Prover :

V=1	V=2	V=k
• $w, \{r_i, d_i; i \in [2, n]\}$ random • $x \leftarrow g^{\alpha}$ • $y = h^{\alpha} g^{1}$ • $a_1 = g^{w}$ • $b_1 = h^{w}$ • $a_2 = g^{r_2} x^{d_2}$ • $b_2 = h^{r_2} (\frac{y}{g^2})^{d_2}$ • … • $a_n = g^{r_2} x^{d_2}$ • $b_n = h^{r_n} (\frac{y}{g^n})^{d_n}$ • $c = Hash(x, y, ai, bi)$ • $d_1 = c - \sum_{i \neq 1} d_i$ • $r_1 = w - \alpha * d_1$	• $w, \{r_i, d_i; i \in [2, n]\}$ random • $x \leftarrow g^{\alpha}$ • $y = h^{\alpha} g^{2}$ • $a_1 = g^{r_1} x^{d_1}$ • $b_1 = h^{r_1} (\frac{y}{g^1})^{d_1}$ • $a_2 = g^{w}$ • $b_2 = h^{w}$ • … • $a_n = g^{r_2} x^{d_2}$ • $b_n = h^{r_n} (\frac{y}{g^n})^{d_n}$ • $c = Hash(x, y, ai, bi)$ • $d_2 = c - \sum_{i \neq 2} d_i$ • $r_2 = w - \alpha * d_2$	• $w, \{r_i, d_i; i \in [1, n] \backslash \{k\}\}$ random • $x \leftarrow g^{\alpha}$ • $y = h^{\alpha} g^{k}$ • $a_1 = g^{r_1} x^{d_1}$ • $b_1 = h^{r_1} (\frac{y}{g^1})^{d_1}$ • $a_k = g^{w}$ • $b_k = h^{w}$ • … • $a_n = g^{r_2} x^{d_2}$ • $b_n = h^{r_n} (\frac{y}{g^n})^{d_n}$ • $c = Hash(x, y, ai, bi)$ • $d_k = c - \sum_{i \neq k} d_i$ • $r_k = w - \alpha * d_k$

Send to the verifier : ZKP = $\{x, y, a_i, b_i, d_i, r_i\}$

Verifier :

$$c =? \sum_{i} d_i$$

$$a_i =? g^{r_i} x^{d_i}$$

$$b_i = h^{r_i} (\frac{y}{g^i})^{d_i}$$