a) $H(i) = \{\{i, r, pK(i), sK(i), pK(r)\}, [SEND_1(i, r, nu_i), SEND_2(i, r, \{\text{"HELLO"}\}_{sK(i)}), RECEIVE_3(i, r, \{\text{"HELLO"}, nu_i\}_{sK(r)})]\}$

$H(r) = \{\{i, r, sK(r), pK(r), pK(i)\}, [RECEIVE_1(r, i, nu_i), RECEIVE_2(r, i, \{\text{"HELLO"}\}_{sK(i)}), SEND_3(r, i, \{\text{"HELLO"}, nu_i\}_{sK(r)})]\}$

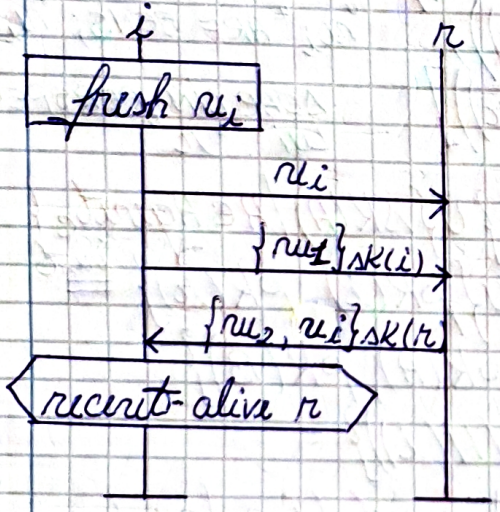
b) $AKN_0 = \{i, r\} \geq Agents_H$

c) $runsof(H, i) = \{(\langle \theta, f, \nabla \rangle, \Delta) \mid \Delta \in \Pi_2(H(i))\}$

$runsof(H, r) = \{(\langle \theta, f, \nabla \rangle, \Delta) \mid \Delta \in \Pi_2(H(r))\}$

Seminar 5

FIE PROTOCOLUL "H":



$H(R) = \{KN_0(R), \Delta(R)\}$

a) $H(i) = \{\{i, r, sK(i), pK(i), pK(r)\}, [SEND_1(i, r, nu_i), SEND_2(i, r, \{nu_1\}_{sK(i)}), RECV_3(i, r, \{nu_2, nu_i\}_{sK(r)})]\}$

$H(r) = \{\{i, r, sK(r), pK(r), pK(i)\}, [RECV_1(r, i, V), RECV_2(r, i, \{nu_1\}_{sK(i)}), SEND_3(r, i, \{nu_2, V\}_{sK(r)})]\}$

$claim_4(i, recruit\text{-}alive, r)$

"r" NU ȘTIE CE PRIMEȘTE; PT. EL E O VALOARE OARECARE "V"

b) $Agents = Agents_{Honest} \cup Agents_{corrupted}$

FOR $(\theta, f, \nabla) \in Instr$, WE DEFINE THE PREDICATE "$honest(\theta, f, \nabla)$" WHICH IS "TRUE" IF THE ROLES = HONEST AGENTS, i.e.

* $honest(\theta, f, \nabla)$ iff $range(f) \subseteq Agents_H$ *

FIE PROTOCOLUL "H":

a) $H(i), H(r) = ?$

b) FIE $R\Delta = \mathbb{N}$ ȘI $f: Role \to Agents$, $f = \{i \mapsto A, r \mapsto B\}$. SĂ SE SCRIE UN "trace" ONEST PT. ACEST PROTOCOL.

c) $AKN_0 = ?$

d) $runsof(H, i), runsof(H, r) = ?$

e) SĂ SE EXECUTE 2-3 PAȘI ÎN "LTS" PT. "i"

f) SĂ SE DEM. CĂ $\gamma = claim(i, recruit\text{-}alive, r) \in ADEV.$

• "TRACE" ONEST = TOATE INSTANȚIERILE SUNT ONESTE.

• P = PROTOCOL, R = ROLE, γ (SECRECY CLAIM) = $claim_1(R, secret, nt)$
FOR ANY $t \in traces(P)$ AND ANY $((\theta, f, T), \gamma) \in t$,
"honest$((\theta, f, T))$" IMPLIES "$AKN(t) \nvdash (\theta, f, T)(nt)$", WHERE
$AKN_{nt} = AKN([\alpha_1, \dots, \alpha_{nt}])$

• $t \in traces(P)$ ONEST DACĂ $(\forall)$ $label = (inst, \gamma) \in t \Rightarrow honest(inst)$,
$[((1, f, \emptyset), create(i)), ((1, f, \emptyset), send_1(i, r, nu_i)),$ "create" ⇒ INCREMENTEZ "run id"
$((2, f, \emptyset), create(r)), ((2, f, \{V \mapsto nu_i^{\#1}\}), recv_1(r, i, V))]$ $\{i$: run id = 1, r: " − " = 2
NU AM VAR. (MESAJELE ÎN CLAR NU SUNT VARIABILE)
$((1, f, \emptyset), send_2(i, r, \{nu_1\}_{SK(i)})), ((2, f, \emptyset), recv_2(r, i, \{nu_1\}_{SK(i)})),$ DIN PERSPECTIVA LUI "i",
$((2, f, \{V \mapsto nu_i^{\#1}\}), send_3(r, i, \{nu_2, V\}_{SK(r)})),$ "nu_i" ARE SENS; "nu_i" = VAR,
$((1, f, \emptyset), recv_3(i, r, \{nu_2, nu_i\}_{SK(r)})),$
$((1, f, \emptyset), claim_4(i, recent\text{-}alive, r))]$ DOAR DIN PERSPECTIVA LUI "r"

c) $AKN_0 = Agents \cup \{pK(A) / A \in Agents\} \cup \{sK(A) / A \in Agents_c\} \cup$
$\cup AdversaryFresh = Agents \cup \{pK(i), pK(r)\} \overset{inst}{=}$
$= \{A, B\} \cup \{pK(A), pK(B)\} = \{A, B, pK(A), pK(B)\}$

d) $runsof(H, i) = \{((1, f, \emptyset), s) / s \in \Pi_2(H(i))\} =$
$= \{((1, f, \emptyset), [send_1(i, r, nu_i), send_2(i, r, \{nu_1\}_{SK(i)}),$
$recv_3(i, r, \{nu_2, nu_i\}_{SK(r)}), claim_4(i, recent\text{-}alive, r)]\}$

e) $\ll AKN_i, F_i \gg$ → CONFIGURAȚIA UNEI STĂRI
$S_0(H) = \ll AKN_0, \emptyset \gg$ ("S_0" SE EXECUTĂ DOAR DIN PERSPECTIVA UNUI ROL)

$$[create_P] \frac{R \in dom(P) \quad ((\theta, f, T), s) \in runsof(P, R) \quad \theta \notin runIDs(F)}{\ll AKN, F \gg \xrightarrow{((\theta, f, \emptyset), create(R))} \ll AKN, F \cup \{((\theta, f, \emptyset), s)\} \gg}$$
(PROTOCOL, ROL)

$runIDs(F) = \{\theta / ((\theta, f, T), s) \in F$, FOR SOME $f, T, s\}$

$F \subseteq Run = Inst \times RoleEvent^*$

$$create_i \frac{i \in \{i, r\} \quad ((1, f, \emptyset), [\dots]) \in runsof(H, i) \quad 1 \notin runIDs(\emptyset)}{\ll A, B, pK(A), pK(B)\}, \emptyset \gg \rightarrow \ll \{A, B, pK(A), pK(B)\}, \{((1, f, \emptyset), [\dots]\} \gg}$$
↳ DIN $runsof(H, i)$

$$[send] = \frac{e = send_{nu}(R_1, R_2, nu) \quad (inst, [e] \cdot s) \in F}{\ll AKN, F \gg \xrightarrow{(inst, e)} \ll AKN \cup \{inst(nu)\}, F - \{(inst, [e] \cdot s)\} \cup \{(inst, s)\} \gg}$$

$$send = \frac{e = send_1(i, r, n_i) \quad ((1, f, \emptyset), [e] \cdot s) \in F}{\ll\{A, B, pK(A), pK(B)\}, ((1, f, \emptyset), [\ldots])\} \rightarrow \ll\{A, B, pK(A), pK(B)\} \cup \{n_A^{\#1}\},}$$

$$\{(1, f, \emptyset), [send_2(i, r, \{n_1\}_{SK(i)}), \ldots]\} \gg$$

(1) $\gamma = claim_4(i, recent\text{-}alive, r) \in A\Delta EV. \Leftrightarrow (\forall) t \in trace(P)$,
$(\forall) inst \in Inst$ a.î. $(inst, \gamma) \in t \wedge honest(inst)$, at:

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

$(\exists) ev' \in t$: $runidof(ev') = runidof(inst) \quad \wedge$

$ev' <_t ev <_t (inst, \gamma)$ ("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 $inst \in Inst$ 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 $(\exists)$ qed