

SS_{KEM}

$DH_{\{1,\dots,4\}}$

KDF

SK

