

Alice

Bob

static,
ephemeral
key pairs

static,
ephemeral
key pairs

```
graph TD; Alice[Alice] --> AliceKeyPairs(static, ephemeral key pairs); Bob[Bob] --> BobKeyPairs(static, ephemeral key pairs); AliceKeyPairs --> SessionKey(session key = { DH(static, ephemeral), DH(ephemeral, static), DH(ephemeral, ephemeral), DH(static, static) }); BobKeyPairs --> SessionKey;
```

session key = {
DH(static, ephemeral),
DH(ephemeral, static),
DH(ephemeral, ephemeral),
DH(static, static)
}