CS 591 G1—Formal Methods in Security and Privacy—Spring 2020

Assignment 2

Due by Wednesday, March 4, at 5pm

1 Noninterference Proofs using Relational Hoare Logic

In this assignment, you will be writing proofs about program noninterference using EasyCrypt's Relational Hoare Logic (a subset of pRHL, probabilistic Relational Hoare Logic).

Begin by downloading the files

- `simpl-fill.ec`,
- `mod3-fill.ec`, and
- `xor-loop-fill.ec`

from the course website, and renaming them to

- `simpl.ec`,
- `mod3.ec`, and
- `xor-loop.ec`

respectively.

For each of these files, your goal is to replace the occurrence of the comment `(* fill in *)` by EasyCrypt proofs, in such a way that running EasyCrypt on your file succeeds. You may add supporting lemmas and your own comments, as needed or appropriate.

- The proof of `simpl.ec` involves only two-sided tactics.
- The program of `mod3.ec` involves computing the remainder of integer division by 3 of a private value, and its proof involves using one-sided `if` tactics. Note the restriction on when the tactics `wp` and `auto` may be used.
- The program of `xor-loop.ec` involves repeated exclusive or-ing by a private value, and its proof requires formulating an interesting loop invariant.

2 Assignment Submission by Email

You should submit your assignment by email, only. Create a zip or tar archive containing the three plain text files `simpl.ec`, `mod3.ec` and `xor-loop.ec`, and email it to Alley (`stough@bu.edu`) and Marco (`gaboardi@bu.edu`), with a subject line including the text `[CS591SUB]`.