

# Exame (Época Normal)

Linguagens e Modelos de Concorrência e Segurança

25 Junho 2008

## I

1. Considere os seguintes processos CCS:

$$GAMBLE1 \triangleq \tau.heads.GAMBLE1 + \tau.tails.GAMBLE1$$

$$GAMBLE2 \triangleq (\text{new coin})(\overline{coin} \mid coin.heads.GAMBLE2 \mid coin.tails.GAMBLE2)$$

- (a) Explique que sistema que *GAMBLE1* está a modelar.
  - (b) Os sistemas especificados por *GAMBLE1* e *GAMBLE2* são equivalentes, em termos da relação de bisimilaridade forte? Justifique a sua resposta: no caso positivo indique qual a bisimulação, no caso negativo, indique um contexto que permita distinguir *GAMBLE1* de *GAMBLE2*.
2. Considere a seguinte especificação muito simples:

$$\begin{aligned}EMPTY &= in.ONE \\ONE &= in.TWO + out.EMPTY \\TWO &= out.ONE\end{aligned}$$

que representa um buffer limitado, com capacidade para dois elementos. Um buffer deste tipo pode ser implementado com dois processos independentes. Descreva uma implementação em CCS deste buffer crescente usando dois processos separados e comunicantes, cada um representando um elemento no buffer. A especificação de cada bit deve ser idêntica (a menos dos nomes dos canais).

Mostre a equivalência entre a especificação e a implementação usando a ferramenta MWB e envie a solução por email.

## II

1. Considere um sistema distribuído constituído por três workstations que partilham uma impressora. Em cada momento, apenas a workstation *i* pode estar a imprimir, o que assinalado através de uma acção *printing<sub>i</sub>* (com *i* entre 1 e 3).

- (a) Apresente um modelo em PI do sistema considerado sob a forma de uma especificação sequencial simples, sem usar composição paralela.
- (b) Apresente um modelo em PI em que a impressora e as workstations são representadas por processos independentes.
- (c) Mostre como exprimir as seguintes propriedades do sistema que descreveu na alínea (b).
  - O sistema tem sempre menos que 5 processos independentes (threads).
  - Apenas uma impressora pode estar a imprimir num dado momento.
  - O sistema nunca atinge uma situação de bloqueio (deadlock).
  - Se uma workstation pretende imprimir, o sistema pode sempre evoluir de forma a satisfazer esse pedido, apesar de não haver garantia de satisfação.
- (d) Verifique as propriedades acima na ferramenta SLMC e envie a solução por email.

### III

Considere o seguinte protocolo criptográfico entre dois principais  $A$  e  $B$ , que usa criptografia simétrica. Inicialmente,  $A$  e  $B$  partilham uma chave secreta  $KAB$ , conhecida apenas por si.

$$\begin{aligned}
 A \rightarrow B &: \text{ida}, \{N_a\}_{KAB} \\
 B \rightarrow A &: \{N_a, N_b\}_{KAB} \\
 A \rightarrow B &: \{N_b\}_{KAB} \\
 B \rightarrow A &: \{KAB', N_a\}_{KAB}
 \end{aligned}$$

O objectivo é que os dois parceiros  $A$  e  $B$  no fim do protocolo partilhem uma nova chave secreta  $KAB'$ , conhecida apenas por ambos. Os dados  $N_a$  e  $N_b$  são identificadores frescos (nonces) gerados no momento (por exemplo, time stamps).

Considere a propriedade de confidencialidade seguinte: se no fim do protocolo  $A$  e  $B$  trocarem uma mensagem cifrada com a chave  $KAB$ , o conteúdo de tal mensagem não poder ser adquirido por nenhum atacante em tempo útil.

1. Modele o sistema numa variante adequada do modelo SPI.  
Justifique se o seu modelo satisfaz a propriedade de confidencialidade referida.
2. Modele o sistema na ferramenta Proverif e verifique a propriedade de confidencialidade referida (envie a sua solução por email).