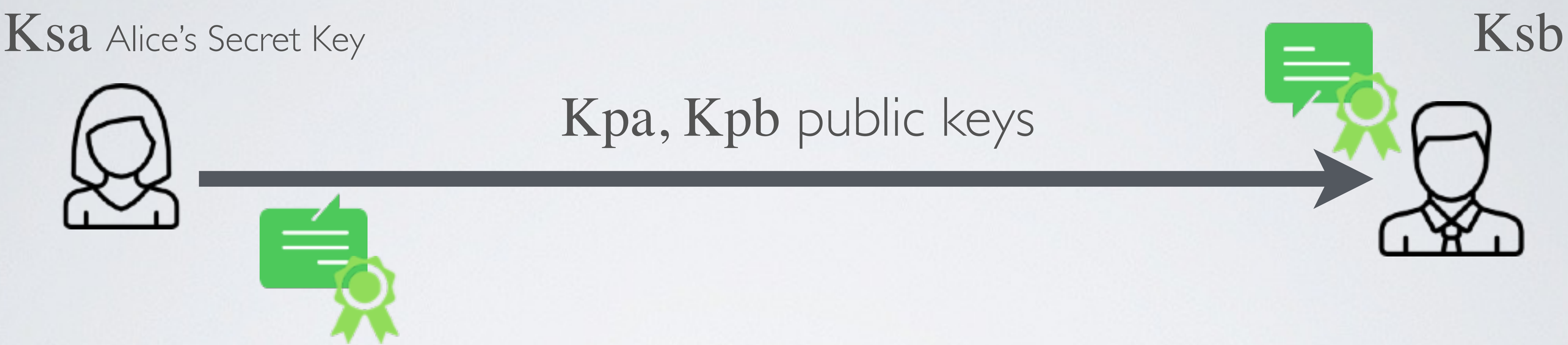
Digital Signatures and Confidentiality



1. Alice generates an asymmetric session key k
2. Use both symmetric and asymmetric cryptography to **encrypt, sign and verify** the message and the key

$$E_{Kpb}(k) \, \| \, E_{k}(m \, \| \, E_{Ksa}(H(m)))$$

Asymmetric encryption for key exchange

Should we use asymmetric encryption for key exchange?

✓ Simple solution for non-interactive protocol (e.g GPG)

◉ But not a good solution for interactive protocols