HAI709I : Fondements cryptographiques de la sécurité, Université de Montpellier, 2024

23/09/2024. Homework for Lecture 3.

Exercise 1. We consider an access structure with four participants A, B, C, D where the authorised groups (groups of participants who can access the secret) are the two-element sets

$$\{A, B\},\ \{B, C\},\ \{C, D\},$$

and all supersets (extensions) of these three sets.

(a) Construct a secret sharing scheme for this access structure with a secret key uniformly distributed in $\{0,1\}^{1024}$.

(b) The same question, but every private key (secret shares for each participants) must be a binary string of length at most 2048 bits.

(c) The same question, but every private key (secret shares for each participants) must be a binary string of length at most 1536 bits.

(d)** Prove that the number 1536 is optimal: there is no secret sharing scheme for this access structure with a secret key uniformly distributed in $\{0,1\}^{1024}$ and each secret key is distributed on $\{0,1\}^m$ for $m < 1536$.

Exercise 2. If $\{A_i : i = 1, 2, 3, \ldots, n\}$ is a finite set of events that are *mutually exclusive* (any two of them cannot both occur at the same time) and *collectively exhaustive* (at least one of the events A_i must occur), then for any event B we have

(a) $\Pr[B] = \sum_{i=1}^{n} \Pr[A_i \cap B]$

(b) $\Pr[B] = \sum_{i=1}^{n} \Pr[B \mid A_i] \Pr[A_n]$

Exercise 3. Which of the following functions are negligibly small?

(a) $1/\log_2 n$

(b) $1/n^{\log_2 n}$

(c) $1/(\sqrt{n})^{\sqrt{n}}$.

(d) $1/2^{\sqrt{n}}$.

Exercise 4. We say that a function $f\colon \mathbb{N} \to \mathbb{R}$ is *negligibly small* if for every polynomial $\mathrm{Q}(x)$ (not identically equal to zero) there exists a natural number n_0 such that for all $n > n_0$ we have $|f(n)| \leq 1/|\mathrm{Q}(n)|$ (i.e., $f(n)$ converges to zero faster than any inverted polynomial). Let $f(n)$ and $g(n)$ be negligibly small functions. Prove that the following functions are also negligibly small:

(a) $f(n) + g(n)$

(b) $f^{10}(n)$

(c) $f(n) \cdot g(n)$

(d) $\sqrt{g(n)}$