

0

"string constant"

chaining key

hash function  
application

input variable

pseudo-random label

output

## Global Domains

PROTOCOL

"mac"

MAC\_WIRE\_DATA

mac &gt;&gt;

"cookie"

COOKIE\_WIRE\_DATA

cookie &gt;&gt;

"peer\_id"

spki // spkr

pidi // pidr &gt;&gt;

"chaining key extract"

"mix"

mix &gt;

"user"

"rosenpass.eu"

"wireguard psk"

osk &gt;

"responder session encryption"

res\_enc &gt;

"initiator session encryption"

ini\_enc &gt;

"handshake encryption"

hs\_enc &gt;

## InitHello

"chaining key init"

spkr

&lt; mix

sidi

&lt; mix

epki

&lt; mix

spkr

&lt; mix

sctr

&lt; mix

sptr

encaps spkr

encrypt ltk

&lt; hs\_enc

key

data

pidi

&lt; mix

spki

&lt; mix

psk

encrypt auth

&lt; hs\_enc

key

auth

&lt; mix

## RespHello

state from InitHello

sidr

&lt; mix

sidi

&lt; mix

epki

&lt; mix

ecti

&lt; mix

epti

encaps epki

encaps spki

&lt; mix

spki

&lt; mix

scti

&lt; mix

spti

&lt; mix

ck

pidi

store\_biscuit()

&lt; mix

key

ct

&lt; mix

encrypt auth

## InitConf

state from RespHello

sidi

&lt; mix

sidr

encrypt auth

&lt; hs\_enc

key

auth

AEAD::enc(empty())

&lt; mix

osk

&lt; mix

res\_enc

&lt; mix

ini\_enc

&lt; mix

res\_enc