HW 9 CMSC 456. DUE Nov 19
SOLUTIONS
NOTE- THE HW IS THREE PAGES LONG

1. (0 points) READ the syllabus- Content and Policy. What is your name? Write it clearly. What is the day of the final? READ the slides and notes on Secret Sharing.

2. (30 points) Assume there is an α-SES. From class we know we can, with a hardness assumption, use the α-SES to get a (t, L) secret sharing scheme with shares of size $\frac{n}{t} + \alpha n$.

   1) (10 points) Use the α-SES to get a (t, L) secret sharing scheme with even SHORTER shares (though see next part). (NOTE – whatever you do to make it shorter, just do once. In a later part of this question you'll get to do it again!)

   2) (5 points) Your answer to the above question might not quite yield shorter shares. You need a condition on t, α. What is that condition?

   3) (10 points) Do a protocol that makes the shares even shorter! (See next part)

   4) (5 points) Your answer to the above question might not quite yield shorter shares. You need a condition on t, α. What is that condition?

SOLUTION TO PROBLEM TWO

1) We begin similar to the $\frac{n}{t} + \alpha n$ protocol.

   (a) Zelda does $k_1 \leftarrow GEN(n)$. Note $|k_1| = \alpha n$.

   (b) $u = ENC_{k_1}(s)$. Note that $|u| = n$. Let $u = u_0 \cdots u_{t-1}$, $|u_i| \sim \frac{n}{t}$.

   (c) Let $p_1 \sim 2^{n/t}$. Zelda forms poly over $\mathbb{Z}_{p_1}$:

$$f(x) = u_{t-1}x^{t-1} + \cdots + u_1 x + u_0$$

   (d) (Here is where we do something different.) We now want to ENCODE k_1. Zelda does $k_2 \leftarrow GEN(\alpha n)$. Note that $|k_2| = \alpha^2 n$.

   (e) $v = ENC_{k_2}(k_1)$. Note that $|v| = \alpha n$. Let $v = v_0 \cdots v_{t-1}$, $|v_i| = \frac{\alpha n}{t}$.

(f) Let $p_2 \sim 2^{\alpha n/t}$. Zelda forms poly over $\mathbb{Z}_{p_2}$:

$$g(x) = v_{t-1}x^{t-1} + \cdots + v_1 x + v_0.$$

(g) Let $p_3 \sim 2^{\alpha^2 n}$. Zelda picks $r_{t-1}, \ldots, r_1 \in \{0, \ldots, p_3\}$. Zelda forms polynomial over $\mathbb{Z}_{p_3}$:

$$h(x) = r_{t-1}x^{t-1} + \cdots + r_1 x + k_2$$

(h) Zelda gives A_i, $(f(i), g(i), h(i))$.

Length:

- $f(i) \in \mathbb{Z}_{p_1}$ where $p_1 \sim 2^{n/t}$, so $|f(i)| \sim \frac{n}{t}$.
- $g(i) \in \mathbb{Z}_{p_2}$ where $p_2 \sim 2^{\alpha n/t}$, so $|g(i)| \sim \alpha n/t$.
- $h(i) \in \mathbb{Z}_{p_3}$ where $p_3 \sim 2^{\alpha^2 n}$, so $|g(i)| \sim \alpha^2 n$.

2) So we need

$$\frac{n}{t} + \frac{\alpha n}{t} + \alpha^2 n < \frac{n}{t} + \alpha n$$

$$\frac{\alpha n}{t} + \alpha^2 n < \alpha n$$

$$\frac{1}{t} + \alpha < 1$$

SO this is the condition that we need.

3)

(a) Zelda does $k_1 \leftarrow GEN(n)$. Note $|k_1| = \alpha n$.

(b) $u = ENC_{k_1}(s)$. Note that $|u| = n$. Let $u = u_0 \cdots u_{t-1}$, $|u_i| \sim \frac{n}{t}$.

(c) Let $p_1 \sim 2^{n/t}$. Zelda forms poly over $\mathbb{Z}_{p_1}$:

$$f_1(x) = u_{t-1}x^{t-1} + \cdots + u_1 x + u_0$$

(d) We now want to ENCODE k_1. Zelda does $k_2 \leftarrow GEN(\alpha n)$. Note that $|k_2| = \alpha^2 n$.

(e) $v = ENC_{k_2}(k_1)$. Note that $|v| = \alpha n$. Let $v = v_0 \cdots v_{t-1}$, $|v_i| = \frac{\alpha n}{t}$.

(f) Let $p_2 \sim 2^{\alpha n/t}$. Zelda forms poly over $\mathbb{Z}_{p_2}$:

$$f_2(x) = v_{t-1}x^{t-1} + \cdots + v_1 x + v_0.$$

(g) We now want to ENCODE k_2. Zelda does $k_3 \leftarrow GEN(\alpha^2 n)$. Note that $|k_3| = \alpha^3 n$.

(h) $v = ENC_{k_3}(k_2)$. Note that $|v| = \alpha^2 n$. Let $v = v_0 \cdots v_{t-1}$, $|v_i| = \frac{\alpha^2 n}{t}$.

(i) Let $p_3 \sim 2^{\alpha^2 n/t}$. Zelda forms poly over $\mathbb{Z}_{p_3}$:

$$f_3(x) = v_{t-1}x^{t-1} + \cdots + v_1 x + v_0.$$

(j) Let $p_4 \sim 2^{\alpha^3 n}$. Zelda picks $r_{t-1}, \ldots, r_1 \in \{0, \ldots, p_3\}$. Zelda forms polynomial over $\mathbb{Z}_{p_3}$:

$$f_4(x) = r_{t-1}x^{t-1} + \cdots + r_1 x + k_3$$

(k) Zelda gives A_i, $(f_1(i), f_2(i), f_3(i), f_4(i))$.

Length:

- $f_1(i) \in \mathbb{Z}_{p_1}$ where $p_1 \sim 2^{n/t}$, so $|f_1(i)| \sim \frac{n}{t}$.
- $f_2(i) \in \mathbb{Z}_{p_2}$ where $p_2 \sim 2^{\alpha n/t}$, so $|f_2(i)| \sim \alpha n/t$.
- $f_3(i) \in \mathbb{Z}_{p_3}$ where $p_3 \sim 2^{\alpha^2 n/t}$, so $|f_3(i)| \sim \alpha^2 n/t$.
- $f_4(i) \in \mathbb{Z}_{p_4}$ where $p_4 \sim 2^{\alpha^3 n}$, so $|f_4(i)| \sim \alpha^3 n$.

4) When is this length better than the earlier algorithm? We need

$$\frac{n}{t} + \frac{\alpha n}{t} + \frac{\alpha^2 n}{t} + \alpha_3 n < \frac{n}{t} + \frac{\alpha n}{t} + \alpha^2 n$$

$$\frac{\alpha^2 n}{t} + \alpha^3 n < \alpha^2 n$$

$$\frac{1}{t} + \alpha < 1$$

Great- same condition as part 2.

GOTO NEXT PAGE

3. (40 points) For this problem you can assume that, for any t, L, there is a protocol for (t, L) secret sharing where everyone gets one share of size the size of the secret (or roughly). For the problems below explain it so that someone who has never seen secret sharing can understand it, though she knows that for all t, L there is a (t, L) secret sharing scheme where blah blah. (This is not hypothetical. I am having this one graded by someone outside the course grading this one.)

   Zelda has a secret $s \in \{0,1\}^n$. She wants to share a secret with $A_1, \ldots, A_{L_1}$, $B_1, \ldots, B_{L_2}$. such that the following happens:

   (a) If $\geq k_1$ of $A_1, \ldots, A_{L_1}$ meet with $\geq k_2$ of $B_1, \ldots, B_{L_2}$ then they can learn the secret

   (b) No other set of people can learn the secret.

   (c) Everyone gets a string of length roughly n (the roughly since we are over $\mathbb{Z}_p$ and not the field on 2^n elements.)

   SOLUTION TO PROBLEM THREE

   i. Zelda generates a random $r_1 \in \{0,1\}^n$.
   ii. Zelda lets $r_2 = s \oplus r_1$.
   iii. Zelda does (t_1, L_1) secret sharing with secret r_1 and people $A_1, \ldots, A_{L_1}$.
   iv. Zelda does (t_2, L_2) secret sharing with secret r_2 and people $B_1, \ldots, B_{L_1}$.

   Recovery:

   If t_1 of $A_1, \ldots, A_{L_1}$ and t_2 of $B_1, \ldots, B_{L_2}$ get together then:

   i. The $A_1, \ldots, A_{L_1}$ can recover r_1.
   ii. The $B_1, \ldots, B_{L_2}$ can recover r_2.
   iii. They can all do

   $$r_1 \oplus r_2 = s$$

   END OF SOLUTION TO PROBLEM THREE

GOTO NEXT PAGE

4. (30 points) In this problem you will investigate the low quality and predictability of the Java random number generator. In order for this problem to work, your code must instantiate a single instance of "java.util.Random" and call the "nextInt()" method to generate random numbers.

   (a) Write a function "genList(int N)" which creates an array of N random integers

   (b) Write a function "countEvenSubseq(int[] list , int n)" which will return the number of contiguous subsequences of even numbers. To put it another way, this is the number indicies i so that list[i] ... list[$i + n - 1$] are all even. For example,

      i. countEvenSubseq({0,4,2,3}, 2) = 2
      ii. countEvenSubseq({0,4,2,2,10,8}, 4) = 3
      iii. countEvenSubseq({0,4,2,9,10,8}, 4) = 0

   (c) If the java random number generator were truly random, then what on average would you expect $countEvenSubseq(genList(N), n)$ to be? (Hint: there are $N - n + 1$ indices which could be the start of a contiguous subsequence. What is the chance that each one is all even? Now multiply those two numbers together.)

   (d) Write a program which outputs $countEvenSubseq(genList(N), n)$ for N=3145728, n=14. Try running it a few more times. How do the results differ from what you would have expected from part (c)?

   (e) (Not worth any points, just for your own information) see `https://www.javamex.com/tutorials/random_numbers/java_util_random_algorithm.shtml` to learn more about how the Java random number generator actually works. Can you figure out why part (d) worked the way it did? Hint: what are the factors of N?

SOLUTION TO PROBLEM FOUR

Note that I chose the specific N, n because it yields 456 on the final question.

END OF SOLUTION TO PROBLEM FOUR