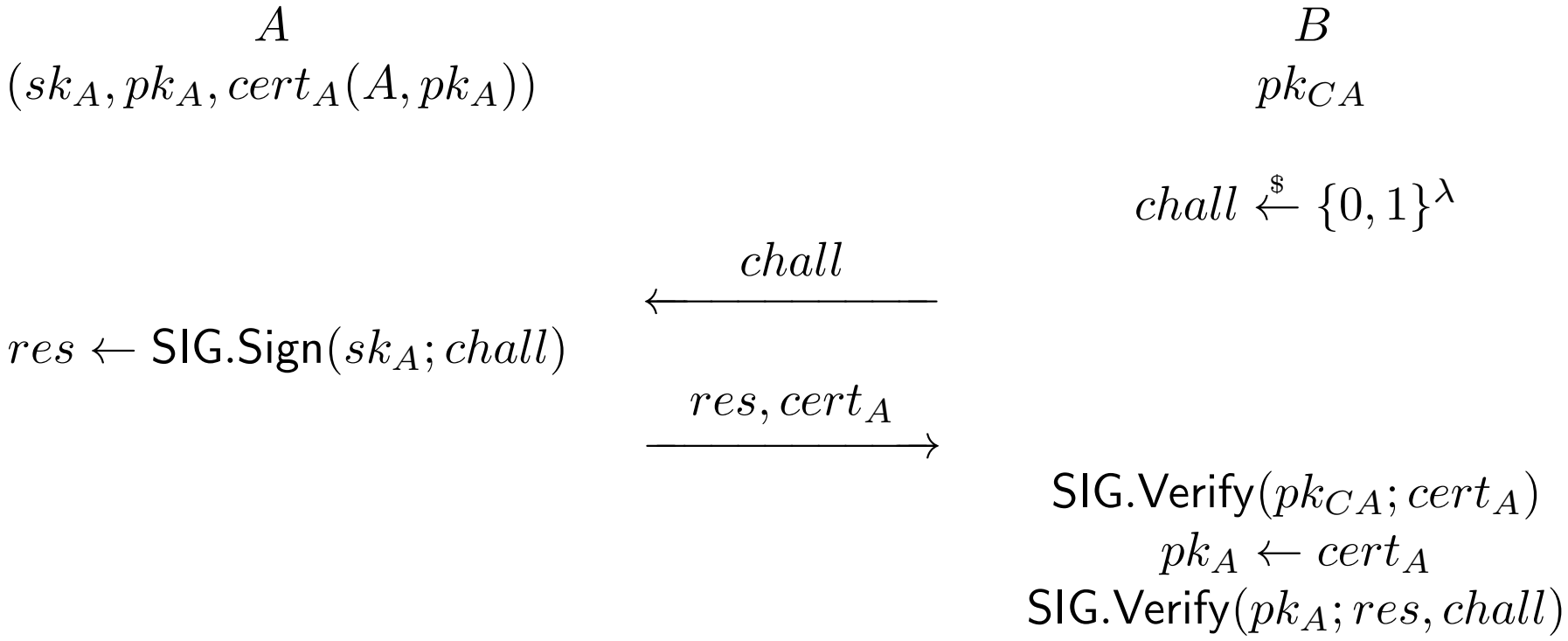
A
$(sk_A, pk_A, cert_A(A, pk_A))$
B
pk_{CA}
$chall \xleftarrow{\$} \{0,1\}^\lambda$
$chall$
$res \leftarrow \mathsf{SIG.Sign}(sk_A; chall)$
$res, cert_A$
$\mathsf{SIG.Verify}(pk_{CA}; cert_A)$
$pk_A \leftarrow cert_A$
$\mathsf{SIG.Verify}(pk_A; res, chall)$