

Notes: Please work on this with your group-mate(s); just submit *one* writeup per group. Consulting other sources (including the Web) is not allowed. Write your solutions neatly; if you are able to make partial progress by making some additional assumptions, then state these assumptions clearly and submit your partial solution. The problem marked (*) may be more difficult than the others.

0. Download Adler's paper *Tradeoffs in probabilistic packet marking for IP Traceback*, Journal of the ACM, 2005, and read the full proof of the upper bound for the case $b = 1$ (where the attacker can set the initial bit arbitrarily). I will assume for the final exam that you have done this reading.

1. In Adler's paper above, prove the upper bound for the number of packets needed for the case where $b > 1$, where the Attacker always initially sets the marking bit to 0, and the $b - 1$ counter bits randomly. **(5 points)**

2(*). This problem comes up in a learning-theory context; time permitting, we will cover the appropriate paper in class.

Toss a coin with $\Pr[\text{heads} = p]$ until you get the first head. Repeat this n times **independently**; let X_i be the number of tosses in the i th trial ($1 \leq i \leq n$), and define $X = \max_{i=1}^n X_i$. Prove that $\mathbf{E}[X] \leq O((1/p) \cdot \log n)$. **Hint:** Recall that if Y takes on only non-negative integer values, then $\mathbf{E}[Y] = \sum_{i \geq 1} \Pr[Y \geq i]$. **(10 points)**