

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 the Topkapi palace in Istanbul. But since the life of a Sultan is at danger sometimes, he asks his Grand Vizier to design a scheme for distributing knowledge of the key among the 27 Viziers.

- a) Either 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 Vizier must not be permitted into the treasury. What secret sharing scheme does the Grand Vizier design for the Sultan?

Hint: Describe the extra power of the Grand Vizier in terms of a number of Viziers.

- b) After the introduction of several Second Viziers to the Empire, power is 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 do they use?

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