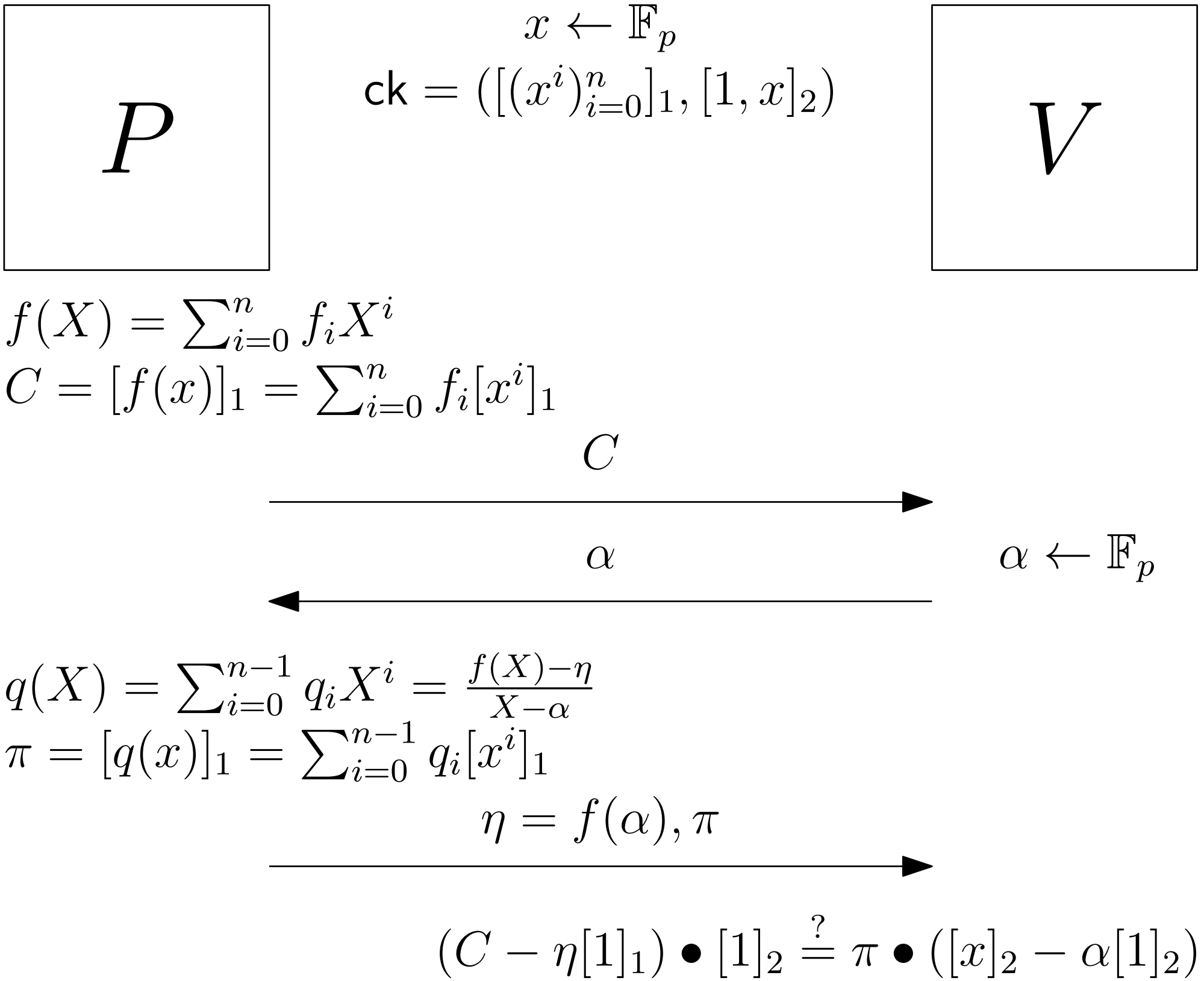
P
$x \leftarrow \mathbb{F}_p$
$\mathsf{ck} = ([(x^i)_{i=0}^n]_1, [1, x]_2)$
V
$f(X) = \sum_{i=0}^n f_i X^i$
$C = [f(x)]_1 = \sum_{i=0}^n f_i [x^i]_1$
C
α
$\alpha \leftarrow \mathbb{F}_p$
$q(X) = \sum_{i=0}^{n-1} q_i X^i = \frac{f(X)-\eta}{X-\alpha}$
$\pi = [q(x)]_1 = \sum_{i=0}^{n-1} q_i [x^i]_1$
$\eta = f(\alpha), \pi$
$(C - \eta[1]_1) \bullet [1]_2 \stackrel{?}{=} \pi \bullet ([x]_2 - \alpha[1]_2)$