be

$$(\alpha_1, ..., \alpha_n) \overset{(t,n)}{\longleftrightarrow} (x|Y, b_iG, H_0),\ i \in \{1, ..., t-1\}.$$

For each $j \in H_0$, α_j is the secret key share of P_j, and will be used to issue a partial signature for the key pair (x, Y).

4.2 Signature Issuing Protocol

Let m be a message and let h be a one-way hash function. Suppose that a subset $H_1 \subseteq H_0$ wants to issue a signature. They use the following protocol:

1. If $|H_1| < t$, stop. Otherwise, the subset H_1 generates a random shared secret as described in Section 2.4. Let the output be

$$(\beta_1, ..., \beta_n) \overset{(t,n)}{\longleftrightarrow} (e|V, c_iG, H_2),\ i \in \{1, ..., t-1\}.$$

2. If $|H_2| < k$, stop. Otherwise, each $P_i \in H_2$ reveals

$$\gamma_i = \beta_i + h(m, V)\alpha_i.$$

3. Each $P_i \in H_2$ verifies that

$$\gamma_k G = V + \sum_{j=1}^{t-1} c_j k^j G + h(m, V)\left(Y + \sum_{j=1}^{t-1} b_j k^j G\right) \text{ for all } k \in H_2.$$

   Let $H_3 := \{P_j | P_j \text{ not detected to be cheating at step 3}\}$.

4. If $|H_3| < t$, then stop. Otherwise, each $P_i \in H_3$ selects an arbitrary subset $H_4 \subseteq H_3$ with $|H_4| = t$ and computes σ satisfying $\sigma = e + h(m, V)x$, where

$$\sigma = \sum_{j \in H_4} \gamma_j \omega_j \text{ and } \omega_j = \prod_{\substack{h \neq j \\ h,j \in H_4}} \frac{h}{h-j}.$$

   The signature is (σ, V). To verify the signature, the same formula as in Schnorr's scheme applies:

$$\sigma G = V + h(m, V)Y \text{ and } \sigma \in Z_q.$$

Remarks

(1) The formula used in step 4 to compute σ holds because of the following: Let

$$F_3(u) := F_2(u) + h(m, V)F_1(u).$$

Then it follows that

$$F_3(0) = F_2(0) + h(m, V)F_1(0) = e + h(m, V)x = \sigma.$$

Therefore, by using Lagrange's formula (Section 2.2), the formula holds.