2.4 Generating a random secret

For the key generation phase of our scheme, it is necessary to generate a random shared secret in a distributed way. The early protocol proposed by Feldman [4] has been shown to have a security flaw, and a secure protocol has been proposed in [11]. We will use the secure protocol for our schemes and recall it in the following.

Suppose a trusted dealer chooses r, r' at random, broadcasts $Y = rG$ and then shares r using among the players P_i using Pedersen's VSS as described above. We would like to achieve this situation without a trusted dealer. This can be achieved by the following protocol (see [11] for more details).

Each player P_i performs the following steps

1. Each player P_i chooses $r_i, r_i' \in Z_q$ at random and verifiably shares (r_i, r_i'), acting as the dealer according to Pedersen's VSS described above. Let the sharing polynomials be $f_i(u) = \sum_{j=0}^{t-1} a_{ij} u^j$, $f_i'(u) = \sum_{j=0}^{t-1} a_{ij}' u^j$, where $a_{i0} = r_i, a_{i0}' = r_i'$, and let the public commitments be $C_{im} = a_{im}G + a_{im}'H$ for $i \in \{0, ..., t-1\}$.
2. Let H_0 :=$\{P_j | P_j$ is not detected to be cheating at step 1$\}$. The distributed secret value r is not explicitly computed by any party, but it equals $r = \sum_{i \in H_0} r_i$. Each player P_i sets his share of the secret as $s_i = \sum_{j \in H_0} f_j(i) \bmod q$, and the value $s_i' = \sum_{j \in H_0} f_j'(i) \bmod q$.
3. Extracting $Y = \sum_{j \in H_0} r_i G$: Each player in H_0 exposes $Y_i = s_i G$ via Feldman's VSS (see [4]):
   3.1. Each player P_i in H_0 broadcasts $A_{ik} = a_{ik}G$ for $k \in \{0, ..., t-1\}$.
   3.2. Each player P_j verifies the values broadcast by the other players in H_0. Namely, for each $P_i \in H_0$, P_j checks if
   $$f_i(j)G = \sum_{k=0}^{t-1} j^k A_{ik}. \tag{2}$$
   If the check fails for an index i, P_j *complains* against P_i by broadcasting the values $(f_i(j), f_i'(j))$ that satisfy Eq. (1) but do not satisfy Eq. (2).
   3.3. For players P_i who received at least one valid complaint, i.e., values which satisfy Eq. (1) but do not satisfy Eq. (2), the other players run the reconstruction phase of Pedersen's VSS to compute $r_i, f_i(\cdot), A_{ik}$ for $k = 0, ..., t-1$ in the clear[1]. All players in H_0 set $Y_i = r_i G$.

After the executing this protocol, the following equations hold [11]:

$$\begin{aligned} Y &= rG \\ f(u) &= r + a_1 u + ... + a_{t-1} u^{t-1}, \text{ where } a_i = \sum_{j \in H_0} a_{ji}, \quad \text{and} \\ f(i) &= s_i. \end{aligned}$$

[1]Every player in H_0 simply reveals his share of r_i. Each player can then compute r_i by choosing t shares that satisfy Eq. (1)