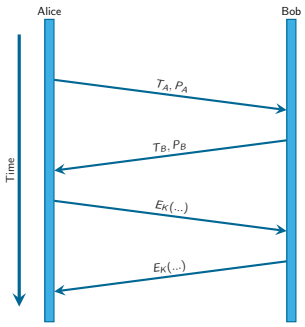
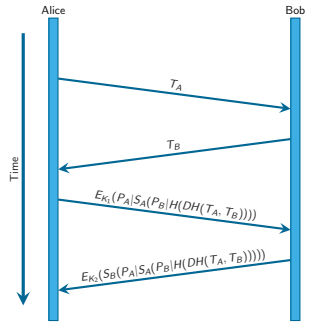
3DH (trevp?)



P_A	Public EdDSA key of Alice
P_B	Public EdDSA key of Bob
T_A	Ephemeral key from Alice
T_B	Ephemeral key from Bob
K	Key derived from $DH(T_A, T_B) \vert DH(T_A, P_B) \vert DH(P_A, T_B)$

Fixing the Wildcard (Tarr)[1]



- P_A Public EdDSA key of Alice
- P_B Public EdDSA key of Bob
- T_A Ephemeral key from Alice
- T_B Ephemeral key from Bob
- K_1 Key derived from $DH(T_A, T_B)|DH(T_A, P_B)$
- K_2 Key derived from $DH(T_A, T_B)|DH(T_A, P_B)|DH(P_A, T_B)$

[1] `http://dominictarr.github.io/secret-handshake-paper/shs.pdf`

Deniable signatures (Burdges, Grothoff)

Assume $Q_a = d_A G$ and $z = H(m)$. As in ECDSA, pick random $k \in [1, n-1]$. Let $C := C_A + C_B$ be the random offset.

$$(x_1, y_1) := kG \quad \underline{+C} \tag{1}$$
$$r := x_1 \mod n \tag{2}$$
$$s := k^{-1}(z + rd_A) \mod n \tag{3}$$

Repeat until $r, s \neq 0$. To verify:

$$w := s^{-1} \mod n \tag{4}$$
$$u_1 := zw \mod n \tag{5}$$
$$u_2 := rw \mod n \tag{6}$$
$$(x_1, y_1) := u_1 G + u_2 Q_A \quad \underline{+C} \tag{7}$$
$$r \equiv x_1 \mod n? \tag{8}$$

Falsification of a deniable signature

Assume $Q_a = d_A G$ and $z = H(m)$. As in ECDSA, pick random $r, s, k \in [1, n-1]$. Bob does not know d_A. So he calculates:

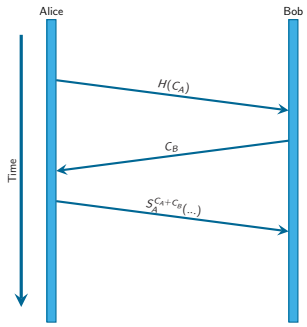
$$w := s^{-1} \mod n \tag{9}$$
$$u_1 := zw \mod n \tag{10}$$
$$u_2 := rw \mod n \tag{11}$$
$$(x_1, y_1) := u_1 G + u_2 Q_A \tag{12}$$
$$C \equiv x_1 - r \mod n \tag{13}$$

Bob now picks a random C_A and sets

$$C_B = C - C_A. \tag{14}$$

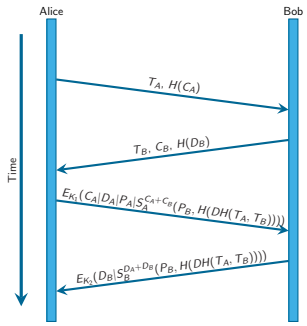
For this C_A, C_B the "random" values (r, s) are a valid signature (per construction).

Deniable signatures illustrated



- C_A Randomly chosen offset from Alice
- C_B Randomly chosen offset from Bob
- S_A^C Deniable signature using offset C and private key A

Staying Meta-OTR (Burdges, Grothoff)



P_A	Public EdDSA key of Alice
P_B	Public EdDSA key of Bob
C_A	Randomly chosen offset from Alice
C_B	Randomly chosen offset from Bob
D_A	Randomly chosen offset from Alice
D_B	Randomly chosen offset from Bob
T_A	Ephemeral key from Alice
T_B	Ephemeral key from Bob
K_1	Key derived from $DH(T_A, T_B)\|DH(T_A, P_B)$
K_2	Key derived from $DH(T_A, T_B)\|DH(T_A, P_B)\|DH(P_A, T_B)$