

# Lógicas para Autenticação e Sigilo

Universidade Federal do Rio de Janeiro

Anna Carolina C. M. de Oliveira  
Luiz Cláudio F. Fernandez

Instituto Alberto Luiz Coimbra de Pós-Graduação e Pesquisa de Engenharia  
Programa de Engenharia de Sistemas e Computação

01 de outubro de 2015

# Sumário

Introdução

Modelo de Dolev & Yao

Reconciling Two Views of Cryptography

Lógica BAN

Lógica Epistêmica Multi-Agentes Dolev/Yao

# Motivação

- Existem duas abordagens: lógica e algébrica;
- Confiabilidade também na lógica do protocolo de segurança;
- Se assegurar de possíveis ataques;
- Raciocínio sobre conhecimento do protocolo (nosso trabalho).

## Artigos

- Danny Dolev and Andrew C. Yao. On the Security of Public Key Protocols.
- Martín Abadi and Phillip Rogaway. Reconciling Two Views of Cryptography (The Computational Soundness of Formal Encryption)\*.
- Martín Abadi and Andrew D. Gordon. A Calculus for Cryptographic Protocols: The Spi Calculus.
- Michael Burrows, Martín Abadi, and Roger Needham. A Logic of Authentication.
- Simon Kramer. Cryptographic Protocol Logic: Satisfaction for (Timed) Dolev-Yao Cryptography.

# Modelo de Dolev & Yao

## Modelo: Protocolos de Chave Pública

Considera uma criptografia perfeita, modelo formal para verificação de protocolos (lógica do protocolo).

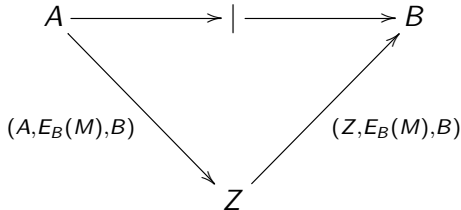
- $E_X$ : função de encriptação (pública);
- $D_X$ : função de deciptação (conhecido apenas pelo agente  $X$ );
- $D_X E_X(M) = M$ ;
- O agente  $X$  conhece os fragmentos  $M$  e  $N \leftrightarrow X$  conhece  $(M, N)$ .

## Exemplo 1

A envia a mensagem  $M$  para  $B$

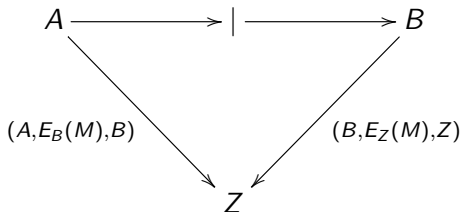
$$A \longrightarrow (A, E_B(M), B) \longrightarrow B$$

O intruso  $Z$  intercepta a mensagem enviada de  $A$  para  $B$  e envia a mensagem  $(Z, E_B(M), B)$  para  $B$



## Exemplo 1

$B$  envia a mensagem  $(B, E_Z(M), Z)$  para  $Z$



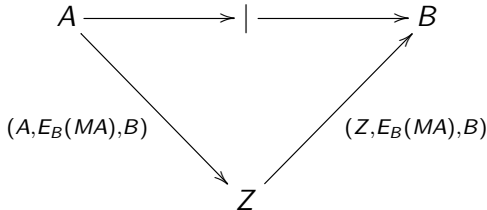
O intruso  $Z$  decodifica  $E_Z(M)$  e obtém  $M$

## Exemplo 2

A envia a mensagem  $MA$  para  $B$

$$A \longrightarrow (A, E_B(MA), B) \longrightarrow B$$

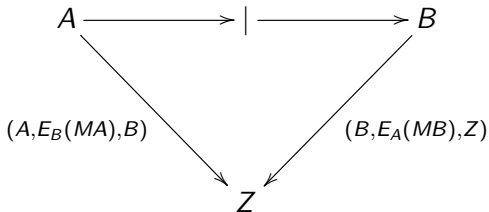
O intruso  $Z$  intercepta a mensagem enviada de  $A$  para  $B$  e envia a mensagem  $(Z, E_B(MA), B)$  para  $B$





## Exemplo 2

$B$  envia a mensagem  $(B, E_A(MB), Z)$  para  $Z$



O intruso  $Z$  **não** decodifica  $E_A(MB)$  para obter  $M$

O protocolo é seguro contra a tentativa maliciosa do intruso de saber o conteúdo da comunicação.

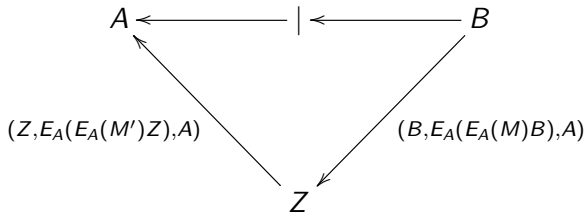
## Exemplo 3

$A$  envia a mensagem  $E_B(E_B(M)A)$  para  $B$

$$A \longrightarrow (A, E_B(E_B(M)A), B) \longrightarrow B$$

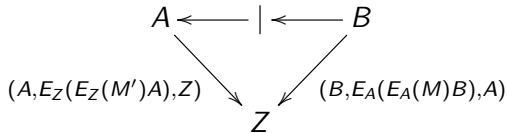
$B$  envia a mensagem  $E_A(E_A(M)B)$  para  $A$

O intruso  $Z$  intercepta a mensagem enviada de  $B$  para  $A$ , denota  $E_A(M)B$  por  $M'$  e envia a mensagem  $(Z, E_A(E_A(M')Z), A)$  para  $A$

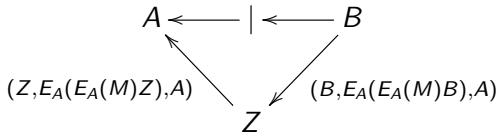


## Exemplo 3

A envia a mensagem  $(A, E_Z(E_Z(M')A), Z)$  para  $Z$

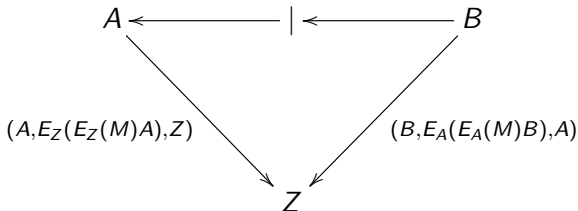


O intruso  $Z$  decodifica  $E_Z(M')$ , obtendo  $E_A(M)$  e envia a mensagem  $(Z, E_A(E_A(M)Z), A)$  para  $A$



## Exemplo 3

A envia a mensagem  $(A, E_Z(E_Z(M)A), Z)$  para Z



O intruso Z decodifica  $E_Z(M)$  e obtém  $M$

# Regras

Essas regras não são apresentadas no artigo original, mas é possível facilmente obtê-las com a teoria contida no paper.

- $\mathcal{K} = \{K_1, \dots\}$  - conjunto de chaves;
- $\{M\}_K$  - mensagem codificada.

# Regras

Reflexividade

$$\frac{M \in T}{T \vdash M}$$

Encriptação

$$\frac{T \vdash K \quad T \vdash M}{T \vdash \{M\}_K}$$

Decriptação

$$\frac{T \vdash \{M\}_K \quad T \vdash K}{T \vdash M}$$

Par-Composição

$$\frac{T \vdash M \quad T \vdash N}{T \vdash (M, N)}$$

Par-Decomposição

$$\frac{T \vdash (M, N)}{T \vdash M} \quad \frac{T \vdash (M, N)}{T \vdash N}$$

## Exemplo 1

- 1  $T = \{Z\}$
- 2  $Z$  intercepta a mensagem enviada de  $A$  para  $B$ :  
 $T = \{Z, (A, (E_B(M), B))\}$ 
  - a Aplicando reflexividade e decomposição:  
 $T = \{Z, (A, (E_B(M), B))\} \vdash (E_B(M), B)$
  - b Aplicando reflexividade e composição em 2.a:  
 $T = \{Z, (A, (E_B(M), B))\} \vdash (Z, (E_B(M), B))$
- 3  $Z$  envia a mensagem  $(Z, E_B(M), B)$  para  $B$ :  
 $T = \{Z, (A, (E_B(M), B))\}$
- 4  $B$  envia a mensagem  $(B, E_Z(M), Z)$  para  $Z$ :  
 $T = \{Z, (A, (E_B(M), B)), (B, (E_Z(M), Z))\}$ 
  - a Aplicando reflexividade e decomposição duas vezes:  $T \vdash E_Z(M)$
  - b Aplicando reflexividade:  $T \vdash Z$
  - c Aplicando decriptação em 4.a e 4.b obtemos:  $T \vdash M$

# Reconciling Two Views of Cryptography

Reconciliando as duas abordagens da confiabilidade dos protocolos de segurança.

- Visão formal, quebra da lógica do protocolo;
- Visão probabilística, quebra da chave da criptografia.



# Encriptação Formal

- Expressão de equivalência;
- Equivalência de expressões:  $E_1 \equiv E_2$ ;
- Duas partes do dado semelhantes;
- $\square$  representa um texto cifrado em que um "bisbilhoteiro" não pode decodificar;
- Se  $E \equiv \square$  significa que o "bisbilhoteiro" não consegue decifrar;
- Expressões são toda informação que o intruso intercepta.

# Linguagem

- Expressões:

$$E ::= i \mid K \mid (E_1, E_2) \mid \{E\}_K \mid \square$$

Onde:

- $i \in \{0, 1\}$  - Bits (Mensagens)
- $K \in \{K_1, \dots\}$  - Chaves
- $\square$  - indecifrável

# Regras

As regras são como no Dolev e Yao. Seja  $M$  e  $N$  expressões

- $M \vdash 0$  e  $M \vdash 1$
- $M \vdash M$
- se  $M \vdash K$  e  $M \vdash N$ , então  $M \vdash \{N\}_K$
- se  $M \vdash \{N\}_K$  e  $M \vdash K$ , então  $M \vdash N$
- se  $M \vdash N_1$  e  $M \vdash N_2$ , então  $M \vdash (N_1, N_2)$
- se  $M \vdash (N_1, N_2)$ , então  $M \vdash N_1$  e  $M \vdash N_2$

# Lógica BAN

- Nome proveniente das iniciais dos autores (Burrows, Abadi e Needham);
- Marco na área de autenticação;
- Protocolos são traduzidos e interpretados até deduzirmos se quem está esperando a mensagem comprova que:
  - ela foi enviada pelo remetente original;
  - ela é recente o suficiente.

## Símbolos

- $A$ ,  $B$  e  $S$ : agentes específicos;
- $K_{ab}$ ,  $K_{as}$  e  $K_{bs}$ : chaves compartilhadas específicas;
- $K_a$ ,  $K_b$  e  $K_s$ : chaves públicas específicas;
- $K_a^{-1}$ ,  $K_b^{-1}$  e  $K_s^{-1}$ : chaves privadas correspondentes;
- $N_a$ ,  $N_b$  e  $N_s$ : declarações específicas;
- $P$ ,  $Q$  e  $R$ : agentes genéricos;
- $X$  e  $Y$ : declarações genéricas;
- $K$ : chave genérica.

## Sintaxe

- O único conectivo proposicional é a conjunção, denotada por uma vírgula (com propriedades tais como associatividade e comutatividade);
- $P$  **believes**  $X$ ;
- $P$  **sees**  $X$ ;
- $P$  **said**  $X$ ;
- $P$  **controls**  $X$ :  $P$  tem jurisdição sobre  $X$ ;
- **fresh**( $X$ ): a fórmula  $X$  é recente;

## Sintaxe

- $P \stackrel{K}{\leftrightarrow} Q$ :  $P$  e  $Q$  usam a chave compartilhada  $K$ ;
- $\stackrel{K}{\mapsto} P$ :  $P$  tem  $K$  como chave pública;
- $P \stackrel{X}{\rightleftharpoons} Q$ :  $X$  é um segredo apenas conhecido por  $P$  e  $Q$ ;
- $\{X\}_K$ : representa a fórmula  $X$  codificada sobre a chave  $K$ ;
- $\langle X \rangle_Y$ : representa  $X$  combinado com a fórmula  $Y$ .

## Regras

*Conteúdo da mensagem:*

Para chaves compartilhadas 
$$\frac{P \text{ believes } Q \stackrel{K}{\leftrightarrow} P, \quad P \text{ sees } \{X\}_K}{P \text{ believes } Q \text{ said } X}$$

Para chaves públicas 
$$\frac{P \text{ believes } \stackrel{K}{\leftrightarrow} Q, \quad P \text{ sees } \{X\}_{K^{-1}}}{P \text{ believes } Q \text{ said } X}$$

Para chaves privadas 
$$\frac{P \text{ believes } Q \stackrel{Y}{\Rightarrow} P, \quad P \text{ sees } \langle X \rangle_Y}{P \text{ believes } Q \text{ said } X}$$



## Regras

$$\text{Controle: } \frac{P \text{ believes } Q \text{ controls } X, \quad P \text{ believes } Q \text{ believes } X}{P \text{ believes } X}$$

$$\text{Visão do agente: } \frac{P \text{ sees } (X, Y)}{P \text{ sees } X} \quad \frac{P \text{ sees } \langle X \rangle_Y}{P \text{ sees } X}$$

$$\frac{P \text{ believes } Q \stackrel{K}{\leftrightarrow} P, \quad P \text{ sees } \{X\}_K}{P \text{ sees } X}$$

## Regras

$$\frac{P \text{ believes } \stackrel{K}{\mapsto} P, \quad P \text{ sees } \{X\}_K}{P \text{ sees } X}$$

$$\frac{P \text{ believes } \stackrel{K}{\mapsto} Q, \quad P \text{ sees } \{X\}_{K^{-1}}}{P \text{ sees } X}$$

*Recentidade:*

$$\frac{P \text{ believes } \text{fresh}(X)}{P \text{ believes } \text{fresh}(X, Y)}$$

## Exemplo 1

- $m_1 : A \longrightarrow B : \{m\}_{K_B}$
- $m_2 : Z \longrightarrow B : \{m\}_{K_B}$
- $m_3 : B \longrightarrow Z : \{m\}_{K_Z}$
- $B$  believes  $A \xleftrightarrow{K_B} B$
- $Z$  believes  $B \xleftrightarrow{K_Z} Z$
- $m_1 : Z$  sees  $\{m\}_{K_B}$
- $m_2 : B$  sees  $\{m\}_{K_B}$
- $B$  sees  $m$  (*regra Visão do agente*)
- $m_3 : Z$  sees  $\{m\}_{K_Z}$
- $Z$  sees  $m$  (*regra Visão do agente*)

## S5<sub>DY</sub>

- Raciocínio sobre conhecimento em protocolos;
- Que tipo de conhecimento?
- Conhecimento sobre:
  - chaves;
  - mensagens;
  - encriptação/decriptação;
  - concatenação;
  - agentes e grupos, etc.

# Linguagem

- As fórmulas são construídas a partir de expressões (dados que podem ser codificados, decodificados ou concatenados) e não apenas de símbolos proposicionais;
- Alfabeto:
  - um conjunto enumerável  $\Phi$  de símbolos proposicionais;
  - um conjunto finito  $\mathcal{A}$  de agentes;
  - um conjunto de chaves  $\mathcal{K} = \{k_1, \dots\}$ ;
  - os conectivos booleanos  $\neg$  e  $\wedge$ ;
  - modalidades  $K_a$  para cada agente  $a$ .

# Linguagem

- Expressões:

$$E ::= p \mid k \mid (E_1, E_2) \mid \{E\}_k$$

onde  $k \in \mathcal{K}$ .

- Fórmulas:

$$\varphi ::= e \mid \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid K_a\varphi$$

onde  $e \in E$ ,  $a \in \mathcal{A}$ .

# Semântica

- *Frame* é uma tupla  $\mathcal{F} = (W, \sim_a)$  onde:
  - $W$  é um conjunto não vazio de estados;
  - $\sim_a \subseteq W \times W$  é uma relação binária reflexiva, transitiva e simétrica em  $W$ , para cada agente  $a \in \mathcal{A}$ ;
- *Modelo* é um par  $\mathcal{M} = (\mathcal{F}, \mathbf{V})$ , onde  $\mathcal{F}$  é um frame e  $\mathbf{V}$  é uma função de valoração  $\mathbf{V} : E \rightarrow 2^W$  satisfazendo:
  - 1  $V(m) \cap V(k) \subseteq V(\{m\}_k)$
  - 2  $V(\{m\}_k) \cap V(k) \subseteq V(m)$
  - 3  $V(m) \cap V(n) = V((m, n))$

# Semântica

- Chamamos de *estado epistêmico* um modelo epistêmico multi-agentes enraizado  $(\mathcal{M}, s)$ ;
- Satisfação  $\mathcal{M}, s \models \varphi$ :
  - $\mathcal{M}, s \models e$  sse  $s \in V(e)$ ;
  - $\mathcal{M}, s \models \neg\phi$  sse  $\mathcal{M}, s \not\models \phi$ ;
  - $\mathcal{M}, s \models \phi \wedge \psi$  sse  $\mathcal{M}, s \models \phi$  e  $\mathcal{M}, s \models \psi$ ;
  - $\mathcal{M}, s \models K_a\phi$  sse, para todo  $s' \in S : s \sim_a s' \Rightarrow \mathcal{M}, s' \models \phi$ .



# Axiomatização

- ① *Todas as instanciações de tautologias proposicionais;*
- ②  $K_a(\varphi \rightarrow \psi) \rightarrow (K_a\varphi \rightarrow K_a\psi)$ ;
- ③  $K_a\varphi \rightarrow \varphi$ ;
- ④  $K_a\varphi \rightarrow K_aK_a\varphi$  (+ introspecção);
- ⑤  $\neg K_a\varphi \rightarrow K_a\neg K_a\varphi$  (- introspecção);
- ⑥  $K_am \wedge K_ak \rightarrow K_a\{m\}_k$  (codificação);
- ⑦  $K_a\{m\}_k \wedge K_ak \rightarrow K_am$  (decodificação);
- ⑧  $K_am \wedge K_an \leftrightarrow K_a(m, n)$  (composição e decomposição).

## Regras de Inferência

M.P.  $\varphi, \varphi \rightarrow \psi / \psi$     U.G.  $\varphi / K_a\varphi$

## Corretude

- “Tudo que o cálculo dedutivo prova é semanticamente válido”;
- I.e., se uma fórmula é provada a partir de um conjunto de fórmulas então ela é consequência lógica do mesmo;
- Demonstramos isso provando que os axiomas do cálculo dedutivo são tautologias.

**Lemma:** Os axiomas abaixo são corretos.

- 1  $\Vdash K_a m \wedge K_a k \rightarrow K_a \{m\}_k$  (codificação)
- 2  $\Vdash K_a \{m\}_k \wedge K_a k \rightarrow K_a m$  (decodificação)
- 3  $\Vdash K_a m \wedge K_a n \leftrightarrow K_a(m, n)$  (composição e decomposição)

## Corretude

### Prova 1.

Supondo  $\not\models K_a m \wedge K_a k \rightarrow K_a \{m\}_k$ . Existe um modelo  $M$  e um estado  $w$  t.q.  $M, w \not\models K_a m \wedge K_a k \rightarrow K_a \{m\}_k$ .

$M, w \models K_a m \wedge K_a k$  sse

$M, w \models K_a m$  (i) e  $M, w \models K_a k$  (ii)

$M, w \not\models K_a \{m\}_k$  (iii)

(i) para todo  $v$ ,  $w \sim_a v \Rightarrow v \in V(m)$

(ii) para todo  $v$ ,  $w \sim_a v \Rightarrow v \in V(k)$

(iii) existe  $v$ ,  $w \sim_a v$  e  $v \notin V(\{m\}_k)$

por (i), (ii) e (iii), temos que existe um  $v$ , t.q.  $v \in V(m)$  e  $v \in V(k)$  mas  $v \notin V(\{m\}_k)$ , o que contradiz a primeira condição da nossa noção de modelo. □

# Completude

- “Tudo que é semanticamente válido é provado pelo cálculo dedutivo”;
- I.e., tudo que é semanticamente obtido pode ser também obtido no sistema dedutivo.
- Prova por modelo canônico;
- Construção Fisher/Ladner  $\Rightarrow$  Modelo finito;
- Propriedade do modelo finito.

$S5_{DY}^{CK}$

$$S5_{DY}^{CK} = S5_{DY} + \text{Conhecimento Comum}$$

Temos os axiomas e regras do  $S5_{DY}$ , acrescentando:

- 9  $E_G \varphi \leftrightarrow \bigwedge_{a \in G} K_a \varphi$ ;
- 10  $C_G(\varphi \rightarrow \psi) \rightarrow (C_G \varphi \rightarrow C_G \psi)$ ;
- 11  $C_G \varphi \rightarrow (\varphi \wedge E_G C_G \varphi)$ ;
- 12  $C_G(\varphi \rightarrow E_G \varphi) \rightarrow (\varphi \rightarrow C_G \varphi)$  (+ indução).

**Regra de Inferência**

U.G.  $\varphi / C_G \varphi$

Podemos assumir que  $k_{XY} = k_{YX}$  para cada agente  $X$  e  $Y$ .

$$KB_0 = \{K_A k_{AB}, K_B k_{AB}, K_B k_{BZ}, K_Z k_{BZ}, K_A m\}$$

$$\begin{array}{c} \text{send}_{AB}(\{m\}_{k_{AB}}) \\ \downarrow \\ \text{---} \end{array}$$

$$\begin{array}{c} Z \text{ intercepts} \\ \downarrow \\ KB_1 := KB_0 \cup K_Z \{m\}_{k_{AB}} \end{array}$$

$$\begin{array}{c} \text{send}_{ZB}(\{m\}_{k_{AB}}) \\ \downarrow \\ KB_2 := KB_1 \cup K_B \{m\}_{k_{AB}} \end{array}$$

$$K_B m \quad ax. 7$$

$$\begin{array}{c}
 K_B \{m\}_{k_{BZ}} \quad ax. 6 \\
 \downarrow send_{BZ}(\{m\}_{k_{BZ}}) \\
 KB_3 := KB_2 \cup K_Z \{m\}_{k_{BZ}}
 \end{array}$$

$$K_Z m \quad ax. 7$$

O intruso  $Z$  sabe  $m$ .

## Uma Extensão do $S5_{DY}$

- Linguagem da mensagem:

$$M ::= a \mid k \mid (M_1, M_2) \mid \{M\}_k$$

- Linguagem:

$$\alpha ::= p \mid \neg\alpha \mid \alpha \wedge \alpha \mid K_a\alpha \mid akM$$

onde:

- $akM$  - expressa o conhecimento *de re* (conteúdo)
- $K_a\alpha$  - expressa o conhecimento *de dicto*



## Uma Extensão do $S5_{DY}$

### Axiomatização:

- 1 *Todas as instanciações de tautologias proposicionais;*
- 2 *aka (todos os agentes sabem seu próprio nome);*
- 3  $akM \wedge akM' \leftrightarrow ak(M, M')$  (composição e decomposição);
- 4  $akM \wedge akk \rightarrow ak\{M\}_k$  (criptação);
- 5  $ak\{M\}_k \wedge akk \rightarrow akM$  (decriptação);
- 6  $K_a\alpha \wedge K_a(\alpha \rightarrow \beta) \rightarrow K_a\beta$ ;
- 7  $K_a\alpha \rightarrow \alpha$ ;
- 8  $K_a\alpha \rightarrow K_aK_a\alpha$ ;
- 9  $\neg K_a\alpha \rightarrow K_a\neg K_a\alpha$ ;
- 10  $akM \rightarrow K_aakM$  (+ *de re introspecção*);
- 11  $\neg(akM) \rightarrow K_a\neg(akM)$  (- *de re introspecção*);