CIS 6930 – Emerging Topics in Network Security

Topic 2.5 Secret Handshake

Goals

- Authenticate without revealing credentials
  - Consider two groups G_1 and G_2
  - Two parties $A \in G_1$ and $B \in G_2$. A and B wants to authenticate each other.
  - If $G_1 \neq G_2$: A and B only know they are not in the same group.
  - If $G_1 = G_2$: A and B can authenticate to each other.
  - A third party learns nothing by observing conversations between A and B.

Secret-Handshake Scheme (SHS)

- SHS.CreateGroup(*G*): executed by an administrator, generates the group secret GroupSecret_G for *G*.
- SHS.AddUser(*U*,*G*,GroupSecret_G): creates pseudonym and user secret $\text{UserSecret}_{U,G}$ for new user *U*.
- SHS.HandShake(*A*,*B*): Users *A* and *B* authenticates each other. *B* discovers $A \in G$ if and only if $A \in$discovers $B \in G$.
- SHS.RemoveUser: Administrator removes user U by broadcasting its pseudonyms to all the other users, so that other users won't accept pseudonyms of U.

CreateGroup

- CreateGroup: Administrator picks (p,g). p is a large prime. Also, she picks a private key x, and computes the public key $y=g^x \bmod p$

Add User

- AddUser: For user *U*, administrator generates id_U, then generates a pair

$$(w, t)$$

so that

$$g^t = wy^{H(w,ID)} \bmod p$$

id_U, *w*, *t* will be given to the user.

– How to generate the pair (*w*,*t*)?

Randomly pick *r*, compute

$$w = g^r \bmod p$$

$$t = r + xH(w, ID) \bmod q$$

Handshake

- Handshake: Assume user *A* has (id_A, w_A, t_A) and user *B* has (id_B, w_B, t_B).

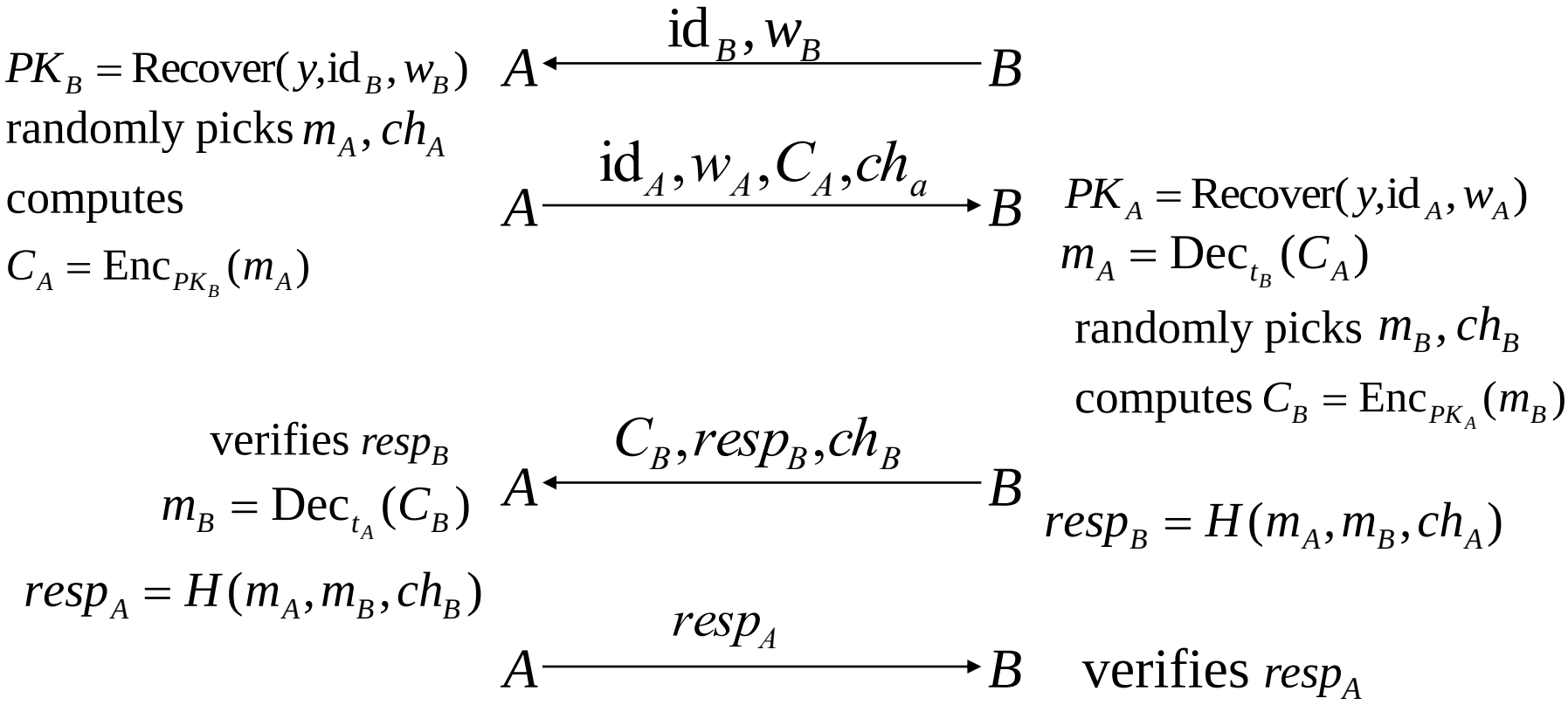
$$\mathrm{Recover}(y, \mathrm{id}, w) = PK = wy^{H(w,\mathrm{id})} \bmod p$$

$$\mathrm{Enc}_{PK}(m) = [c_1, c_2]$$
$$= [g^r \bmod p, m \oplus H'(PK^r \bmod p)]$$

$$\mathrm{Dec}_t([c_1, c_2]) = m = c_2 \oplus H'(c_1^t \bmod p)$$

Handshake (cont'd)

- Handshake:



Questions

- Question 1: Can A and B know who they are talking to during the authentication?
- Question 2: Can they know that they are in the same group?
- Question 3: What happens if we remove Ch_a and Ch_b?

Intuition

- If A and B are in the same group, they use has the same group private key x and each of them can decrypt the random number m_a and m_b.
- If not, neither of them can get any information about m_a or m_b.