise 5 so that one can grade it.