18/09/2023. Lecture 2.

1 Secret sharing.

In this chapter we discuss the notion of *secret sharing* and discuss simple examples of secret sharing schemes. We begin with a brief motivation. Assume that we want to distribute a *secret* k (it can be a password, a secret code for a safebox, $\ldots$) among a group of n people (participants of the secret sharing scheme). We do not want to let any individual participant know this secret; we require that only *authorised groups* of participants are able to reveal it.

Example 1. We may require that only all n participants together can get the secret.

Example 2. We may require that only the majority of participants (i.e., every group that consists of more than $n/2$ participants) can get the secret.

Example 3. We may fix a threshold t between 1 and n and require that every group of at least t participants can get the secret. Observe that Example 1 above is a special case of this rule for $t = n$, and Example 2 is a special case of this rule for $t = \lceil (n+1)/2 \rceil$.

The groups of participants that are *not authorised* should not have *any* information about the secret. Let us proceed with a more formal definition.

Let $\mathcal{K}$ be the space of all potential secrets. (In all our examples below we let $\mathcal{K} = \{0,1\}^m$ for some integer m or $\mathcal{K} = \mathbb{Z}/p\mathbb{Z}$ for some integer number p.) A secret sharing scheme with n is a randomised algorithm (*Dealer*) that samples for each $k \in \mathcal{K}$ a probability distribution $p_k(s_1, \ldots, s_n)$

$$\mathrm{Prob}^{(k)}[S_1 = s_1, \ldots, S_n = s_n] = p_k(s_1, \ldots, s_n),$$

the distribution of random *shares* compatible with the key k. These distributions must respect the following two conditions.

(I) For every *authorised* group of participants $\{i_1, \ldots, i_r\}$, the random variables $\langle S_{i_1}, \ldots, S_{i_t} \rangle$ contain enough information to reconstruct the secret key k. This means that for every vector of value $(s_{i_1}, \ldots, s_{i_t})$ there can be only one secret $k \in \mathcal{K}$ such that

$$\mathrm{Prob}^{(k)}[S_{i_1} = s_{i_1}, \ldots, S_{i_t} = s_{i_t}] > 0.$$

(II) For every *non authorised* group of participants $\{i_1, \ldots, i_\ell\}$, the random variables $\langle S_{i_1}, \ldots, S_{i_\ell} \rangle$ contain *no* information on k. This means that for all $k \in \mathcal{K}$ the restrictions of the distribution

$$\mathrm{Prob}^{(k)}[S_1 = s_1, \ldots, S_n = s_n]$$

on the coordinates $i_1, \ldots, i_\ell$ are identical[1].

Example 1 *revisited* (*only all n participants together know the secret*). We let $\mathcal{K} = \{0,1\}^m$ and define the scheme as follows. For every secret $k = (k_1 \ldots k_m) \in \{0,1\}^m$ we sample the shares $S_1, \ldots, S_{n-1}$ as

[1] In the examples that we discuss below, the joint distributions $(S_{i_1}, \ldots, S_{i_\ell})$ for non authorised groups are always the uniform distributions of ℓ random variables, though the general definition admits more complicated constructions.

independent uniformly distributed binary strings in $\{0,1\}^m$. The last share S_n (for the n-th participant) is defined as the bitwise XOR of $S_1, \ldots, S_{m-1}$ and the m-bit secret $k_1 \ldots k_m$.

Example $1'$ (*again, only all n participants together know the secret*). We let $\mathcal{K} = \mathbb{Z}/p\mathbb{Z}$ and define the scheme as follows. For every secret $k \in \mathbb{Z}/p\mathbb{Z}$ we sample the shares $S_1, \ldots, S_{n-1}$ as independent uniformly distributed random values in $\mathbb{Z}/p\mathbb{Z}$. The last share S_n (for the n-th participant) is defined as

$$k - S_1 - \ldots - S_{n-1} \mod p.$$

Example 2 revisited (*threshold secret sharing scheme for $n = 3$ and $t = 2$, every two participants of three know the secret*). We fix a prime number $p > 3$ and let $\mathcal{K} = \mathbb{Z}/p\mathbb{Z}$. We fix three (pairwise distinct) non-zero elements $a_1, a_2, a_3 \in \mathbb{Z}/p\mathbb{Z}$. For every secret $k \in \mathbb{Z}/p\mathbb{Z}$ the Dealer sample the shares S_1, S_2, S_3 as follows. We choose a random element $c \in \mathbb{Z}/p\mathbb{Z}$, define a function (a polynomial of degree at most 1)

$$f(x) = cx + k \mod p$$

and let

$$S_1 = f(a_1),\ S_2 = f(a_2),\ S_3 = f(a_3).$$

In other words, we choose a random polynomial $f(x) = cx + c_0$ incident to the point $(0, k)$ (i.e., the constant terms is equal to $c_0 = k$) and take its values at the points a_i as the shares of the secret S_i for $i = 1, 2, 3$.

In the class we verified that this construction satisfies the definition of a secret sharing scheme.

Example 3 revisited: threshold secret sharing scheme for $t = 3$ and $n = 5$ (*every three participants know the secret*). We fix a prime number $p > 3$ and let $\mathcal{K} = \mathbb{Z}/p\mathbb{Z}$. We fix 5 (pairwise distinct) non-zero elements $a_1, \ldots, a_5 \in \mathbb{Z}/p\mathbb{Z}$. For every secret $k \in \mathbb{Z}/p\mathbb{Z}$ we sample the shares $S_1, \ldots, S_5$ as follows. We choose at random (uniformly and independently) elements $c_1, c_2 \in \mathbb{Z}/p\mathbb{Z}$, define a function (a polynomial of degree at most 2)

$$f(x) = c_2 x^2 + c_1 x + k$$

and let $S_i = f(a_i)$ for $i = 1, \ldots, 5$.

In the class we proved that these schemes respect conditions (I) and (II) from the definition of a secret sharing scheme.

Digression 1: arithmetic modulo a prime number. If p is a prime number then for every integer $a \neq 0 \mod p$ there exists an integer a' such that $a \cdot a' = 1 \mod p$. In other words, every non-zero element in $\mathbb{Z}/p\mathbb{Z}$ has an inverse.

Given p and a we can find such an a' algorithmically. A naive is the brute-force search: we try all numbers in the list $1, 2, \ldots, p-1$ until we find a' such that $a \cdot a' = 1 \mod p$. A more efficient approach uses the extended euclidean algorithm.

Digression 2: roots of a polynomial. To show that the secret sharing scheme defined above satisfies the conditions (I) and (II), we used a well-known theorem from algebra:

Theorem 1. *Let p be a prime number and $c_0, \ldots, c_{d-1}$ be elements from $\mathbb{Z}/p\mathbb{Z}$. Then the polynomial*

$$f(x) = c_0 + c_1 x + \ldots + c_d x^d \mod p$$

cannot have more than d roots in $\{0, 1, \ldots, p-1\}$ (unless all c_i are equal to zero).

Corollary 1. *The graphs of two polynomials $g(x)$ and $h(x)$ of degree $\geq d$ have at most d points of intersection in the arithmetic $\mathbb{Z}/p\mathbb{Z}$, i.e., there is at most d points $a_i \in \{0, \dots, p-1\}$ such that*

$$g(a_i) = h(a_i) \mod p.$$

Sketch of the proof. The degree of the polynomial $f(x) := g(x) - h(x)$ is at most d, and therefore it cannot have more than d roots modulo p.

N.B.: We stress that Theorem 1 is true only for prime numbers p.

References

[1] B. Martin. Codage, cryptologie et applications. PPUR presses polytechniques, 2004

[2] V. V. Yaschenko, Cryptography: An Introduction, AMS, 2002

[3] C. Walter. Arithmétique. Univ. de Nice, 2011. Chapitre 3.
`https://math.unice.fr/~walter/L1_Arith/`