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

Assignment 3

Due by Wednesday, March 25, at 5pm

1 Probabilistic Noninterference Proofs using pRHL

In this assignment, you will be writing proofs about probabilistic noninterference using EasyCrypt's pRHL, probabilistic Relational Hoare Logic.

Begin by downloading the file

- `prob-noninter-fill.ec`

from the course website, and renaming it to

- `prob-noninter.ec`

Your goal is to replace the two 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.

In the file, there are two problems for you to solve:

- The first is a formalization in EasyCrypt of the one-time pad example presented in lecture.
- The second features a program that branches on a private input.

When solving both problems there is a *restriction*: you may only use the `smt` tactic in the from that explicitly says which lemmas or axioms may be used: `smt(...)`.

2 Assignment Submission by Email

You should submit your assignment by email, only. Email the plain text file `prob-noninter.ec`—or a zip or tar archive containing the file—to Alley (`stough@bu.edu`) and Marco (`gaboardi@bu.edu`), with a subject line including the text `[CS591SUB]`.