HW 9, Problem 2, REDO CMSC 456. DUE Dec 3
NO extensions

NOTE- THE HW IS THREE PAGES LONG

If you got ≤ 20 points on hw 09, Problem 2 then do the problem below. Your score on this will be added your HW09 score.

Be CLEAR and CORRECT. You will get 0 points if your answer is unclear or incorrect. No regrade requests are allowed. Note that the max you can get is 20 points. Each part will be graded either full credit OR 0.

PROBLEM:

Assume there is an α-SES. From class we know we know that there is a (t, L) secret sharing scheme with shares of size $\frac{n}{t} + \alpha n$. We state this as:

With ONE iteration we get shares of size $\frac{n}{t} + \alpha n$.

In class when going over the solution to hw09, problem 2, I proved:

With TWO iteration we get shares of size $\frac{n}{t} + \frac{\alpha n}{t} + \alpha^2 n$.

With THREE iteration we get shares of size $\frac{n}{t} + \frac{\alpha n}{t} + \frac{\alpha^2 n}{t} + \alpha^3 n$.

1. (15 points) Give the protocol for M iterations. Use the format on the slides that had the solution.

2. (3 points) How short are the shares? Express how short the shares are in closed form, without a summation or a $\cdots$.

3. (1 point) If α is fixed and M goes to infinity, what does the expression approach?

4. (1 point) If M is fixed and α goes to zero, what does the expression approach?