Exercises III

Note: We discuss solutions to the exercises together in the class on the **11th December 2025**.

Exercise 1. *Properties of Replicated Secret Sharing*

Let us consider the replicated secret sharing (RSS) scheme introduced during the lecture.

1. Make a concrete execution of the Share algorithm of RSS over $\mathbb{Z}/q\mathbb{Z}$ for $N = 4$, $t = 2$ and $q = 17$ and $\alpha = 5$.
2. Now, reconstruct using the set $S = \{2, 4\}$.
3. As for Shamir's secret sharing scheme, the replicated secret sharing scheme is *linear*.

   Show that for every $\alpha, \alpha' \in \mathbb{Z}/q\mathbb{Z}$, for every valid reconstruction set $S \subset \{1, \ldots, N\}$ with $|S| = t$, it holds

   $$\Pr_{\substack{\mathsf{Share}(\alpha) \to (s_1, \ldots, s_N) \\ \mathsf{Share}(\alpha') \to (s'_1, \ldots, s'_N)}} \left[\mathsf{Reconstruct}((s_i + s'_i)_{i \in S}) = \alpha + \alpha' \right] = 1,$$

   where Share and Reconstruct refer to the replicated secret sharing algorithms.

   Hint: You can use the correctness property proven during the lecture.
4. Can you detail out RSS for $t = N$? What secret sharing scheme, which we have already seen in the lecture, does it remind you of?
5. As opposed to Shamir's secret sharing scheme, the replicated secret sharing scheme is not *multiplicative*. Provide a counter example, by concretely setting N, t and q and executing the Share algorithm, such that the product of the shares (of some secret shared values α and α') do not allow for reconstructing the product $\alpha \cdot \alpha$.

Exercise 2. *GGM-Tree*

In this exercise we will learn about the GGM-tree construction, a generic construction of pseudo-random functions (PRF) from pseudo-random generators (PRG).

Let $G \colon \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a length-doubling PRG with output split as $G(x) = G_0(x) \| G_1(x)$, where both $G_b(x) \in \{0,1\}^\lambda$. Here $\|$ denotes the concatenation of bits.

For $k \in \{0,1\}^\lambda$ and $x \in \{0,1\}^\ell$, define the function $F(k, x) = G_{x_\ell}(\cdots G_{x_2}(G_{x_1}(k)) \cdots)$.

1. Can you try to visualize the construction of $F(k, x)$ in form of a binary tree for $\ell = 3$? Label the path for the input $x = 010$.

   Hint: Going "left" means taking the output $G_0(\cdot)$ and going "right" means taking the output $G_1(\cdot)$ as a fresh input to the next evaluation of G.
2. Let H_0 be the experiment where the adversary interacts with the real oracle $F(k, \cdot)$. Let H_ℓ be the experiment where the adversary interacts with a truly random function f sampled from the set of all functions $\{0,1\}^\ell \to \{0,1\}^\lambda$.

   Describe the hybrids $H_1, \ldots, H_{\ell-1}$, where the first i levels of the tree are replaced with random values.

   Explain why there are exactly ℓ hybrids.
3. Prove that distinguishing two sequential hybrids H_{i-1} and H_i would give an adversary that breaks the pseudorandomness of the PRG G.

Note: Reference for further reading: *How to Construct Random Functions* by Oded Goldreich, Shafi Goldwasser and Silvio Micali, Journal of ACM'1986.