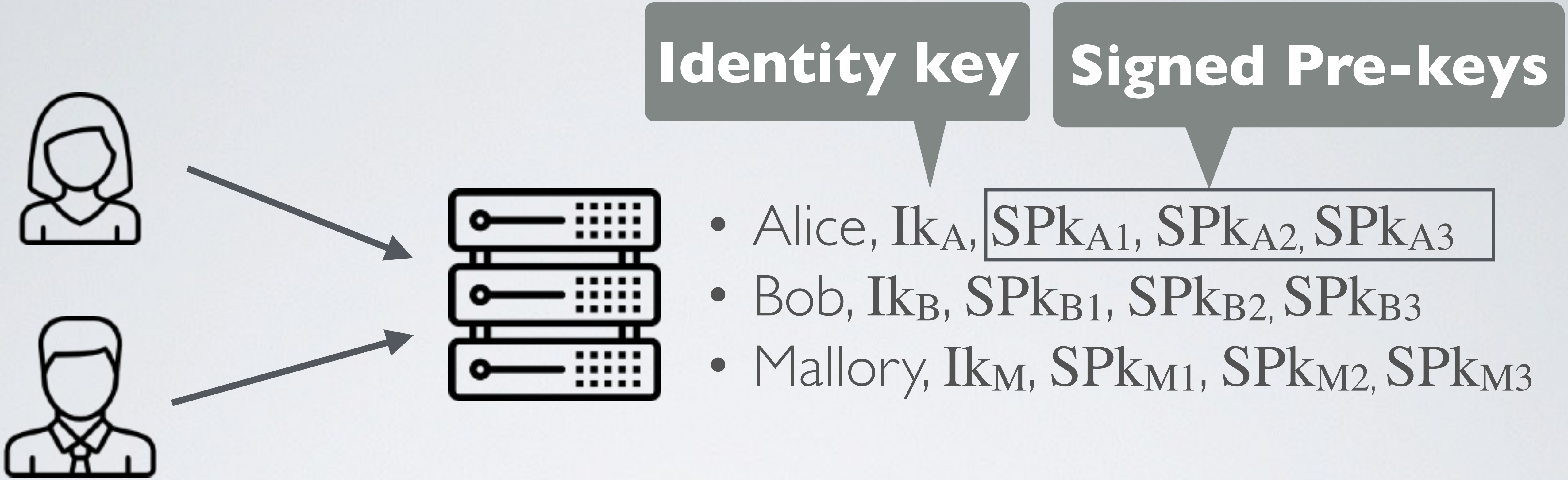
Signal in a Nutshell

➡ Asynchronous Protocol

Two phases

- **Triple Diffie-Hellman Key Exchange (3DH)**
  Open a communication channel between Alice and Bob
- **Double Ratchet Protocol**
  Exchange message exchange with forward secrecy

Signing-up with Signal



Identity key

Signed Pre-keys

- Alice, Ik_A, $\boxed{SPk_{A1}, SPk_{A2}, SPk_{A3}}$
- Bob, Ik_B, SPk_{B1}, SPk_{B2}, SPk_{B3}
- Mallory, Ik_M, SPk_{M1}, SPk_{M2}, SPk_{M3}

- Users sign-up with the signal server that verifies their identity (email, phone number, 2FA and so on)
- Users upload an identity key (public) and several pre-keys (public) signed with their identify key