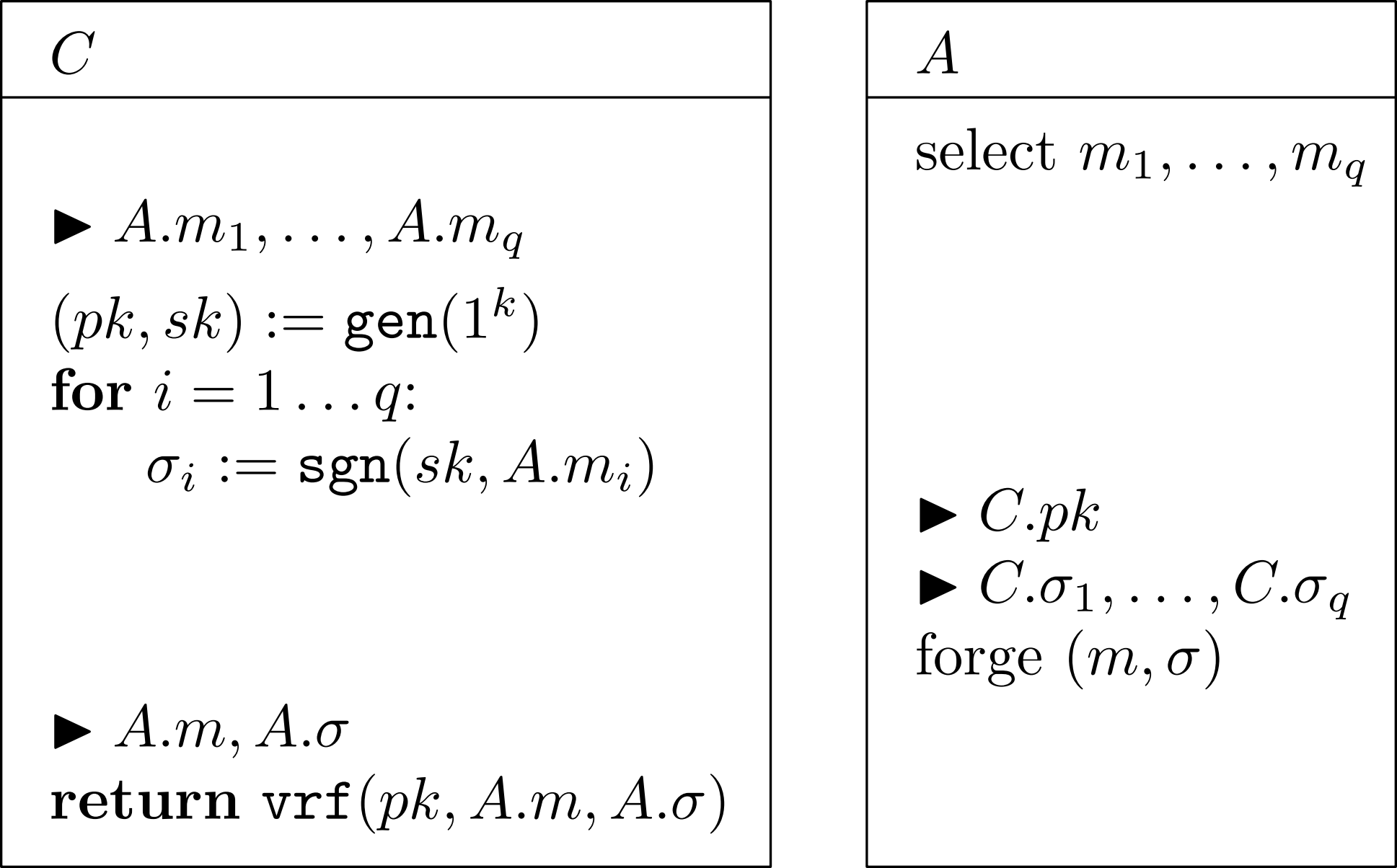
C
► $A.m_1, \ldots, A.m_q$
$(pk, sk) := \mathtt{gen}(1^k)$
for $i = 1 \ldots q$:
$\sigma_i := \mathtt{sgn}(sk, A.m_i)$
► $A.m, A.\sigma$
return $\mathtt{vrf}(pk, A.m, A.\sigma)$
A
select $m_1, \ldots, m_q$
► $C.pk$
► $C.\sigma_1, \ldots, C.\sigma_q$
forge (m, σ)