Ex. Suppose $p=17$, $t=3$, $n=5$ and I want to distribute $s=13$

Then, $f(x) = 13 + 10x + 2x^2$

$\Rightarrow$ To player 1, $(1, f(1)) = (1, 8)$

player 2, $(2, f(2)) = (2, 17)$

player 3, $(3, f(3)) = (3, 10)$

player 4, $(4, f(4)) = (4, 0)$

player 5, $(5, f(5)) = (5, 11)$

denoted by $\langle 13 \rangle$

Let $f'(x) = a_0 + a_1 x + a_2 x^2$ where $a_i \in \mathbb{Z}_p$.

Then,
$$\begin{cases} a_0 + a_1 + a_2 = 8 \\ a_0 + 3a_1 + 9a_2 = 10 \\ a_0 + 5a_1 + 25a_2 = 11 \end{cases}$$

$\Rightarrow$ We can obtain a_0, a_1 and a_2 by solving equations.

<u>Multiplication by SPDZ</u>. (Goal: compute $\langle xy \rangle$ given some $\langle x \rangle$ and $\langle y \rangle$)

Through homomorphic encryption, generate $\{\langle a \rangle, \langle b \rangle, \underset{}{\overset{c}{\overset{\shortparallel}{\langle ab \rangle}}}\}$.

Then, i) each party broadcasts $x_i - a_i$ and $y_i - b_i$. $\rightarrow \{a, b, c\}$ cannot reuse.
$\left[\because (x_1 - a) - (x_2 - a) = x_1 - x_2\right]$

ii) each party computes $x-a$ and $y-b$.

iii) each party computes $c_i + (x-a)b_i + (y-b)a_i =: z_i$.

iv) one party chosen arbitrary adds $(x-a)\cdot(y-b)$

v) $z = \sum z_i + (x-a)\cdot(y-b) = \sum(c_i + (x-a)\cdot b_i + (y-b)a_i) + (x-a)(y-b)$

$= c + (x-a)\cdot b + (y-b)a + (x-a)(y-b)$.