Seminar 2

I) OTWAY-REES PROTOCOL: → (CEVA SIMILAR LA EXAMEN)

$A \to B: M, A, B, \{N_A, M, A, B\}_{K_{AS}}$

$B \to S: M, A, B, \{N_A, M, A, B\}_{K_{AS}}, \{N_B, M, A, B\}_{K_{BS}}$

$S \to B: M, \{N_A, K_{AB}\}_{K_{AS}}, \{N_B, K_{AB}\}_{K_{BS}}$

$B \to A: M, \{N_A, K_{AB}\}_{K_{AS}}$

$N_A, N_B, M \Rightarrow$ NONCES

1) IDEALIZARE: $A \to B: \{N_A, M\}_{K_{AS}}$

$B \to S: \{N_A, M\}_{K_{AS}}, \{N_B, M\}_{K_{BS}}$

$S \to B: \{N_A, A \overset{K_{AB}}{\leftrightarrow} B, B \sim M\}_{K_{AS}}, \{N_B, A \overset{K_{AB}}{\leftrightarrow} B, A \sim M\}_{K_{BS}}$

$B \to A: \{N_A, A \overset{K_{AB}}{\leftrightarrow} B, B \sim M\}_{K_{AS}}$

3) SCOP: $A \models B \models M$ și $B \models A \models M$

2) ASUMPȚII:

$(\rho 1)\ A \models A \overset{K_{AS}}{\leftrightarrow} S$; $(\rho 2)\ B \models B \overset{K_{BS}}{\leftrightarrow} S$; $(\rho 3)\ S \models A \overset{K_{AS}}{\leftrightarrow} S$; $(\rho 4)\ S \models B \overset{K_{BS}}{\leftrightarrow} S$

$(\rho 5)\ S \models A \overset{K_{AB}}{\leftrightarrow} B$

$(\rho 6)\ A \models S \mid\Rightarrow A \overset{K_{AB}}{\leftrightarrow} B$; $(\rho 7)\ B \models S \mid\Rightarrow A \overset{K_{AB}}{\leftrightarrow} B$

$(\rho 8)\ A \models S \mid\Rightarrow (B \sim M)$; $(\rho 9)\ B \models S \mid\Rightarrow (A \sim M)$

$(\rho 10)\ A \models \#(N_A)$; $(\rho 11)\ B \models \#(N_B)$

$(\rho 12)\ A \models \#(M)$; $(\rho 13)\ B \models \#(M)$

4) DERIVARE:

- $B \models A \models M$?

(1) $B \lhd \{N_B, A \overset{K_{AB}}{\leftrightarrow} B, A \sim M\}_{K_{BS}}$ (PAS 3 IDEALIZARE)

(2) $B \models S \sim (N_B, A \overset{K_{AB}}{\leftrightarrow} B, A \sim M)$ (MM-SK: $\rho 2$, 1)

(3) $B \models \#(N_B, A \overset{K_{AB}}{\leftrightarrow} B, A \sim M)$ (NC: $\rho 11$)

(4) $B \models S \models (N_B, A \overset{K_{AB}}{\leftrightarrow} B, A \sim M)$ (NV: 2, 3)

(5) $B \models S \models N_B$ (BC3: 4)

(6) $B \models S \models A \overset{K_{AB}}{\leftrightarrow} B$ (BC3: 4)

(7) $B \models S \models A \sim M$ (BC3: 4)

(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) $A \rightarrow B: \{M\}_{K_A^{-1}}$ M ⇒ 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