

Alice

1

$[R, PK_{\text{proxy}}]_A, K_{A,B}(SK_{\text{proxy}})$

Bob

2

$[R, PK_{\text{proxy}}]_A$

3

$PK_{\text{proxy}}(N)$

4

$N$

Server

