

Election Authority

Choose domain parameters a, b, p, G, n, h

Choose private key d where $1 \leq d \leq n - 1$

Compute public key $\beta = dG$

Voter_i

Choose vote v_i on the curve

Choose private key a_i where $1 \leq a_i \leq n - 1$

Compute ephemeral key $a_i G = K_{E_i}$

Compute masking key $a_i \beta = K_{M_i}$

Compute encrypted vote $\check{v}_i = v_i + K_{M_i}$

Vote Average Calculator

Compute

$$\check{V} = \sum_{1 \leq i \leq n} \check{v}_i = \check{v}_1 + \check{v}_2 + \dots + \check{v}_n$$

Election Authority

Compute masking key

$$K_M = \sum_{1 \leq i \leq n} dK_{E_i}$$

Compute masking key inverse

$$= -K_M$$

Compute the sum of plaintext votes.

$$\check{V} - K_M = \check{v}_1 + \check{v}_2 + \dots + \check{v}_n - dK_{E_1} - dK_{E_2} - \dots - dK_{E_n}$$

$$= v_1 + a_1\beta + v_2 + a_2\beta + \dots + v_n + a_n\beta - (dK_{E_1} + dK_{E_2} + \dots + dK_{E_n})$$

$$= v_1 + a_1dG + v_2 + a_2dG + \dots + v_n + a_ndG - (da_1G + da_2G + \dots + da_nG)$$

$$= v_1 + v_2 + \dots + v_n = \sum_{1 \leq i \leq n} v_i$$