Homework 8

May 14, 2022

You will need 50% of all homework points to qualify for the exam.

You may hand in your solutions in person or by email to kristinessaarmann@gmail.com. If you submit by email, either scan a handwritten solution or typeset your solution readably. I do not consider ASCII formulas readable.

When submitting, indicate your name and your matriculation number.

The total number of points for each homework is 20 (not including points for bonus problems, if available).

For submitting your solution in a nicely typeset way (e.g., using LaTeX), you get up to 3 bonus points, but not more than 30% of the points you reached for content.

Problem 1: Yao’s Garbled Circuits

(a) One application of secure function evaluation is the so-called “dating problem”. Two parties $A$ and $B$ are wondering whether they should date, but none of them wishes to admit their interest unless they know that the other side is interested, too. The solution is to perform a two-party computation on their inputs $a$ and $b$ (where $a$ and $b$ are a bit corresponding to whether $A$ or $B$ wishes to date) that returns $f(a, b) := a \land b$. (We ignore the fact that this is silly: by suggesting to run this SFE, one already expresses interest. But we could consider a case where some app is doing this automatically with all potential matches – a privacy preserving dating app.)

$A$ and $B$ want to use Yao’s Garbled Circuits for this. (We ignore the fact that that protocol only has security against passive adversaries.) That is, $A$ will have to pick some circuit $C$, and $B$ some input $x$ for that circuit. What should $C$ and $x$ be in this concrete case (i.e., how to convert $a$ and $b$ into $C$ and $x$) so that $B$ learns $f(a, b)$?

(b) (Bonus problem) Implement part of Yao’s protocol. That is, implement a function `make_gate` that garbles a single gate. (Given four input keys, and four messages.)

And a function `eval_gate` that recovers the message $m_{ij}$ given the corresponding keys.

Use the template in `yao-gate.py`.

1
Problem 2: Previous Homeworks

Which were the three most difficult homework problems this semester? Which were the three easiest? Approximately how much time did it take you to solve them?