Messaging summary

vrijdag 6 januari 2023 15:13

On top of Confidentiality, Authenticity and Integrity, Deniability may also be a desirable property of secure communication.

Deniability can be achieved using a Message Authentication Code (MAC); if a message has a valid MAC, it must come from the communication partner. However, this proof is not transferable, because both parties could generate a MAC.

OTR protocol:

- Initial key share authenticated with long-term private keys
- Later key shares authenticated by MAC
- HMAC used for all encrypted messages
- Forward secrecy is guaranteed because long-term keys are only used for the signing of encryption keys, not for encryption itself.
- After a round trip, the MAC keys are leaked in the next iteration, providing deniability.
- A disadvantage is that OTR requires both users to be online.

Multi-party OTR: *(roughly)* pairwise OTR in groups; does not have (perfect) forward secrecy (during communication phase)

Socialist millionaires' protocol: check whether wealth is equal without revealing how much one owns (i.e. checking equality of shared secret value).

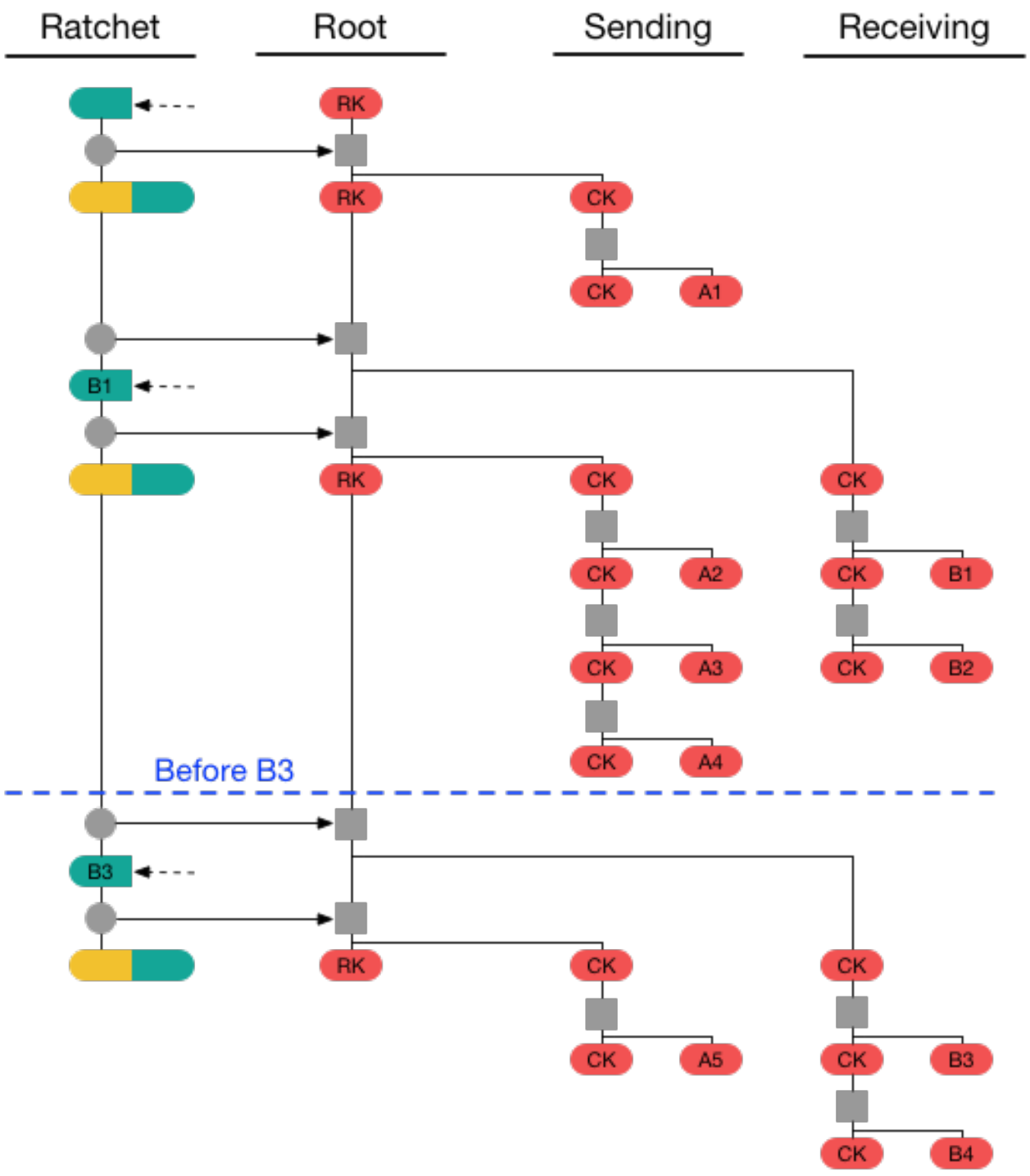
Note: the *(non-socialist)* millionaires protocol checks whose wealth is greatest

Silent Circle Instant Message Protocol (SCIMP):

- leaking encryption key leaks all following messages (in that session)
- authentication is done out of band
- both parties have authentication/encryption key, providing deniability (since either one could have written message)

Signal protocol:

- Combine DHE forward-secure key update with hash-based forward-secure key update
- Authenticate keys by mixing in previous authenticated keys



A new chain of keys is derived using the combination of:

- The private key whose public key was last sent to the other party
- The public key which was last received from the other part

This effectively means that, as soon as

- One changes from receiving to sending, newly sent messages cannot be decrypted anymore with existing keys
- One changes from sending to receiving, newly received messages cannot be decrypted anymore with existing keys