Institute of Computer Science, University of Bern
Cryptographic Protocols, FS 2021

Prof. Christian Cachin
Jovana Mićić

Exercise 9

9.1 Library for $(t+1)$-of-n secret sharing (10pt)

Realize a prototype of a library that implements $(t+1)$-of-n secret sharing using polynomials over a field $GF(q)$. The prime q may be large, for example, up to 2000 bits long.

The library should contain a method to *share* a secret x, which takes t and n as inputs and outputs a list of n *shares*. Furthermore, there should be a method that takes any $t+1$ such shares and *reconstructs* the original secret from them.

Computation may be completely local. You may realize this in Python, Java, Golang, or C++ (... we limit the choice of programming languages due to our limited understanding of this world).