Exercises II

Note: We discuss solutions to the exercises together in the class on the **10th December 2025**.

Exercise 1. *Properties of Shamir's Secret Sharing*

Let us consider the Shamir secret sharing scheme introduced during the lecture. In this exercise, we want to prove that it is *linear*. That means, if a party owns a share of two different values α and α', the sum of the two shares provide a valid share of the sum $\alpha + \alpha'$.

1. 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 Shamir's secret sharing algorithms.

Hint: You can use the correctness property proven during the lecture.

Interestingly, under some careful parameter constraints, Shamir's secret sharing is even *multiplicative*. We'll go through it together.

2. Let's start with a concrete example, considering $N = 6, t = 2, q = 17$ and $\alpha = 1, \alpha' = 2$. Provide an execution of the Share algorithm from Shamir's secret sharing to compute some exemplary $w(x)$ and $w'(x)$ and shares $s_1, \ldots, s_N$ and $s'_1, \ldots, s'_N$. Compute their product $(w \cdot w')(x)$ and prove that $w \cdot w'$ evaluated at 0 gives $\alpha \cdot \alpha' = 2$.

3. Let $w(x)$ be a polynomial in $\mathbb{Z}/q\mathbb{Z}[x]$ of degree at most d and $w'(x)$ be a polynomial in $\mathbb{Z}/q\mathbb{Z}[x]$ of degree at most d'. What is the largest degree their sum $(w + w')(x)$ can have? And how about their product $(w \cdot w')(x)$?

4. Back to our concrete example from Item 2. For $S = \{1, 2, 3\}$, show that $(s_i \cdot s'_i)_{i\in S}$ provide enough information to reconstruct $\alpha \cdot \alpha' = 2$.

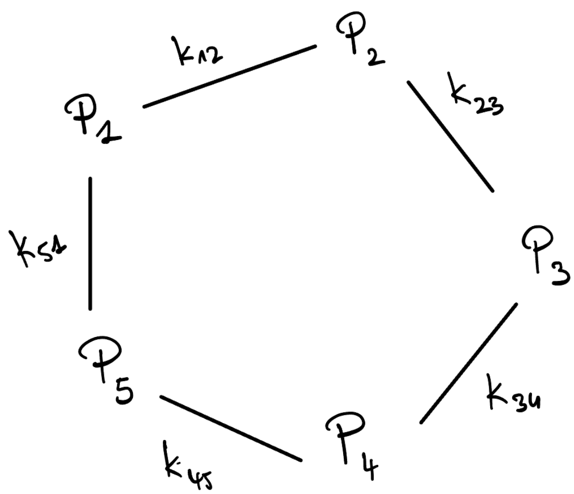
5. We can know prove the following general result. Assume that $(s_1, \ldots, s_N) \leftarrow \mathsf{Share}(\alpha)$ is a t-out-of-N secret sharing of α and $(s'_1, \ldots, s'_N) \leftarrow \mathsf{Share}(\alpha')$ a t-out-of-N secret sharing of α'. And that each party i knows s_i and s'_i. Prove that every set $S \subset \{1, \ldots, N\}$ with $|S| = 2t - 1$ is a valid reconstruction set. More concretely, prove that knowing $(s_i \cdot s'_i)_{i\in S}$ suffices to reconstruct $\alpha \cdot \alpha'$.

Exercise 2. *Pseudo-Random Zero-Sharing*

Let us consider the example of a pseudo-random secret sharing for $N = 5$ parties, where

- Party 1 gets $k_1 = (k_{12}, k_{51})$
- Party 2 gets $k_2 = (k_{12}, k_{23})$
- ...
- Party 5 gets $k_5 = (k_{45}, k_{51})$

And for a given input x (for instance a time stamp with access to a common clock), every Party i computes their share s_i as $s_i = F(k_i[0], x) \oplus F(k_i[1], x)$, where F is a pseudo-random function and $k_i = (k_i[0], k_i[1])$ is the partie's key. For every set $S \subset \{1, \ldots, N\}$, the Reconstruction algorithm is given by $\bigoplus_{i\in S} s_i$.



1. Prove that the scheme is correct only for the set $\{1, \ldots, N\}$. In other words, all parties are required for the reconstruction of the zero value.

Hint: Show that reconstruction works for the set $\{1, \ldots, N\}$, but does not work for any strict subset of it.

2. Prove that security is guaranteed for subsets of size one.

3. Prove that security is *not* guaranteed for subsets of size two.

Hint: It's enough to provide one counter example.

Note: Reference for further reading: *Compressing Cryptographic Resources* by Niv Gilboa and Yuval Ishai, Crypto'1999.