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

16/09/2024. Lecture 2.

1 Secret sharing.

In this chapter we introduce 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, ...) among a group of m 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. Non-authorised groups of participants should get even partial information on the secret key. To this ends, we will provide each participants with a *share* of the secret. In what follows we discuss several natural and practically interesting examples. In the next lecture we will give a general abstract definition of secret sharing.

Example 1 (unanimity rule). We may require that only all m participants together can get the secret. In the class we discussed in full detail the cases $m = 2$ and $m = 3$ and then addressed the general case, with an arbitrary number of participants m.

We denote $\mathcal{K}$ be the space of all potential secrets. In all our examples below we let $\mathcal{K} = \{0,1\}^n$ for some integer n or $\mathcal{K} = \mathbb{Z}/p\mathbb{Z}$ for some integer number p. We always assume that a secret $k \in \mathcal{K}$ is chosen at random with a uniform distribution. A secret sharing scheme with m participants is a randomised algorithm (*Dealer*) that takes k as an input and produces a tuple of shares $(s_1, \ldots, s_m)$ for the participants $i = 1, \ldots, m$,

$$\text{Dealer}(k) \to (s_1, \ldots, s_m).$$

This means that for each $k \in \mathcal{K}$ we have a probability distribution $p_k(s_1, \ldots, s_m)$

$$p_k(s_1, \ldots, s_m) := \text{Prob}^{(k)}\left[[\text{share for participant no. 1}] = s_1, \ldots, [\text{share for participant no. } m] = s_m\right],$$

which is the distribution of random *shares* compatible with the value of the secret key k. These distributions must respect the following two conditions: (I) all participants together can reconstruct the secret, and (II) if at least one participant is messing, the other participants have no information on the secret. More formally, these requirements can be reformulated as follows.

(I) the random variables

$$\langle[\text{share for participant no. 1}], \ldots, [\text{share for participant no. } m]\rangle$$

all together contain enough information to reconstruct the secret key. This means that for every vector of value $(s_1, \ldots, s_m)$ there can be only one secret $k \in \mathcal{K}$ such that

$$\text{Prob}^{(k)}\left[[\text{share for participant no. 1}] = s_1, \ldots, [\text{share for participant no. } m] = s_m\right] > 0$$

(II) For $\ell < m$, for any group of ℓ participants $\{i_1, \ldots, i_\ell\}$, the random variables

$$\langle[\text{share for participant no. } i_1], \ldots, [\text{share for participant no. } i_\ell]\rangle$$

contain *no* information on k. This means that the conditional probability

$$\text{Prob}\left[[\text{secret key}] = k \;\middle|\; [\text{share for participant no. } i_1] = s_1, \ldots, [\text{share for participant no. } i_\ell] = s_{i_\ell}\right]$$

is equal to the unconditional probability $\text{Prob}\left[[\text{secrte key}] = k\right]$.

Remark 1. Condition (II) can be equivalently reformulated as follows: for all $k \in \mathcal{K}$ the restrictions of the distribution

$$\mathrm{Prob}^{(k)}\,[\text{[share for participant no. } i_1] = s_1, \ldots, \text{[share for participant no. } i_\ell] = s_m]$$

on the coordinates $i_1, \ldots, i_\ell$ (for $\ell < m$) are identical for all values of the secret key k. Thus, for all values of the secret key k, one and the same sampling procedure is used to produce

$$\mathrm{Prob}^{(k)}\,[\text{[share for participant no. } i_1] = s_{i_1}, \ldots, \text{[share for participant no. } i_\ell] = s_{i_\ell}]\,.$$

So a group of $\ell < m$ participants cannot see any difference between different values of k.

Case 1. For $\mathcal{K} = \{0,1\}^n$ we can construct the scheme that respects the requirements (I) and (II) as follows. For every secret $k = (k^1 \ldots k^n) \in \{0,1\}^n$ we sample the shares

$(*)_1$ [share for participant no. 1], ..., [share for participant no. $(m-1)$]

(all except for one) as independent random variables, each of them uniformly distributed on $\{0,1\}^n$. The very last share (for the m-th participant) is defined as the bitwise XOR of the $(m-1)$ sampled bit-strings in $(*)_1$ and of the n-bit secret $k = (k_1 \ldots k_n)$.

Remark 2. As k is uniformly distributed on $\mathcal{K} = \{0,1\}^n$, then the joint distribution of

$(**)_1$ ([secret key], [share for participant no. 1], ..., [share for participant no. m])

can be described in more symmetric terms: we take the uniform distribution on the set of all tuples $(**)_2$ where the bitwise XOR for each position is equal to 0. Observe that there are $\underbrace{2^n \times 2^n \times \ldots \times 2^n}_{m} = 2^{nm}$ such tuples; if we sample a random secret key and then corresponding (random) shares, then each possible tuple $(**)_1$ can be obtained with probability $1/2^{nm}$.

In the class we discussed why this construction respects the required properties (I) and (II), i.e., why all parties together know the secret key, and if at least one participant is messing then the other ones together have no information on the secret key.

Case 2. For $\mathcal{K} = \mathbb{Z}/q\mathbb{Z}$ we can construct a secret sharing scheme as follows. For every secret $k \in \mathbb{Z}/q\mathbb{Z}$ we sample the shares

$(*)_2$ [share for participant no. 1], ..., [share for participant no. $(m-1)$]

as independent uniformly distributed random values in $\mathbb{Z}/q\mathbb{Z}$. The last share (for the m-th participant) is defined as

$$k - S_1 - \ldots - S_{m-1} \mod q.$$

If k is uniformly distributed on $\mathbb{Z}/q\mathbb{Z}$ then the joint distribution of

$(**)_2$ ([secret key], [share for participant no. 1], ..., [share for participant no. m])

can be described in more symmetric terms: we take the uniform distribution on the set of all tuples $(**)_2$ where the sum of all values modulo q is equal to 0. There are q^m such tuples. if we sample a random secret key and then corresponding (random) shares, then then each possible tuple $(**)_2$ is obtained with the probability $1/q^m$.

For this scheme we also discussed in the class why this construction respects the required properties (all parties together know the secret key, and if at least one participant is messing then the other ones together have no information on the secret key).

Example 2 (threshold secret sharing scheme for $m = 3$ participants and threshold $t = 2$, i.e., every two participants of three can access the secret).

In this example every two participants know the secret key while every single participant has no information on the secret key. Let $\mathcal{K}$ be again the space of all potential secrets. Fromally speaking, a secret sharing scheme with three participants is a randomised algorithm (*Dealer*) that takes k as an input and produces a tuple of shares (s_1, s_2, s_3) for the participants,

$$\text{Dealer}(k) \to (s_1, s_2, s_3).$$

In other words, for each $k \in \mathcal{K}$ we have a probability distribution $p_k(s_1, s_2, s_3)$, which is

$$\text{Prob}^{(k)}\left[\text{[share for participant no. 1]} = s_1, \text{[share for participant no. 2]} = s_2, \text{[share for participant no. 3]} = s_3\right].$$

These distributions must respect the following two conditions:

(I) every pair of random variables $\langle$[share for participant no. i_1], [share for participant no. i_2]$\rangle$ contains enough information to reconstruct uniquely the secret key k,

(II) every single random variable [share for participant no. i_1] is independent with k.

A scheme that satisfies these requirements can be defined as follows. We fix a prime number $p > 3$ and let $\mathcal{K} = \mathbb{Z}/p\mathbb{Z}$. We fix three (pairwise distinct) non-zero elements $a_1, a_2, a_3 \in \mathbb{Z}/p\mathbb{Z}$. These parameters define the scheme (they are public, so everyone including the adversary may know p, a_1, a_2, a_3). Now we specify the procedure of secret sharing. For every secret $k \in \mathbb{Z}/p\mathbb{Z}$, the Dealer samples

$$(\text{[share for participant no. 1]}, \text{[share for participant no. 2]}, \text{[share for participant no. 3]})$$

as follows. The Dealer lets $c_0 = k$, smaples a random element $c_1 \in \mathbb{Z}/p\mathbb{Z}$, and then defines a function (a polynomial of degree at most 1)

$$L(x) = c_0 + c_1 x \mod p$$

and lets

$$\text{[share for participant no. } i\text{]} := L(a_i),\ i = 1, 2, 3.$$

In other words, we choose a random polynomial $L(x) = c_1 x + c_0$ incident to the point with coordinates $(0, k)$ (which means that the constant term c_0 of $L(x)$ is equal to k) and take its values $L(a_i)$ at the points a_i (for $i = 1, 2, 3$) as the shares of the secret given to the participants.

In the next lecture we will give a complete proof of correctness of this scheme.

Example 3 (threshold secret sharing scheme for $m = 5$ participants and threshold $t = 3$, i.e., every three participants know the secret).

We fix a prime number $p > 5$ 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 of the secret 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)

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

and let [share for participant no. i] $= L(a_i)$ for $i = 1, \ldots, 5$.

In the next lecture we will give a complete proof of correctness of this scheme.

2 Modular arithmetic.

In this section we discuss some algebraic facts useful for cryptographic constructions.

Proposition 1. *For all positive natural numbers x, y there exist integer (non necessary positive) numbers v, w such that*

$$x \cdot v + y \cdot w = \mathrm{PGCD}(x, y).$$

Sketch of the proof: Let us define

$$\mathcal{I}_{x,y} = \{z \mid \text{there exist integer numbers } v, w \text{ such that } z = x \cdot v + y \cdot w\}$$

Let c be the minimal positive element of $\mathcal{I}_{x,y}$. We claim that $c = \mathrm{PGCD}(x, y)$ (which implies the proposition).

Indeed, it is obvious that $\mathrm{PGCD}(x, y)$ divides every element of $\mathcal{I}_{x,y}$ (including the number c). It remains to show that c divides $\mathrm{PGCD}(x, y)$. To this end, we show that c divides x and y.

Claim. c divides x.

Proof of claim: For the sake of contradiction we assume that c does not divide x. Let us consider the series of numbers

$$c, 2c, 3c, \ldots$$

It is easy to see that all these numbers belong to $\mathcal{I}_{x,y}$. Observe that x must be sandwiched between two neighbouring elements in this series,

$$kc < x < (k + 1)c.$$

Observe that $x - kc$ is a positive number strictly smaller than c and it belongs to $\mathcal{I}_{x,y}$. We get a contradiction with the definition of c.

A similar argument proves that c divides y. Thus, $c = \mathrm{PGCD}(x, y)$ and the proposition is proven. □

For every integer $n > 0$, in the modular arithmetic $\mathbb{Z}/n\mathbb{Z}$ we have the usual properties of addition and multiplication (modulo n):

- $\forall x\; x + 0 = x \mod n$
- $\forall x \exists x'\; x + x' = 0 \mod n$
- $\forall x \forall y\; x + y = y + x \mod n$
- $\forall x \forall y \forall z\; (x + y) + z = x + (y + z) \mod n$
- $\forall x\; x \cdot 1 = x \mod n$
- $\forall x \forall y\; x \cdot y = y \cdot x \mod n$
- $\forall x \forall y \forall z\; (x \cdot y) \cdot z = x \cdot (y \cdot z) \mod n$
- $\forall x \forall y \forall z\; x \cdot (y + z) = x \cdot y + x \cdot z \mod n$

Proposition 2. *If n is a prime number, than for all integer $x \neq 0 \mod n$ there exists an integer x' such that $x \cdot x' = 1 \mod n$.*

Proof: As n is prime (by the condition of the theorem) and does not divide x (since $x \neq 0 \mod n$), we conclude that n and x are co-prime, and

$$\mathrm{PGCD}(n, x) = 1.$$

Hence, there exist integer numbers v and w such that

$$x \cdot v + n \cdot w = 1.$$

It follows that $x \cdot v = 1 \mod n$, and we are done. □

Proposition 3. *If n is a prime number and $x \cdot y = 0 \mod n$, then $x = 0 \mod n$ or $y = 0 \mod n$.*

Proof: Assume that $x \neq 0 \mod n$. Then there exist integer numbers v and w such that

$$x \cdot v + n \cdot w = 1.$$

It follows that

$$x \cdot y \cdot v + n \cdot w \cdot y = y.$$

In the last expression, in the left-hand side the term $x \cdot y$ is divisible by n (by the condition of the theorem) and the term $n \cdot w \cdot y$ is divisible by n (trivial). Hence, y is divisible by n, and we are done. □

Lemma 1. $x^n - a^n = (x - a)(x^{n-1} + x^{n-2}a + x^{n-3}a^2 + \ldots + a^{n-1})$

(Proven in the class.)

Proposition 4. *Let*

$$L(x) = c_0 + c_1 x + \ldots + c_d x^d$$

be a polynomial of degree d with integer coefficients. Assume that for some integer a

$$L(a) = 0 \mod n.$$

Then there exists a polynomial $R(x)$ of degree $d - 1$ with integer coefficients such that

$$L(x) = (x - a)R(x) \mod n$$

Sketch of the proof: We know that

$$c_0 + c_1 a + c_2 z^2 + \ldots + c_d a^d = 0 \mod n.$$

Therefore, in the arithmetic modulo n

$$\begin{aligned} L(x) &= \quad c_0 + c_1 x + c_2 x^2 + \ldots + c_d x^d \\ &\quad -c_0 - c_1 a - c_2 a^2 - \ldots - c_d a^d \\ &= c_1(x - a) + c_2(x^2 - a^2) + \ldots + c_d(x^d - a^d) \\ &= c_1(x - a) + c_2(x - a)(x + a) + \ldots + c_d(x - a)(x^{n-1} + x^{n-2}a + x^{n-3}a^2 + \ldots + a^{n-1}) \\ &= (x - a)(\ldots\ldots\ldots\ldots) \end{aligned}$$

□

Theorem 1. *Let n be a prime number and $c_0, \ldots, c_d$ be be integer numbers. Then the polynomial*

$$L(x) = c_0 + c_1 x + \ldots + c_d x^d \mod n$$

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

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

We will re-discuss this theorem in the next lecture.

References

[1] H. Tyagi and S. Watanabe. Information-Theoretic Cryptography. Cambridge Univ. Press 2023. [section 11.1]

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