Elliptic Curves - List 5

Task 1 (15 pts) Implement the Lim-Lee "fast exponentiation with precomputations" method on elliptic curves. Use NIST P-521 curve to demonstrate the solution `https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf`. The solution should contain three parts:

(a) The first part that for given bitlength ℓ of the scalar and given storage bound S (S is the maximum number of precomputed group elements allowed to be stored in memory) finds the optimal parameters a, b of the last version of the Lim-Lee algorithm discussed during the lecture[1]. Optimal a, b will minimize the number of online operations on elliptic curve points and will not exceed the storage bound.

(b) The second part that for given (ℓ, S, a, b) and given domain parameters (including the base-point G) pre-computes multiples of the base-point G that will by used by the third part of the solution.

(c) The third part that for given scalar e and pre-computed points finds the value $e \cdot G$.

Present the solution both for $S = 100$ and $S = 5000$. Show how many EC-point operations are needed online for both values of S.

[1] that is, the version from the paper: Biljana Cubaleska, Andreas Rieke, Thomas Hermann *Improving and Extending the Lim/Lee Exponentiation Algorithm*. Selected Areas in Cryptography 1999: 163-174