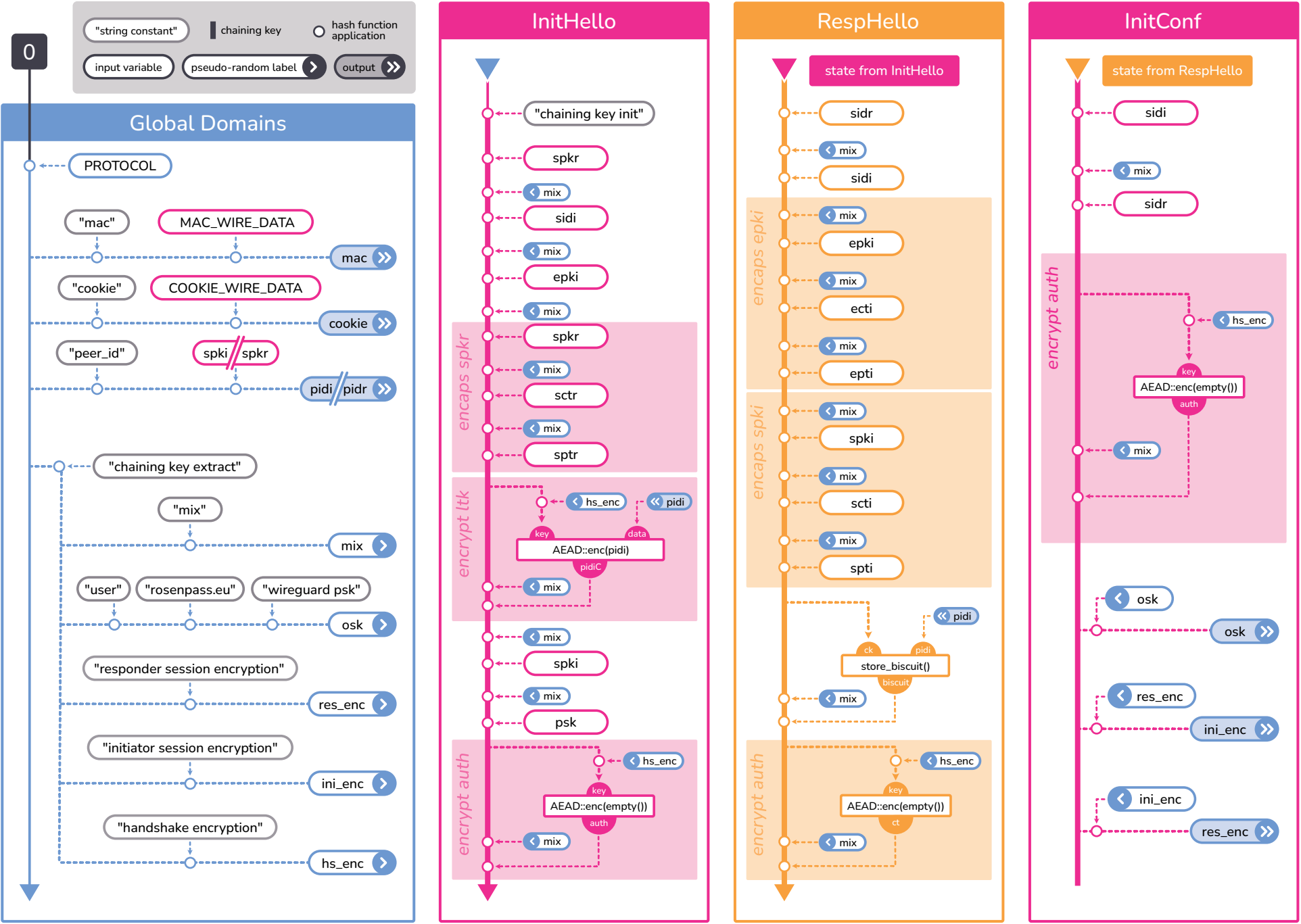
"string constant"
chaining key
hash function application
input variable
pseudo-random label
output
0
Global Domains
PROTOCOL
"mac"
MAC_WIRE_DATA
mac
"cookie"
COOKIE_WIRE_DATA
cookie
"peer_id"
spki
spkr
pidi
pidr
"chaining key extract"
"mix"
mix
"user"
"rosenpass.eu"
"wireguard psk"
osk
"responder session encryption"
res_enc
"initiator session encryption"
ini_enc
"handshake encryption"
hs_enc
InitHello
"chaining key init"
spkr
mix
sidi
epki
encaps spkr
sptr
encrypt ltk
hs_enc
pidi
key
data
AEAD::enc(pidi)
pidiC
spki
psk
encrypt auth
AEAD::enc(empty())
auth
RespHello
state from InitHello
sidr
encaps epki
ecti
epti
encaps spki
scti
spti
ck
store_biscuit()
biscuit
ct
InitConf
state from RespHello
encrypt auth
osk
res_enc
ini_enc