$$send = \frac{i \cdot send_1(i,r,n_i) \quad ((l,f,\emptyset),[e]\cdot s) \in F}{\langle\langle\{A,B,pk(A),pk(B)\}, ((l,f,\emptyset),[\dots])\rangle \mapsto \langle\langle\{A,B,pk(A),pk(B)\} \cup \{n_A^{\#1}\}, \{(l,f,\emptyset),[send_2(i,r,\{n_i\}_{sk(i)}),\dots]\}\rangle\rangle}$$

(1) $\gamma = claim_4(i, recent\text{-}alive, r) \in ADEV \iff (\forall) t \in trace(P)$,
$(\forall) inst \in Just$ a.î. $(inst, \gamma) \in t \wedge honest(inst)$, at:

$(\exists) ev \in t : actor(ev) = \langle inst \rangle(r) \wedge$

$(\exists) ev' \in t : runid of(ev') = runid of(inst) \wedge$

$ev' <_t ev <_t (inst, \gamma)$ ("r" "alive" DIN PERSPECTIVA LUI "i" SI ÎNTRE 2 ACȚIUNI CONSECUTIVE ALE LUI "i", $(\exists)$ O ACȚIUNE A LUI "r")

FIE $t \in trace(P)$, FIE $inst \in Just$ a.î. $(inst, \gamma) \in t \wedge honest(inst)$

$ev' = send_1(i,r,n_i)$

$ev = send_3(r,i,\{n_2, n_i\}_{sk(r)})$ } RESPECTĂ PROPRIETĂȚILE,

$\gamma' = claim_4(i, recent\text{-}alive, r)$ DECI $(\exists)$ ged

Seminar 6 (Model Examen)

FIE URMĂTORUL PROTOCOL:

$i \to r : \{\text{"Hello"}, n_i\}_{sk(i)}$

$r \to i : \{\text{"Hi"}, n_i, i\}_{sk(r)}$

CERINȚE: (1p OFICIU)

5p a) SĂ SE IDEALIZEZE PROTOCOLUL ÎN LOGICA "BAN" ȘI SĂ SE DISCUTE DACĂ $(\exists)$ O AUTENTIFICARE MUTUALĂ MODULO "n_i", I.E.:

$i \models r \models n_i$

$r \models i \models n_i$

1p b) CONSIDERĂM SPECIFICAȚIA "P". SĂ SE DETERMINE $P(i)$, $P(r)$.

1p c) SĂ SE SCRIE UN TRACE NEONEST.

1p d) PE UN TRACE ONEST SĂ SE EXECUTE 2-3 PAȘI ÎN SEMANTICA OPERAȚIONALĂ

1p e) SĂ SE VERIFICE DACĂ ȚINE CLAIM-UL $\gamma = claim(i, recent\text{-}alive, r)$

#

REZOLVARI:

a) 1) IDEALIZARE: FORMALIZARE

$i \to r : \{ \text{"HELLO"}, n_i \}_{K_i^{-1}}$

$r \to i : \{ \text{"Hi"}, n_i, i \}_{K_r^{-1}}$

K_i = CHEIE PUBLICA
K_i^{-1} = " - " SECRETA

2) ASUMPTII:

(A1) $i \models \xrightarrow{K_r} r$ (A2) $r \models \xrightarrow{K_i} i$ (A3) $i \models \#(n_i)$

(A4) $r \triangleleft \{ \text{"HELLO"}, n_i \}_{K_i^{-1}}$ (A5) $i \triangleleft \{ \text{"Hi"}, n_i \}_{K_r^{-1}}$

(DACĂ MĂ BLOCHEZI LA DEM., MAI ADAUG ASUMPTII)

(A6) $r \models \#(n_i)$

(A7) $r \models i \Rightarrow n_i$

(A8) $i \models n_i$

3) DERIVARE:

(P1) $r \models i \sim (\text{"HELLO"}, n_i)$ (MM-PK: A2, A4)

(P2) $r \models \#(\text{"HELLO"}, n_i)$ (NC: A6)

(P3) $r \models i \models (\text{"HELLO"}, n_i)$ (NV: P1, P2)

(P4) $r \models i \models n_i$ (BC: P3) ✓ (q.e.d. DIN PERSPECTIVA LUI "r")

(P1) $i \models r \sim (\text{"Hi"}, n_i)$ (MM-PK: A1, A5)

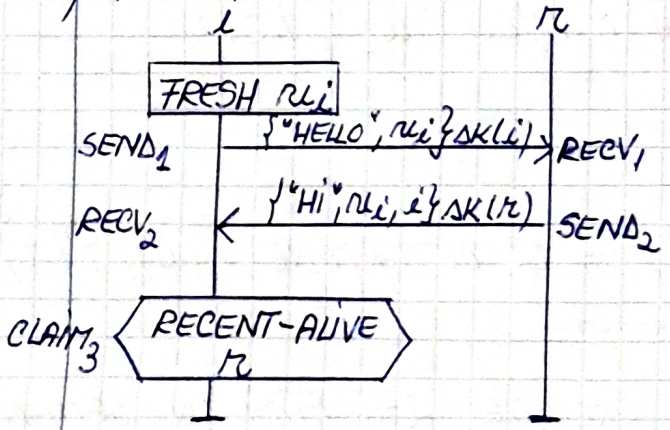
(P2) $i \models \#(\text{"Hi"}, n_i)$ (NC: A3)

(P3) $i \models r \models (\text{"Hi"}, n_i)$ (NV: P1, P2)

(P4) $i \models r \models n_i$ (BC: P3) ✓ (q.e.d. → "i")

• PUTEM DEM. $r \models n_i$? → DA, PRIN (JR: A7, P4)

b) P:



$P(R) = H(R) = \{KN_0(R), S(R)\}$

↑ DIN SEMINARII ANTERIOARE (NUME ARBITRAR PROTOCOL)

$P(i) = \{\{i, r, pK(i), SK(i), pK(r)\},$
$[send_1(i, r, \{\text{"HELLO"}, n_i\}_{SK(i)}),$
$recv_2(i, r, \{\text{"Hi"}, n_i, i\}_{SK(r)}),$
$claim_3(i, recent\text{-}alive, r)]\}$

$[P(r) = \{\{i, r, pK(r), SK(r), pK(i)\},$
$[recv_1(i, r, \{\text{"HELLO"}, n_i\}_{SK(i)}),$
$send_2(i, r, \{\text{"Hi"}, n_i, i\}_{SK(r)})]]$

→ AICI TB. CU "V" (CA ÎN SEMINAR ANTERIOR)

c) i — Eve — r

$i \to Eve$: $\{\text{"HELLO"}, n_i\}_{SK(i)}$

$Eve \to r$: $\{\text{"HELLO"}, n_i\}_{SK(i)}$

$r \to Eve$: $\{\text{"Hi"}, n_i, i\}_{SK(r)}$

$(init, \gamma) \in \mathcal{T}$; $f = \{i \to A, Eve \to E, r \to B\}$

$[((1, f, \emptyset), create(i)), ((1, f, \emptyset), send_1(A, E, \{\text{"HELLO"}, n_A^{\#1}\}_{AK(A)})),$
$((2, f, \emptyset), create(Eve)), ((2, f, \{V \to n_A^{\#1}\}), recv_1(E, A, \{\text{"HELLO"}, V\}_{SK(A)}),$
$((2, f, \{V \to n_A^{\#1}\}), send_2(E, B, \{\text{"HELLO"}, V\}_{SK(A)})), \dots]$ → TRACE NE-ONEST

d) $f : Role \to Agents$

$f = \{i \to A, r \to B\}$

$RID = \mathbb{N}$

$\nabla : Var \to RunTrace$

"1" PT. "i"

"2" PT. "r"

TRACE ONEST = $[((1, f, \emptyset), create(i)),$
$((1, f, \emptyset), send_1(A, B, \{\text{"HELLO"}, n_A^{\#1}\}_{SK(A)})),$
$((2, f, \emptyset), create(r)),$
$((2, f, \{V \to n_A^{\#1}\}), recv_1(B, A, \{\text{"HELLO"}, V\}_{SK(A)})),$
$((2, f, \{V \to n_A^{\#1}\}), send_2(B, A, \{\text{"Hi"}, V, A\}_{SK(B)})),$
$((1, f, \emptyset), recv_2(A, B, \{\text{"Hi"}, n_A^{\#1}, A\}_{SK(B)})),$
$((1, f, \emptyset), claim_3(A, recent\text{-}alive, B))]$

AKN_0 (CUNOSTINTE INITIALE ATACATOR PASIV) $= \{A, B, pK(A), pK(B)\}$

$runsof(P, i) = \{(1, f, \emptyset), [send_1(i, r, \{\text{"HELLO"}, n_i\}_{SK(i)}),$
$recv_2(i, r, \{\text{"Hi"}, n_i, i\}_{SK(r)}),$
$claim_3(i, recent\text{-}alive, r)]\}$

$runsof(P, r) = \{(2, f, \emptyset), [recv_1(r, i, \{\text{"HELLO"}, n_i\}_{SK(i)}),$
$send_2(r, i, \{\text{"Hi"}, n_i, i\}_{SK(r)})]\}$

$\ll AKN_0, \emptyset \gg = S_0(P)$

REGULI DIN CURS →

$create_i$: $\dfrac{ic\ dom(f) \quad ((1, f, \emptyset), \Delta) \in runsof(P, i) \quad 1 \notin runIDs(\Gamma)}{\ll AKN, \Gamma \gg \xrightarrow{((1, f, \emptyset), create\ i)} \ll AKN, \Gamma \cup \{((1, f, \emptyset), \Delta)\} \gg}$

$\ll \{A, B, pK(A), pK(B)\}, \emptyset \gg \xrightarrow{((1, f, \emptyset), create\ i)} \ll \{A, B, pK(A), pK(B)\},$
$\{((1, f, \emptyset), runsof(P, i))\} \gg \xrightarrow{((1, f, \emptyset), send_1)} \ll \{A, B, pK(A), pK(B),$

$\{\text{"HELLO"}, n_A^{\#1}\}_{SK(A)}\}, \{(1, f, \emptyset), [recv_2, claim_3]]\} \xrightarrow{(2,f,\emptyset), create(r)}$

$\rightarrow \ll \{A, B, pK(A), pK(B), \{\text{"HELLO"}, n_A^{\#1}\}_{SK(A)}\}, \{(1, f, \emptyset), [recv_2, claim_3]]\} \cup$

$\cup \{(2, f, \emptyset), runidof(P, r)\}\} \gg \longrightarrow \ldots$

ÎNCEP CU $\Delta_0(P)$. RULEZ PAȘII TRACE-ULUI ONEST (DEASUPRA SĂGEȚILOR SUNT FIX PAȘII, DAR SCRIȘI CU "i" ȘI "r"). APLIC REGULA PASULUI ("create", "send", "recv" → DIN CURSURI). CÂND TREC LA UN PAS NOU, ÎL SCOT DIN DREAPTA "→".

c) $\delta = claim_\ell(R, recent\text{-}alive, R')$ dacă

$(\forall) t \in traces(P) \wedge (\forall)(\theta, f, \nabla) \in Just$ a.î. $((\theta, f, \nabla), \delta) \in t$

$\wedge honest(\theta, f, \nabla)$, atunci:

$(\exists) ev, ev' \in t$ a.î. $actor(ev) = f(R') \wedge role(ev) = R' \wedge$

$runidof(ev') = runidof(\theta, f, \nabla) \wedge ev' <_t ev <_t ((\theta, f, \nabla), \delta)$

FIE $t \in traces(P)$, FIE $(\theta, f, \nabla) \in Just$. a.î. $((\theta, f, \nabla), \delta) \in t$

$\wedge honest(\theta, f, \nabla)$:

$ev' = send_1$

$ev = send_2$

$\delta = claim_3(i, recent\text{-}alive, r)$

} RESPECTĂ PROPRIETĂȚILE, DECI $(\exists)$

q.e.d