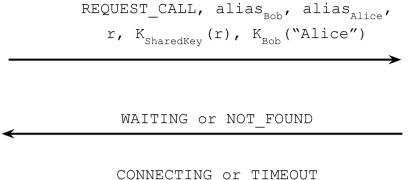
# RequestCall

### Alice

### <u>Network</u>

Generate random r



Verify a phone with alias alias<sub>Alice</sub> is registered to current LA.

Send a call requests if phone with alias alias<sub>Bob</sub> is found.

# **AcceptCall**

<u>Bob</u>

#### Network

Check if decryption of  $K_{Bob}$  ("Alice") is intelligible and corresponds to a contact whose current alias is alias<sub>Alice</sub>.

If answer, decrypt:

$$r' = K^{-1}(K_{\text{sharedKey}}(r))$$

ANSWER\_CALL, r'

Check if r' = r. Connect call if so, reject if not