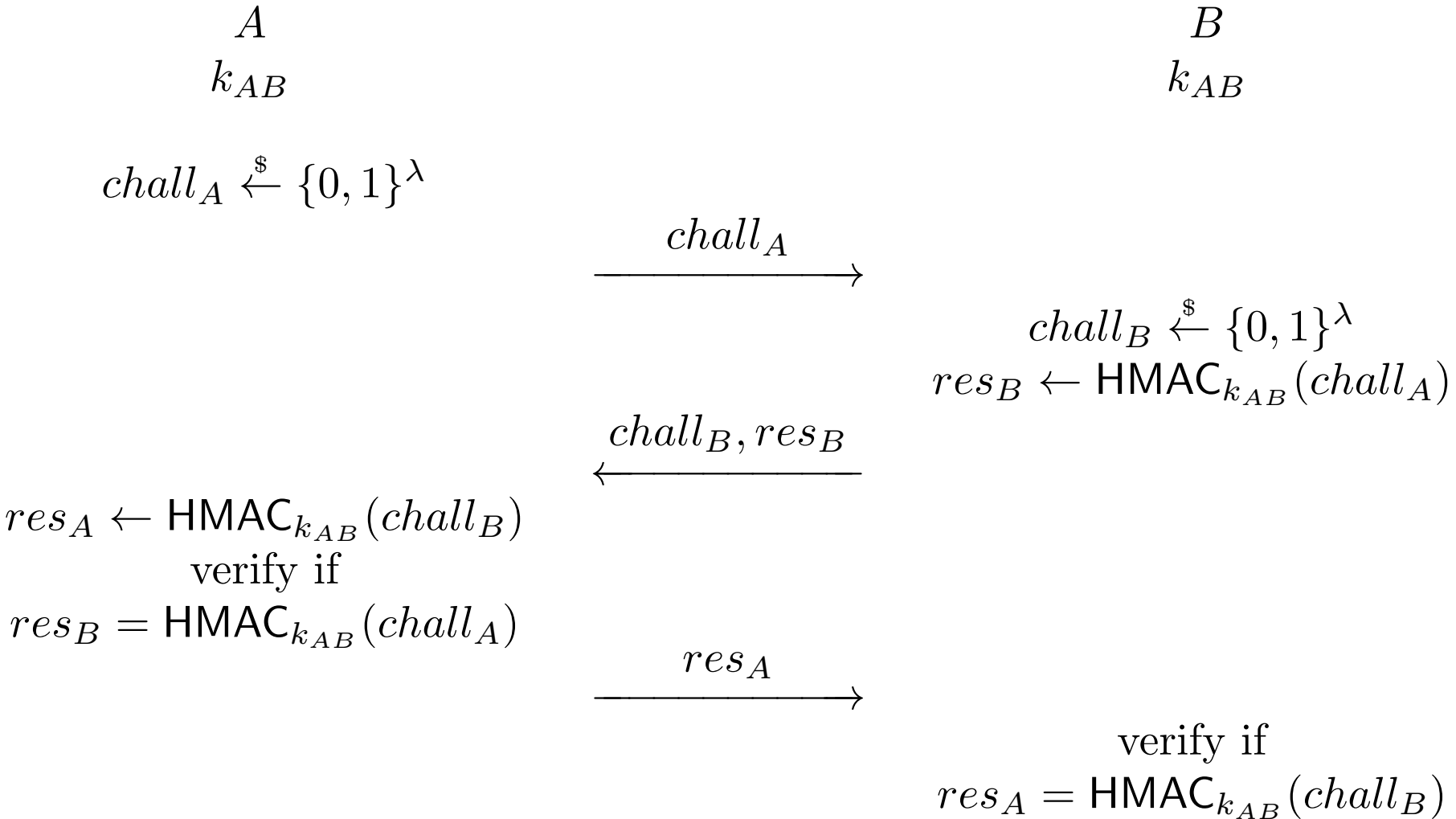
A
k_{AB}
$chall_A \xleftarrow{\$} \{0,1\}^\lambda$
$chall_A$
B
k_{AB}
$chall_B \xleftarrow{\$} \{0,1\}^\lambda$
$res_B \leftarrow \mathsf{HMAC}_{k_{AB}}(chall_A)$
$chall_B, res_B$
$res_A \leftarrow \mathsf{HMAC}_{k_{AB}}(chall_B)$
verify if
$res_B = \mathsf{HMAC}_{k_{AB}}(chall_A)$
res_A
verify if
$res_A = \mathsf{HMAC}_{k_{AB}}(chall_B)$