(8) $B \models A \sim M$ (JR: p9, 7)

(9) $B \models A \models M$ (NV: p13, 8) ✓

($A \models B \models M$ SIMETRIC, CA MAI SUS)

(10) $B \models A \leftrightarrow^{K_{AB}} B$ (JR: p7, 6)

• $B \models A \models A \leftrightarrow^{K_{AB}} B$? ⇒ NU

II) $A \to B: \{M\}_{K_A^{-1}}$ $M \Rightarrow$ NONCE

Ce se poate demonstra?

2) ASUMPȚII:

(p1) $B \triangleleft \{M\}_{K_A^{-1}}$

(p2) $B \models K_A$; (p3) $A \models K_A$; ?(p4) $A \models K_A^{-1}$

(p5) $A \models \#(M)$; (p6) $B \models \#(M)$

4) DERIVARE:

(1) $B \models A \sim M$ (MM-PK: p1, p2)

?(2) $B \models A \models M$ (NV: 1, p6)

NU AVEM NICIO GARANȚIE CĂ P6 ȚINE

= Seminar 3 =

SEMANTICĂ OPERAȚIONALĂ – EXERCIȚII

$\sqsubseteq_{acc}$ → RELAȚIE DE ACCESIBILITATE PE TERMENI

$\sqsubseteq_{acc} \subseteq RoleTerm^2$ IS THE REFLEXIVE AND TRANSITIVE CLOSURE OF THE: $\begin{cases} t_1 \sqsubseteq_{acc} (t_1, t_2) \\ t_2 \sqsubseteq_{acc} (t_1, t_2) \\ t_1 \sqsubseteq_{acc} \{|t_1|\}_{t_2} \end{cases}$, WHERE $RoleTerm ::= \begin{cases} Var \mid Fresh \mid Role \mid \\ Func(RoleTerm^*) \mid (RTerm, RT...) \\ \mid \{|RT|\}_{RT} \mid sk(RT) \mid pk(RT) \mid \\ h(RT, RT) \end{cases}$

AND $\{|m|\}_m$ = ENCRYPTION OF "m" WITH "n".

$(t_1, t_2, t_3) \overset{NOT.}{=} ((t_1, t_2), t_3)$; $\{|(t_1, t_2)|\} \overset{NOT.}{=} \{|t_1, t_2|\}$

1) DAȚI EX. DE TERMENI "s", "t", a.î. $\{s\} \vdash t$, DAR $s \not\sqsubseteq_{acc} t$.

- $\{s\} \vdash t \Rightarrow$ "t" SE DEDUCE DIN "s"
- $\dfrac{t_1 \quad t_2}{(t_1, t_2)} \qquad \dfrac{(t_1, t_2)}{t_2} \qquad \dfrac{\{t\}_K \quad K^{-1}}{t} \qquad \dfrac{t \quad K}{\{t\}_K}$

SI. DEDUCȚIE PE TERMENI

- THE INVERSE FUNCTION ENCRYPTION: $^{-1} : RoleTerm \to RoleTerm$

PT. ORICE TERMEN $rt \in RoleTerm$, DEFINIM INVERSUL $rt^{-1} \in RT$:

$$rt^{-1} = {}^{-1}(rt) = \begin{cases} sk(t); & rt = pk(t), \text{ UNDE } t \in RoleTerm \\ pk(t); & rt = sk(t), \quad -\text{''}- \quad -\text{''}- \\ rt; & \text{ALTFEL} \end{cases}$$

sk = SECRET KEY; pk = PUBLIC KEY → ASYMMETRIC ENCRYPTION

k = SYMMETRIC KEY

$s = (rt_1, rt_2)$; $t = \{rt_1\}_{rt_2}$

$$\{s\} \vdash t \Rightarrow \begin{cases} \{(rt_1, rt_2)\} \vdash rt_1 \\ \{(rt_1, rt_2)\} \vdash rt_2 \\ \{(rt_1, rt_2)\} \vdash \{rt_1\}_{rt_2} \end{cases} \Rightarrow t \not\sqsubseteq_{acc} s, \text{ DAR } s \sqsubseteq_{acc} t$$

SAU $t = (rt_2, rt_1)$ ATUNCI $s \not\sqsubseteq_{acc} t$

DEDUCTION ON $RoleTerm$: $\vdash \subseteq \mathcal{P}(RoleTerm) \times RoleTerm$

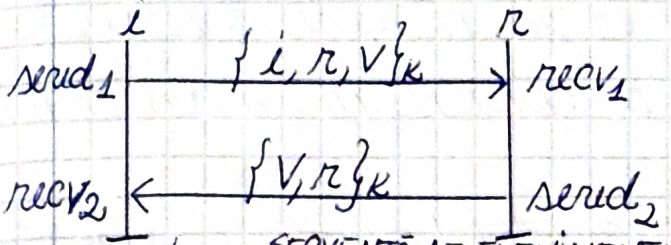
$\vdash \subseteq \mathcal{P}(RoleTerm \cup RoleTerm) \times (RoleTerm \cup Funct)$

$M \vdash t \Rightarrow$ "t" POATE FI DEDUS ȘTIIND M

DACĂ $t \in M$	ATUNCI $M \vdash t$
DACĂ $M \vdash t_1$ ȘI $M \vdash t_2$	ATUNCI $M \vdash (t_1, t_2)$
DACĂ $M \vdash (t_1, t_2)$	ATUNCI $M \vdash t_1$ ȘI $M \vdash t_2$
DACĂ $M \vdash t$ ȘI $M \vdash k$	ATUNCI $M \vdash \{t\}_k$
DACĂ $M \vdash \{t\}_k$ ȘI $M \vdash k^{-1}$ (PRIVATE KEY)	ATUNCI $M \vdash t$
DACĂ $M \vdash t_1, \ldots M \vdash t_n$	ATUNCI $M \vdash f(t_1, \ldots, t_n)$, $f \in Funct$

$$Cons(M) = \{t \in RoleTerm \mid M \vdash t\}$$

2) FIE URMĂTOAREA DESCRIERE DE ROL $\mathcal{P}(i) = (\{i, r, K\}, [send_1(i, r, \{i, r, V\}_K), recv_1(r, i, \{V, r\}_K)])$. V = VARIABILĂ.



SECVENȚĂ DE EVENIMENTE A UNUI ROL

ESTE ACEASTĂ ROL WELL-FORMED? ⇒ NU.

• $\mathcal{P}$ (SECVENȚĂ EVENIMENTE PT. UN ROL) ∈ RoleEvents* ESTE "WELL-FORMED" DACĂ PRIMA APARIȚIE A ORICĂREI VARIABILE E ÎNTR-O POZIȚIE ACCESIBILĂ PT. UN EVENIMENT "receive", i.e.:

$(\forall) V \in vars(\mathcal{P}), (\exists) \mathcal{P}', L, R, R', rtb, \mathcal{P}'' :$

vars(P) în Var — TOATE VAR. DIN "P"

$: (\mathcal{P} = \mathcal{P}' \cdot [recv_L(R, R', rtb)] \cdot \mathcal{P}'') \wedge V \notin vars(\mathcal{P}') \wedge V \sqsubseteq_{acc} rtb$

NOT.: WELLFORMED($\mathcal{P}$) → ✓, DACĂ PRIMA APARIȚIE A ORICĂREI VAR. E ÎNTR-UN "receive".]*

• $RoleEvents_R ::= send_{Label}(R, Role, RoleTerm) \mid$
$recv_{Label}(Role, R, \_\text{"}-\text{"}) \mid$
$claim_{Label}(R, Claim, [\_\text{"}-\text{"}])$

$send_L(R, R', rtb)$ → "R" TRIMITE "rtb" (MESAJ) LUI "R'"
$recv_L(R', R, rtb)$ → "R" PRIMEȘTE " — " DE LA "R'"
$claim_L(R, c, rtb)$ → PROPRIETATE A SECURITĂȚII CARE TB. SATISFĂCUTĂ DUPĂ EXECUȚIA LUI "R"

CA SĂ DEM., SPUNEM CĂ (∃) O VAR. PT. CARE NU ȚINE PROPRIETATEA (AKA NEGĂM IPOTEZA: $(\forall) V \Rightarrow (\exists) V$)

$(\exists) V \in vars(\mathcal{P})$

$\mathcal{P} = [send_1(i, r, \{i, r, V\}_K)] \cdot [recv_1(r, i, \{V, r\}_K)] \cdot \emptyset$

↯ CU DEF. WELLFORMED

3) • RUN = SINGLE EXECUTION OF A ROLE.

• RID (RUN IDENTIFIERS) = DIFFERENT RUNS ARE DESCRIBED USING RID.

• RUN TERM = CONCRETE EXECUTION OF THE PROTOCOL IS DESCRIBED USING IT.

• INSTANTIATION = TURNING A ROLE DESCRIPTION INTO A RUN WITH THE HELP OF RID.

• $RuniTerm ::= Var^{\#RID} \mid Fresh^{\#RID} \mid Role^{\#RID} \mid Agents \mid Func(RuniTerm^*) \mid (RuniTerm, RuniTerm) \mid \{|RuniTerm|\}_{RuniTerm} \mid$
$AdversaryFresh \mid sk(RuniTerm) \mid pk(RuniTerm) \mid K(RuniTerm, RuniTerm)$

RUN TERMS GENERATED BY AN ADVERSARY

• INST (INSTANTIATION) = $(\theta, f, \nabla) \in RID \times (Role \to Agents) \times (Var \to RuniTerm)$

$\langle \theta, f, \nabla \rangle(rt) = inst(rt) = \begin{cases} n^{\#\theta}; n \in Fresh & \text{(NONCE IN RUNDA CURENTĂ)} \\ f(R); R = rt \in Role \cap dom(f) \\ R^{\#\theta}; R = rt \in Role - dom(f) \\ \nabla(V); V = rt \in Var \cap dom(f) \\ V^{\#\theta}; V = rt \in Var - dom(f) \end{cases}$

EX: $\theta = 1$

$f = \{i \mapsto Alice, j \mapsto Bob\}$

$\nabla = \{V \mapsto n, \dots\}$

$\begin{cases} inst(f(t_1, \dots, t_n)) = f(inst(t_1), \dots, inst(t_2)) \\ inst(t_1, t_2) = (inst(t_1), inst(t_2)) \\ inst(\{|t_1|\}_{t_2}) = \{|inst(t_1)|\}_{inst(t_2)} \\ inst(sk(t)) = sk(inst(t)) \quad \text{(LA FEL PT. } pk) \\ inst(K(t_1, t_2)) = K(inst(t_1), inst(t_2)) \end{cases}$

$\#_{n_i \in Fresh, n \in Role}$ CALCULEAZĂ INSTANȚIEREA $\langle 1, \{i \mapsto A, n \mapsto B\}, \emptyset \rangle(\{|n_i, i|\}_{pk(n)}) =$

$= \{\langle 1, \{i \mapsto A, n \mapsto B\}, \emptyset \rangle((n_i, i))\}_{\langle 1, \{i \mapsto A, n \mapsto B\}, \emptyset \rangle(pk(n))} =$

$= \{(n_i^{\#1}, A)\}_{pk(\langle 1, \{i \mapsto A, n \mapsto B\}, \emptyset \rangle(n))} = \{(n_i^{\#1}, A)\}_{pk(B)}$

4) SĂ SE DEM. CĂ "$h(K)$" POATE FI DEM. DIN MULȚIMEA URMĂTOARE DE TERMENI: $\{\{n^{-1}\}_k, \{K^{-1}\}_{pk(b)}, \{h(K)\}_n, sk(b)\}$

DEM:

$$\dfrac{\dfrac{\{K^{-1}\}_{pk(b)} \quad sk(b)}{K^{-1}} \quad \{n^{-1}\}_k}{n^{-1}} \quad \{h(K)\}_n \checkmark$$

$h(K)$

Aplic și. deducție

(SAU) (ECHIVALENT) DEM. PE LINII, NOTÂND MULȚIMEA DE TERMENI CU "T":

$T \vdash sk(b)$

$T \vdash \{k^{-1}\}_{pk(b)}$

$T \vdash k^{-1}$

$\vdots$

5) PREDICATUL MATCH: $Match \subseteq Inst \times RoleTerm \times RunTerm \times Inst$

DEF (∀) $inst = \langle \theta, f, \nabla \rangle$; $inst' = \langle \theta', f', \nabla' \rangle$; $pt \in RoleTerm$; $ru \in RunTerm \rightarrow$

$\rightarrow Match(inst, pt, ru, inst')$ e adevărat dacă:

(*) $\begin{cases} \theta = \theta'; \ f = f'; \ \nabla \subseteq \nabla' \\ inst'(pt) = ru \\ (\forall) v \in dom(\nabla'), \nabla'(v) \in type(v) \\ \quad = dom(\nabla) \cup vars(pt) \end{cases}$

FUNCTION THAT DEPENDS ON THE AGENT MODEL

PRESUPUN $f = \{i \mapsto A, r \mapsto B\}$, $type(X) \geq S_3 = Fresh$

$Match(\langle 1, f, \emptyset \rangle, \{ru_i, r\}_{pk(i)}, \{ru_i^{\#1}, B\}_{pk(A)}, \langle 1, f, \emptyset \rangle)$

(IAU LA RÂND CONJUNCȚIILE IPOTEZELE (*))

$\langle 1, f, \emptyset \rangle (\{ru_i, r\}_{pk(i)}) = \{ru_i^{\#1}, B\}_{pk(A)}$ q.e.d.

$type(V) \in \{S_1, S_2, S_3, S_4, S_5\}$:

$\begin{cases} S_1 ::= Agents \quad S_2 ::= Func(RunTerm^*) \\ S_3 ::= Fresh \mid AdversaryFresh \\ S_4 ::= sk(RunTerm) \mid pk(RunTerm) \\ S_5 ::= k(\text{"}-\text{"}, RunTerm) \end{cases}$