Institute of Computer Science, University of Bern
Cryptographic Protocols, FS 2023

Prof. Christian Cachin
Jovana Mićić

# Exercise 9

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

Realize a prototype of a library that implements $(f+1)$-of-$n$ secret sharing using polynomials over the field $\mathbb{Z}_q$. 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 $f$ and $n$ as inputs and outputs a list of $n$ *shares*. Furthermore, there should be a method that takes any $f+1$ such shares and *reconstructs* the original secret from them.

Computation may be completely local. You may write it in a language of your choice or use the attached Python file (`ex09.py`) and implement the missing methods. Once you are done, run the file and check if the tests pass.