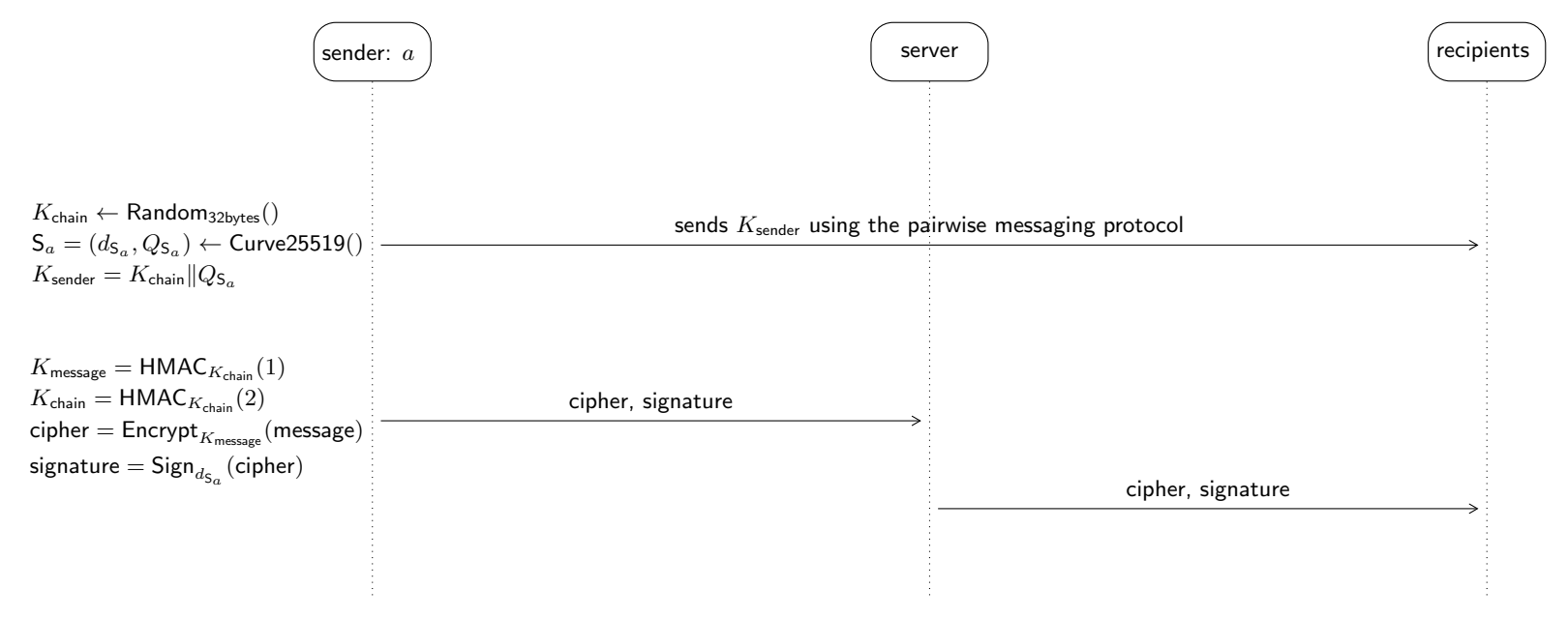
sender: a
server
recipients
$K_{\text{chain}} \leftarrow \text{Random}_{32\text{bytes}}()$
$\text{S}_a = (d_{\text{S}_a}, Q_{\text{S}_a}) \leftarrow \text{Curve25519}()$
$K_{\text{sender}} = K_{\text{chain}} \| Q_{\text{S}_a}$
sends K_{sender} using the pairwise messaging protocol
$K_{\text{message}} = \text{HMAC}_{K_{\text{chain}}}(1)$
$K_{\text{chain}} = \text{HMAC}_{K_{\text{chain}}}(2)$
$\text{cipher} = \text{Encrypt}_{K_{\text{message}}}(\text{message})$
$\text{signature} = \text{Sign}_{d_{\text{S}_a}}(\text{cipher})$
cipher, signature
cipher, signature