erase
→ wymazać

Participant (world, participantID, privatekey)

extends

SIGMA

World C=<q>, N

Initiator (Alice)

~~t, A private~~

a - private key

A - public key $A = g^a$

x - ephemeral key

X - ephemeral public key $X = g^x$

sessionID ← rand()

Responder (Bob)

b - private

$g^b = B$

y

$g^y = Y$

communicat 1

$x \leftarrow rand()$

$X = g^x$

sessionID, A, X →

otrzymuje A, X, sessionID

$y \leftarrow rand$

$Y = g^y$

$K_{session} = (g^x)^y = X^y = g^{xy}$

$signature_B = SchnorrSignature($ (podpisuje swoim priv)

$m = g^x \| g^y \| ID_B \| B)$

communicat 2

← sessionID, Y, B, $signature_B$

MAC_B

otrzymuje Y, B,

podpis B pod g^x i g^y

MAC_B

$K_0 = PRF(K_{session}, 0)$

$K_1 = PRF(K_{session}, 1)$

$MAC_B = MAC_{K_1}(B)$ → public B

podpis B upewnia go ze B otrzymał odpowiednie $X = g^x$ i A otrzymał odpowiednie $Y = g^y$ dowiej sesji.

MAC_B upewnia go, ze rozmawia z Bobem

$K_{session} = Y^x = (g^y)^x = g^{yx} = g^{xy}$ (taki sam)

$signature_A$ - SchnorrSignature ($m = g^y \| g^{x/ID_A} \| A$)

K_0, K_1 (analogicznie jak Bob)

$MAC_A = MAC_{K_1}(A)$

↓ public A

communicat 3

sessionID, $signature_A$ →

MAC_A

upewnię się ze otrzymał odpowiednie $Y = g^y$ (w 1 wymianie) oraz ze Alice otrzymała $X = g^x$ i ze to ta sama sesja

MAC_A - Bob upewnia się ze gadał z Alice