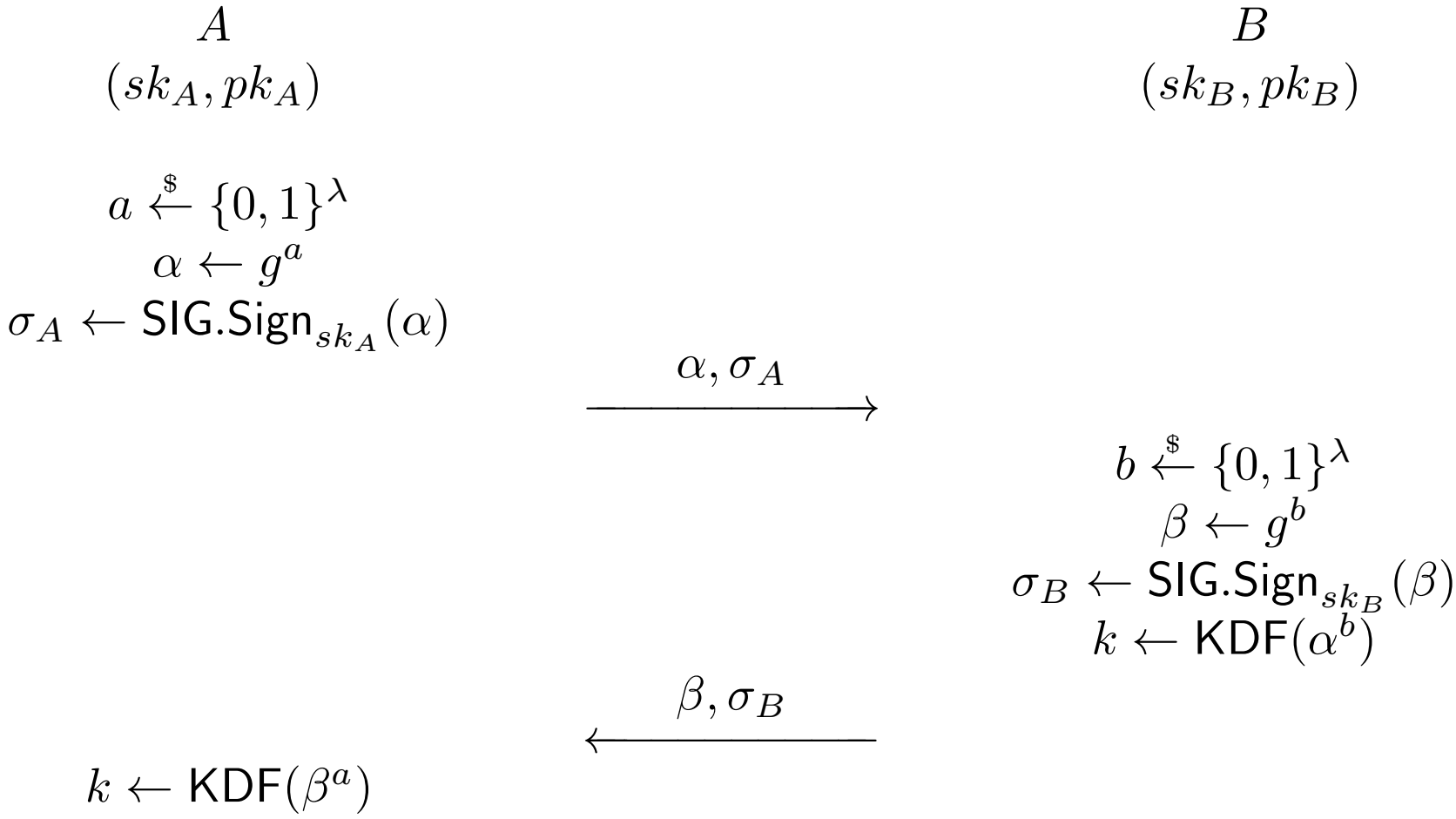
A
(sk_A, pk_A)
$a \xleftarrow{\$} \{0,1\}^\lambda$
$\alpha \leftarrow g^a$
$\sigma_A \leftarrow \mathsf{SIG.Sign}_{sk_A}(\alpha)$
α, σ_A
B
(sk_B, pk_B)
$b \xleftarrow{\$} \{0,1\}^\lambda$
$\beta \leftarrow g^b$
$\sigma_B \leftarrow \mathsf{SIG.Sign}_{sk_B}(\beta)$
$k \leftarrow \mathsf{KDF}(\alpha^b)$
β, σ_B
$k \leftarrow \mathsf{KDF}(\beta^a)$