

## Exercise 7

### 1 Secret Sharing for Monotone Access Structures

Access to the treasury of the Ottoman Empire is closely guarded. Only the Sultan knows the key to enter the treasure chamber in Topkapi palace of Istanbul. But since the life of a Sultan was sometimes at danger, he asked his Grand Vizier to design a scheme for distributing knowledge of the key among the 27 viziers.

- a) Only the Grand Vizier together with two viziers or five viziers together should know the key. Four or fewer viziers or the Grand Vizier with one viziers must not be permitted into the treasury. What secret sharing scheme did the Grand Vizier design for the Sultan?
- b) After the introduction of several Second Viziers to the Empire, power was spread further. Now, the Grand Vizier together with any Second Vizier should know the key, or the Grand Vizier together with two viziers, or one of the Second Viziers together with five viziers. What secret sharing scheme did they use?

Hint: The “access structure” for the secret sharing scheme is a monotone Boolean formula with AND, OR, and THRESHOLD operators. Define a (recursive) distribution method for every operator. It should allow to transform any monotone access structure into a secret sharing scheme.

### 2 Threshold Pseudorandom Function

Using a discrete-logarithm setting with  $G = \langle g \rangle$ , let  $x$  be a *seed* and define a  $F_x : \{0, 1\}^* \rightarrow \{0, 1\}^k$  as

$$F_x(s) = H'(H(s)^x),$$

where  $H : \{0, 1\}^* \rightarrow G$  and  $H' : G \rightarrow \{0, 1\}^k$  are hash functions. The family  $F = \{F_x\}$  is a pseudorandom function assuming the hardness of the DLP (which can proven formally in the random oracle model).

Design a non-interactive threshold pseudorandom function based on  $F$  that is secure against a passive adversary.