The shares are distributed securely to the participants from the set $\mathcal{P} = \{P_1, \ldots, P_t\}$.

At the pooling time, the combiner Clara can reconstruct the secret only if she is given all shares as

$$k = \sum_{i=1}^{t} s_i \pmod{p}.$$

Obviously, any $(t-1)$ or fewer shares provide no information about the secret k.

9.1.2 Shamir Scheme

Shamir [465] used Lagrange polynomial interpolation to design (t, n) threshold schemes. All calculations are done in $GF(p)$ where the prime p is a big enough integer (so the secret is always smaller than p).

A (t, n) Shamir scheme is constructed by the dealer Don. First Don chooses n different points $x_i \in GF(p)$ for $i = 1, \ldots, n$. These points are public. Next Don selects at random coefficients $a_0, \ldots, a_{t-1}$ from $GF(p)$. The polynomial $f(x) = a_0 + a_1 x + \ldots + a_{t-1} x^{t-1}$ is of degree at most $(t-1)$. The shares are $s_i = f(x_i)$ for $i = 1, \ldots, n$, and the secret is $k = f(0)$. The share s_i is distributed to the participant $P_i \in \mathcal{P}$ via a secure channel and is kept secret.

When t participants agree to cooperate, the combiner Clara takes their shares and tries to recover the secret polynomial $f(x)$. She knows t points on the curve $f(x)$

$$(x_{i_j}, f(x_{i_j})) = (x_{i_j}, s_{i_j}) \text{ for } j = 1, \ldots, t.$$

These points produce the following system of equations:

$$\begin{aligned} s_{i_1} &= a_0 + a_1 x_{i_1} + \ldots + a_{t-1} x_{i_1}^{t-1} \\ s_{i_2} &= a_0 + a_1 x_{i_2} + \ldots + a_{t-1} x_{i_2}^{t-1} \\ &\vdots \\ s_{i_t} &= a_0 + a_1 x_{i_t} + \ldots + a_{t-1} x_{i_t}^{t-1} \end{aligned} \tag{9.2}$$

The system (9.2) has a unique solution for $(a_0, \ldots, a_t)$, since

$$\Delta = \begin{vmatrix} 1 & x_{i_1} & \ldots & x_{i_1}^{t-1} \\ 1 & x_{i_2} & \ldots & x_{i_2}^{t-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_{i_t} & \ldots & x_{i_t}^{t-1} \end{vmatrix}$$

is a Vandermonde determinant different from zero. The Lagrange interpolation formula allows to determine the polynomial $f(x)$ of degree $(t-1)$ from the t different points (x_{i_j}, s_{i_j}), thus

$$f(x) = \sum_{j=1}^{t} s_{i_j} \prod_{\substack{1 \le \ell \le t \\ \ell \ne j}} \frac{x - x_{i_\ell}}{x_{i_j} - x_{i_\ell}}.$$

The secret $k = f(0)$, therefore we obtain

$$k = a_0 = \sum_{j=1}^{t} s_{i_j} b_j$$

where,

$$b_j = \prod_{\substack{1 \le \ell \le t \\ \ell \ne j}} \frac{x_{i_\ell}}{x_{i_\ell} - x_{i_j}}.$$

If Clara knows $(t-1)$ shares, she cannot find the unique solution for $k = a_0$ as the system (9.2) contains $(t-1)$ equations with t unknowns. The security is discussed later.

Consider a simple $(3, 6)$ Shamir scheme over $GF(7)$. The dealer selects six public numbers, say $x_i = i$ for $i = 1, \dots, 6$, and a random polynomial of degree at most 2. Let it be $f(x) = 5 + 3x + 2x^2$. Shares are

$$s_1 = f(x_1) = 3; \quad s_2 = f(x_2) = 5;$$
$$s_3 = f(x_3) = 4; \quad s_4 = f(x_4) = 0;$$
$$s_5 = f(x_5) = 0; \quad s_6 = f(x_6) = 4.$$

The shares are sent to the corresponding participants in a secure way.

Assume that three participants P_1, P_3 and P_6 cooperate and have revealed their shares to the combiner. Clara solves the following system of equations:

$$3 = a_0 + a_1 + a_2$$
$$4 = a_0 + 3a_1 + 2a_2$$
$$4 = a_0 + 6a_1 + a_2$$

According to the Lagrange interpolation formula, the coefficients $b_1 = 6$, $b_2 = 6$, and $b_3 = 3$ and the secret $k = a_0 = b_1 s_1 + b_2 s_3 + b_3 s_6 = 5$.