hw09 Solutions

hw09 Problem 2: Shorter Shares

Problem 2.1

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 $\frac{n}{t} + \alpha n$.

PART 1: Use the α-SES to get a (t, L) secret sharing scheme with even SHORTER shares.

Problem 2.1: The Protocol

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

1. Zelda does $k_1 \leftarrow GEN(n)$. $|k_1| = \alpha n$.
2. $u = ENC_{k_1}(s)$. that $|u| = n$. Let $u = u_0 \cdots u_{t-1}$, $|u_i| \sim \frac{n}{t}$.
3. Let $p_1 \sim 2^{n/t}$. $f(x) = u_{t-1}x^{t-1} + \cdots + u_0$
4. Zelda does $k_2 \leftarrow GEN(\alpha n)$. $|k_2| = \alpha^2 n$.
5. $v = ENC_{k_2}(k_1)$. $|v| = \alpha n$. Let $v = v_0 \cdots v_{t-1}$, $|v_i| = \frac{\alpha n}{t}$.
6. Let $p_2 \sim 2^{\alpha n/t}$. $g(x) = v_{t-1}x^{t-1} + \cdots + v_0$.
7. Let $p_3 \sim 2^{\alpha^2 n}$. $h(x) = r_{t-1}x^{t-1} + \cdots + r_1 x + k_2$
8. Zelda gives A_i, $(f(i), g(i), h(i))$.

Problem 2.1: Length of Shares

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 $|g(i)| \sim \alpha^2 n$.

So the length is $\frac{n}{t} + \frac{\alpha n}{t} + \alpha^2 n$.

When is:

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

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

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

Note: This is usually satisfied!

Problem 2.2: Even Shorter Shares: Protocol

1. Zelda does $k_1 \leftarrow GEN(n)$. $|k_1| = \alpha n$.
2. $u = ENC_{k_1}(s)$. that $|u| = n$. Let $u = u_0 \cdots u_{t-1}$, $|u_i| \sim \frac{n}{t}$.
3. Let $p_1 \sim 2^{n/t}$. $f_1(x) = u_{t-1}x^{t-1} + \cdots + u_0$
4. Zelda does $k_2 \leftarrow GEN(\alpha n)$. $|k_2| = \alpha^2 n$.
5. $v = ENC_{k_2}(k_1)$. $|v| = \alpha n$. Let $v = v_0 \cdots v_{t-1}$, $|v_i| = \frac{\alpha n}{t}$.
6. Let $p_2 \sim 2^{\alpha n/t}$. $f_2(x) = v_{t-1}x^{t-1} + \cdots + v_0$.
7. Zelda does $k_3 \leftarrow GEN(\alpha^2 n)$. $|k_3| = \alpha^3 n$.
8. $w = ENC_{k_3}(k_2)$. $|v| = \alpha^2 n$. Let $w = w_0 \cdots w_{t-1}$, $|w_i| = \frac{\alpha^2 n}{t}$.
9. Let $p_3 \sim 2^{\alpha^2 n/t}$. $f_3(x) = w_{t-1}x^{t-1} + \cdots + w_0$.
10. Let $p_4 \sim 2^{\alpha^3 n}$. $f_4(x) = r_{t-1}x^{t-1} + \cdots + r_1 x + k_3$
11. Zelda gives A_i, $(f_1(i), f_2(i), f_3(i), f_4(i))$.

Problem 2.2: Even Shorter Shares: Length

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 $|f_4(i)| \sim \alpha^3 n$.

So the length is $\frac{n}{t} + \frac{\alpha n}{t} + \frac{\alpha^2 n}{t} + \alpha^3 n$
When is

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

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

Note: Great! Same condition as before, and usually holds.

Problem 2.ω: Pushing The Method To the Limit

One Iteration got us $\frac{n}{t} + \alpha n$
Two Iteration got us $\frac{n}{t} + \frac{\alpha n}{t} + \alpha^2 n$
Three Iteration got us $\frac{n}{t} + \frac{\alpha n}{t} + \frac{\alpha^2 n}{t} + \alpha^3 n$

Your chance to get back some points on hw09 Problem 2:
Do CLEANLY and CLEARLY the problem of M Iteration. Include the protocol and how they recover the secret.

1. DUE Mon Dec 3. This is a courtesy. NO DEAD CAT EXT.
2. If you got $\leq X$ on and you do it CLEANLY and CORRECTLY then you will get Y. Have not determined X and Y yet.
3. You will likely either get 0 or Y. We will not spend that much time grading this one – just do it CLEANLY, CORRECTLY.
4. Will post formally what we want soon.

hw09 Problem 3: A Different Access Structure

Problem 3: A Different Access Structure

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:

1. 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
2. No other set of people can learn the secret.
3. Everyone gets a string of length roughly n.

Problem 3: The Protocol

1. Zelda generates a random $r_1 \in \{0, 1\}^n$.
2. Zelda lets $r_2 = s \oplus r_1$.
3. Zelda does (t_1, L_1) secret sharing with secret r_1 and people $A_1, \ldots, A_{L_1}$.
4. 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:

1. The $A_1, \ldots, A_{L_1}$ can recover r_1.
2. The $B_1, \ldots, B_{L_2}$ can recover r_2.
3. They can all do

$$r_1 \oplus r_2 = s$$