

Confidentiality
 integrity
 authenticity
 不可否认性 → message must be actually sent (lack of confidentiality)

in the real world, we usually have CIA in a 'private conversation' setting

but such a conversation is desirable
 ↓
 not always desirable

message authentication code:

both parties have same key

incoming message has valid MAC ⇒ comes from communication partner
since it doesn't come from myself

both parties could have generated MACs

ephemeral keys: short-lived keys, from communication

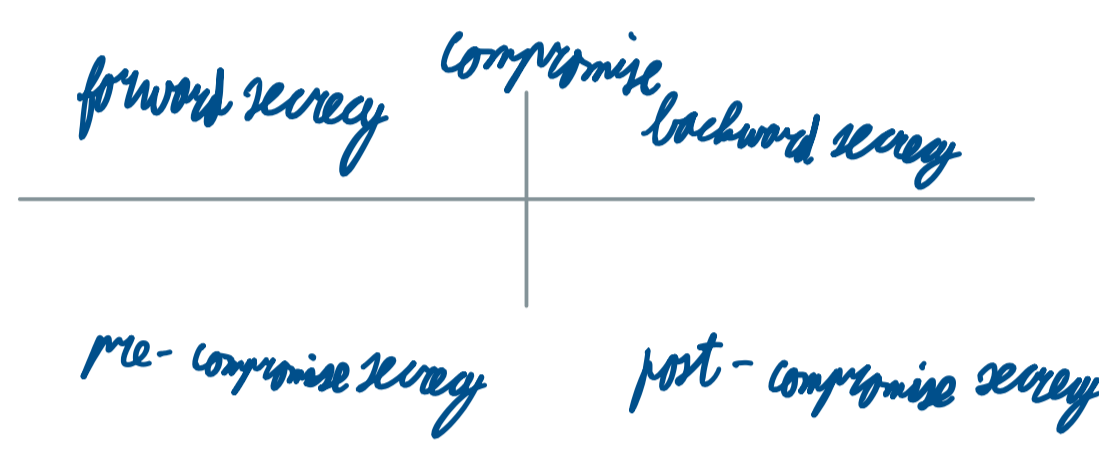
forward secrecy → secrecy maintained even if keys compromised

OTR: off the record messaging over XMPP

have separate keys for encryption & signing (sign = hash + sign)
 delete DH keys when you don't need them anymore

'leak' signing key later on to establish deniability

Use AES in counter mode



identity-mixing attack

$$A \rightarrow E: g^x, \text{sign}_{sk_A}(g^x), PK_A$$

$$E \rightarrow B: g^x, \text{sign}_{sk_E}(g^x), PK_E$$

$$B \rightarrow E: g^y, \text{sign}_{sk_B}(g^y), PK_B$$

$$E \rightarrow A: g^y, \text{sign}_{sk_B}(g^y), PK_B$$

Alice is talking to Bob
 Bob is talking to Eve

breaks authenticity

OTR v2: ties ephemeral public key to party

users must use an out-of-band channel for authentication

socialist millionaire protocol: check equality of two values without revealing either of those values

multi-party OTR: roughly the same as pairwise OTR

but:

encryption with group key shared entire group

signing with ephemeral signing keys

shutdown phase: send back of all messages to other group members; 'leak' signing key for deniability

Signal circle instant message protocol now discontinued, but formal building block for Signal

↳ sometimes outputs SAS = short authentication string

which should be covered out of band

anybody can claim to have had a conversation with Bob

Signal:

combine DHE ratchet (OTR) with hash-ratchet (SCMP)

ratchet = forward secure key update

avoid pre-advertisement of new key shares (first sending a MAC over share)

authenticate keys by mixing in previous authenticated keys

Keying chain

Receiving chain

initial root key authenticated with public keys of participants

Signal provides
 authenticity

forward secrecy

deniability

confidentiality

integrity