Descrizione del Protocollo MPS[1] tramite logica BAN

Protocollo Reale

M_1: A → S: $E_{k_s}(\,A, B, N_a)\,||\,E_{k_a^-}(S(E_{k_s}(\,A, B, N_a)))$

M_2: S → A: $E_{k_a}\big(\,A, B, N_a, g_b, p_{b,} k_{b,} E_{k_s^-}(k_a, N_a)\big)\,||\,E_{k_s^-}(S(\,E_{k_a}\Big(\,A, B, N_a, g_b, p_{b,} k_{b,} E_{k_s^-}(k_a, N_a)\Big)\,))$

M_3: A → B: $E_{k_b}\big(\,A, B, N_a, N_b, Y_A, E_{k_s^-}(k_a, N_a)\big)\,||\,E_{k_a^-}(S(\,E_{k_b}\Big(\,A, B, N_a, N_b, Y_{A,} E_{k_s^-}(k_a, N_a)\Big)\,))$

M_4: B → A: $E_{k_a}\big(\,A, B, N_b, Y_B, E_{k_{ab}}(N_a)\big)\,||\,E_{k_b^-}(S(\,E_{k_a}\big(\,A, B, N_b, Y_B, E_{k_{ab}}(N_a)\big)\,))$

M_5: A → B: $E_{k_{ab}}(N_a - 1)$

Protocollo Idealizzato

M_1: A → S: $\{A, B, N_a\}_{k_s}\,||\,\{S(\{\,A, B, N_a\}_{k_s})\}_{k_a^-}$

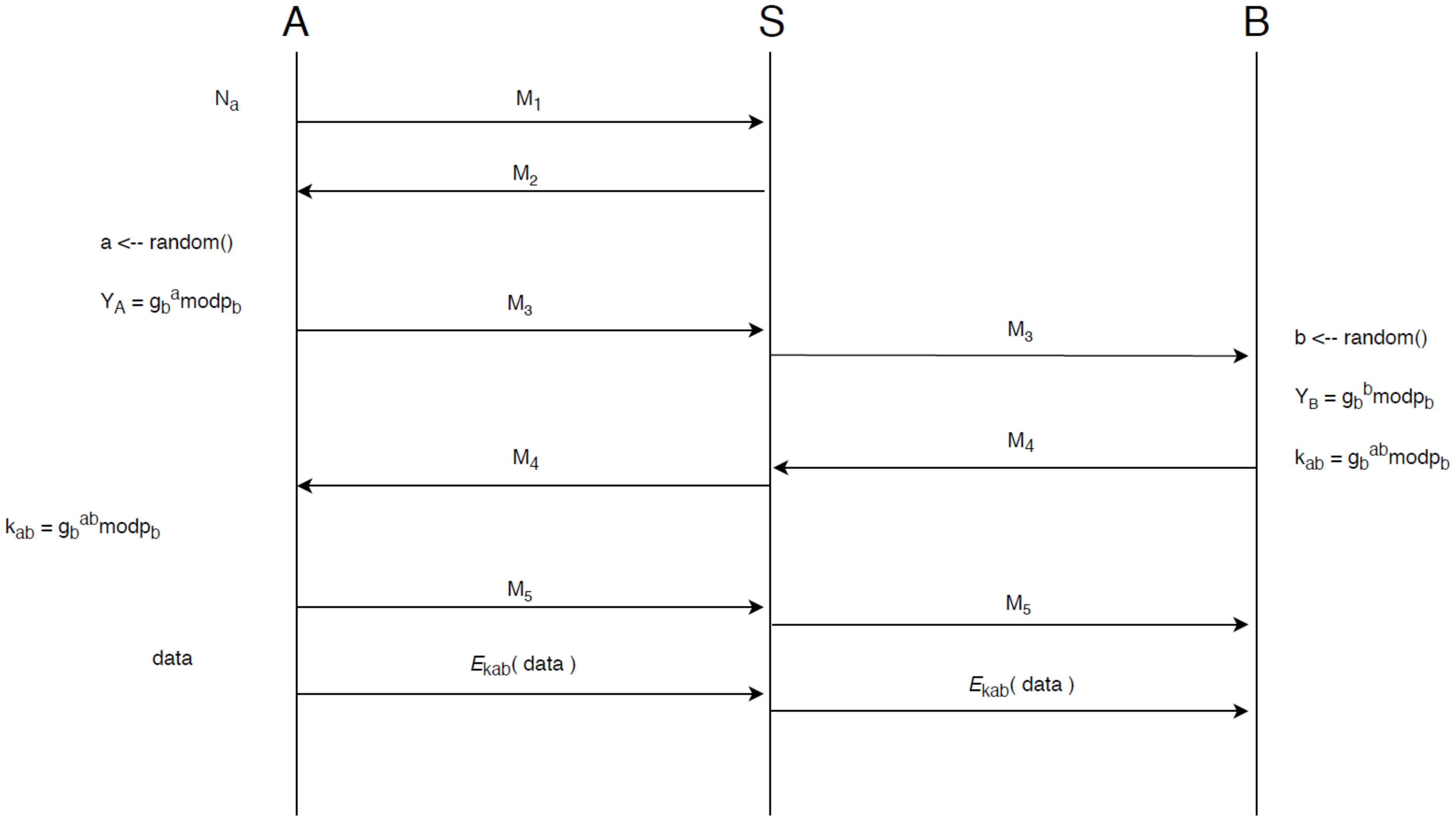
M_2: S → A: $\Big\{A, B, N_a, B \Rightarrow g_b,\ B \Rightarrow p_b, \overset{k_b}{\rightarrow} B, \Big\{\overset{k_a}{\rightarrow} A, N_a\Big\}_{k_s^-}, \#(N_a)\Big\}_{k_a}\ ||\ \Big\{S(\Big\{A, B, N_a, B \Rightarrow g_b,\ B \Rightarrow p_b, \overset{k_b}{\rightarrow} B, \Big\{\overset{k_a}{\rightarrow} A, N_a\Big\}_{k_s^-}\Big\})\Big\}_{k_s^-}$

M_3: A → B: $\Big\{A, B, N_a, N_b, A \Rightarrow Y_A, \Big\{\overset{k_a}{\rightarrow} A, N_a\Big\}_{k_s^-}, \#(N_a)\,\Big\}_{k_b}\ ||\ \Bigg\{S(\Big\{A, B, N_a, N_b, A \Rightarrow Y_A, \Big\{\overset{k_a}{\rightarrow} A, N_a\Big\}_{k_s^-}, \#(\overset{k_a}{\rightarrow} A)\,\Big\}_{k_b}\,)\Bigg\}_{k_a^-}$

M_4: B → A: $\{A, B, N_b, B \Rightarrow Y_B, \#(\,B \Rightarrow Y_B), \{N_a\}_{k_{ab}}\,\}_{k_a}\ ||\ \{S(\{A, B, N_b, B \Rightarrow Y_B, \#(\,B \Rightarrow Y_B), \{N_a\}_{k_{ab}}\,\}_{k_a})\}_{k_b^-}$

M_5: A → B: $\{N_a - 1\}_{k_{ab}}$

[1] Magherini – Pochiero – Sieni (MPS)


A
S
B
N_a
M_1
M_2
a <-- random()
$Y_A = g_b{}^a mod p_b$
M_3
M_3
b <-- random()
$Y_B = g_b{}^b mod p_b$
M_4
M_4
$k_{ab} = g_b{}^{ab} mod p_b$
$k_{ab} = g_b{}^{ab} mod p_b$
M_5
M_5
data
E_{kab}(data)
E_{kab}(data)

Analisi

Obiettivi

$A \models A \overset{k_{ab}}{\longleftrightarrow} B\,,\qquad B \models A \overset{k_{ab}}{\longleftrightarrow} B$ # Key Authentication

$A \models B \models A \overset{k_{ab}}{\longleftrightarrow} B,\qquad B \models A \models A \overset{k_{ab}}{\longleftrightarrow} B$ # Key Confirmation

Assunzioni

$A \models \overset{k_s}{\rightarrow} S\,,\qquad B \models \overset{k_s}{\rightarrow} S$ # Server Key Registration

$S \models \overset{k_a}{\rightarrow} A\,,\qquad A \models S \models \overset{k_b}{\rightarrow} B$ # Key Registration

$A \Rightarrow N_a\,,\qquad A \Rightarrow N_b,\ S \models A \Rightarrow N_a\,,\ S \models A \Rightarrow N_b$ # Nonce Authority

$A \models \#(N_a),\ \ A \models \#(N_b)$ # Freshness

$$\frac{S \models B \models (g_b, p_b),\ \ S \models B \Rightarrow (g_b, p_b)}{S \models (g_b, p_b)}$$

# Jurisdiction Rule

$A \models B \Rightarrow Y_B\,,\qquad B \models A \Rightarrow Y_A$ # Authority on Y parameters

Dopo M_1:

$$\frac{S \models \overset{k_a}{\rightarrow} A\ ,\ \ S \lhd \{A, B, N_a\}_{k_a^-}}{S \models A \mid\sim (A, B, N_a)}$$

$$\frac{S \models A \mid\sim (A, B, N_a),\ \ S \models \#(N_a)}{S \models A \models (A, B, N_a)}$$

*Na è un timestamp, il server può verificare la freschezza controllando che il messaggio sia arrivato entro un tempo limite

Dopo M_2:

$$\frac{A \models \overset{k_s}{\rightarrow} S \;,\; A \triangleleft \left\{A, B, N_a, B \Rightarrow g_b,\; B \Rightarrow p_b, \overset{k_b}{\rightarrow} B, \left\{\overset{k_a}{\rightarrow} A, N_a\right\}_{k_s^-}, \#(\overset{k_a}{\rightarrow} A)\right\}_{k_s^-}}{A \models S \mid\!\sim (A, B, N_a, B \Rightarrow g_b,\; B \Rightarrow p_b, \overset{k_b}{\rightarrow} B, \left\{\overset{k_a}{\rightarrow} A, N_a\right\}_{k_s^-}, \#(\overset{k_a}{\rightarrow} A))}$$

$$\frac{A \models S \mid\!\sim (X),\; A \models \#(N_a)}{A \models S \models (X)}$$

$$\frac{A \models S \models \overset{k_b}{\rightarrow} B \;,\; A\ trusts\ S\ on\ k_b}{A \models \overset{k_b}{\rightarrow} B}$$

$$\frac{A \models S \models (g_b, p_b) \;,\; A\ trusts\ S\ on\ (g_b, p_b)}{A \models (g_b, p_b)}$$

Dopo M_3:

$$\frac{B \models \overset{k_s}{\rightarrow} S \;,\; B \triangleleft \left\{\overset{k_a}{\rightarrow} A, N_a\right\}_{k_s^-}}{B \models S \mid\!\sim \overset{k_a}{\rightarrow} A}$$

$$\frac{B \models S \mid\!\sim \left(\overset{k_a}{\rightarrow} A\right),\; B \models \#(N_a)}{B \models S \models \left(\overset{k_a}{\rightarrow} A\right)}$$

$$\frac{B \models S \models \overset{k_a}{\rightarrow} A \;,\; B\ trusts\ S\ on\ k_a}{B \models \overset{k_a}{\rightarrow} A}$$

$$\frac{B \models \overset{k_a}{\rightarrow} A \;,\; B \triangleleft \{X\}_{k_a^-}}{B \models A \mid\!\sim (X)}$$

$$\frac{B \models A \mid\sim (X),\ \ B \models \#(N_a)}{B \models A \models (X)}$$

$$\frac{B \models A \models Y_A,\ \ B \models A \Rightarrow Y_A}{B \models Y_A}$$

$$\frac{B \models Y_A,\ \ B \Rightarrow Y_B}{B \models A \overset{k_{ab}}{\longleftrightarrow} B}$$

Dopo M_4:

$$\frac{A \models \overset{k_b}{\rightarrow} B\,,\ \ A \triangleleft \{X\}_{k_b^-}}{A \models B \mid\sim (X)}$$

$$\frac{A \models B \mid\sim (X),\ \ A \models \#(N_b)}{A \models B \models (X)}$$

$$\frac{A \models B \models Y_B,\ \ A \models B \Rightarrow Y_B}{A \models Y_B}$$

$$\frac{A \models Y_B,\ \ A \Rightarrow Y_A}{A \models A \overset{k_{ab}}{\longleftrightarrow} B}$$

$$\frac{A \models A \overset{k_{ab}}{\longleftrightarrow} B,\ \ A \triangleleft \{N_a\}_{k_{ab}}}{A \models B \mid\sim (N_a)}$$

$$\frac{A \models B \mid\sim (N_a),\ \ A \models \#(N_a)}{A \models B \models A \overset{k_{ab}}{\longleftrightarrow} B}$$

Dopo M_5:

$$\frac{B \models A \overset{k_{ab}}{\longleftrightarrow} B,\ B \triangleleft \{N_a - 1\}_{k_{ab}}}{B \models A \mid\sim (N_a - 1)}$$

$$\frac{B \models A \mid\sim (N_a - 1),\ B \models \#(N_a - 1)}{B \models A \models A \overset{k_{ab}}{\longleftrightarrow} B}$$