292 – Homework Assignment 1

Fall 2021

Due: Thursday, October 14, 11:00AM in class

Do not discuss the problems with anyone other than the instructor.

1. Given two random variables X and Y:
(a) Show that the conditional entropy $H(X|Y)$ is the expected value of $\log_2(1/p(X|Y))$.

(b) Show that the entropy of a pair of random variables $H(X,Y)$ is equal to the entropy of one plus the conditional entropy of the other, i.e., $H(X,Y) = H(X) + H(Y|X)$.

(c) Show that mutual information $I(X;Y)$ can be computed as: $I(X;Y) = H(X) + H(Y) - H(X,Y)$.

2. Consider two random variables X and Y with the following joint distribution:

Y \ X	0	1	2	3
0	1/16	1/16	1/16	1/16
1	1/8	1/32	1/16	1/32
2	0	1/4	0	0
3	1/32	1/16	1/32	1/8

Compute the following: $H(X)$, $H(Y)$, $H(X|Y)$, $H(X,Y)$, $I(X;Y)$, $H_\infty(X)$, $H_\infty(Y)$, $H_\infty(X|Y)$, $H_\infty(X,Y)$, $I_\infty(X;Y)$. Please show the steps of your computation.

3. Consider a 32 bit secret value S with a uniform distribution and the following program:

```
f(S) {
  if (S % 32 == 0)
    sleep(S+5);
}
```

Assume that O denotes the execution time of the program and compute the following: $H(S)$, $H(O)$, $H(S|O)$, $I(S;O)$, and $H_\infty(S)$, $H_\infty(O)$, $H_\infty(S|O)$, $I_\infty(S;O)$. Please show the steps of your computation.

4. Consider the following programs where S is a 32 bit non-negative secret value with a uniform distribution and P is the public input:

```
f(S, P) {
  if (S > P)
    sleep(10);
  else
    sleep(20);
}
```

Compute $\phi_H(n)$ (i.e., the remaining uncertainty after maximum amount of leakage for the program against an attack of length n) for $n = 1, 2, 3$. Please show the steps of your computation. What is the sequence of public inputs for the optimum attack and what is the worst case length of the optimum attack?

5. Consider the following program where S is a 3 bit non-negative secret value with a uniform distribution and P is the public input:

```
f(S, P) {
  if (P == 1)
  switch(S) {
      case 0: case 1: case 2: sleep(0); break;
      case 3: case 4: sleep(1); break;
      case 5; case 6: sleep(2); break;
      case 7: sleep(3);
    }
  else if (P == 2)
   switch(S) {
      case 0: case 1: case 2: case 3: case 4: sleep(0); break;
      case 5: sleep(1); break;
      case 6; case 7: sleep(2);
    }
  else if (P == 3)
    switch(S) {
      case 0: sleep(0); break;
      case 1: sleep(1); break;
      case 2: case 3: case 4: sleep(2); break;
      case 5; case 6: sleep(3); break;
      case 7: sleep(4);
    }
  else if (P == 4)
     case 0: sleep(0); break;
      case 1: case 2: case 3: sleep(1); break;
      case 4: sleep(2); break;
      case 5; case 6: sleep(3); break;
      case 7: sleep(4);
    }
}
```

For this program show the partitions resulting from the timing side-channel and construct the attack trees for 1) an optimal non-adaptive attack strategy, 2) an adaptive attack strategy computed using the greedy heuristic, and 3) the optimal adaptive attack strategy.