Each ω_i is non-zero and can be easily computed from public information. Note that the constant term of a polynomial of degree at most $t-1$ is not given through $t-1$ equations of the form $f(i) = s_i$. Furthermore, each possible value for the constant term is equally possible. A coalition of $t-1$ players can therefore neither compute the secret nor get any information about it.

2.3 Verifiable Secret Sharing Scheme

A Verifiable Secret Sharing Scheme (VSS) prevents the dealer from cheating. In a VSS, each player can verify his share. If the dealer distributes inconsistent shares, he will be detected. Pedersen presented a non-interactive VSS in [7] which we will use in this paper. His scheme is as follows.

Assume the dealer has a secret $s \in Z_q$ and a random number $s' \in Z_q$, and is committed to the pair (s, s') through public information $C_0 = sG + s'H$. The secret s can be shared among $P_1, ..., P_n$ as follows.

The dealer performs the following steps

1. Choose random polynomials

$$f(u) = s + f_1 u + \cdots + f_{t-1} u^{t-1}, \;\; f'(u) = s' + f'_1 u + \cdots + f'_{t-1} u^{t-1}$$

   where $s, s', f_j, f'_j \in Z_q$. Compute $(s_i, s'_i) = (f(i), f'(i))$ for $i \in \{1, ..., n\}$.

2. Send (s_i, s'_i) secretly to player P_i for $1 \leq i \leq n$.

3. Broadcast the values $C_j = f_j G + f'_j H$ for $1 \leq j \leq t-1$.

Each player P_i performs the following steps

1. Verify that

$$s_i G + s'_i H = \sum_{j=0}^{t-1} i^j C_j. \tag{1}$$

   If this is false, broadcast a *complaint* against the dealer.

2. For each complaint from a player i, the dealer defends himself by broadcasting the value $(f(i), f'(i))$ that satisfies the checking equation (1).

3. Reject the dealer if

   - he received more than t complaints in step 1, or
   - he answered to a complaint in step 2 with values that violate Eq. (1).

Pedersen proved that any coalition of less than t players cannot get any information about the shared secret, provided that the discrete logarithm problem in E is hard (see [7]).