3. If $|H_2| < k$, stop. Otherwise, each $P_i \in H_2$ computes $C = V + V_u$ and reveals

$$\gamma_i = \beta_i + h(I_u, C)\alpha_i. \tag{3}$$

4. Each $P_i \in H_2$ verifies that

$$\gamma_l G = V + \sum_{j=1}^{t-1} c_j i^j G + h(I_u, C)\left(Y + \sum_{j=1}^{t-1} b_j i^j G\right) \text{ for all } l \in H_2. \tag{4}$$

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

5. If $|H_3| < t$ stop. Otherwise, each $P_i \in H_3$ selects an arbitrary group $H_4 \subseteq H_3$ with $|H_3| = t$ and computes σ satisfying $\sigma = e + h(I_u, C)x$ by

$$\sigma = \sum_{j \in H_4} \gamma_j \omega_j, \text{ where } \omega_j = \prod_{\substack{h \neq j \\ h, j \in H_4}} \frac{h}{h - j}. \tag{5}$$

The implicit certificate is (σ, C). At least t shareholders send the implicit certificate to the user.

6. The user computes his private key SK_u as $SK_u = c_u + \sigma$ and verifies the correctness of the certificate by the following equation:

$$SK_u G = C + h(I_u, C)Y \text{ and } \sigma \in Z_q. \tag{6}$$

To reconstruct the public key of the user from the implicit certificate, we use following formula:

$$\sigma PK_u = C + h(I_u, C)Y. \tag{7}$$

Remark A corrupt shareholder might send a wrong certificate $\tilde{\sigma}$ to the user. Since t shareholders send their certificates to the user, the user got at least one valid certificate (since there is at least one honest shareholder among t shareholders). To identify the valid certificate, the user simply checks for each σ if equation (6) holds.

8 Security

8.1 Correctness

We have to verify that the private key SK_u computed by the user corresponds to the public key PK_u implied by the implicit certificate (formula 7). Thus, we have to verify that following formula holds:

$$SK_u G \stackrel{!}{\equiv} C + h(I_u, C)PK_0. \tag{8}$$