

**Exercice 1** Équivalence à renommage près

On considère la fonction pattern suivante :

$$\begin{aligned}
 p(K, C) &= K && K \in \mathbf{Keys} \\
 p(b, C) &= b && b \in \mathbf{Bool} \\
 p(\langle M, N \rangle, C) &= \langle p(M, C), p(N, C) \rangle \\
 p(\{M\}_K, C) &= \{p(M, C)\}_K && \text{si } K \in C \\
 p(\{M\}_K, C) &= \{\square\}_K && \text{si } K \notin C
 \end{aligned}$$

On définit ensuite la notion d'équivalence et d'équivalence à renommage près comme vu en cours. Dire pour chacun des couples de termes  $(T_1, T_2)$  suivants, si  $T_1$  et  $T_2$  sont équivalents à renommage près (selon cette nouvelle définition).

$T_1$	$T_2$
$\mathbf{0}$	$\mathbf{0}$
$\mathbf{0}$	$\mathbf{1}$
$\{\mathbf{0}\}_K$	$\{\mathbf{1}\}_K$
$\langle K, \{\mathbf{0}\}_K \rangle$	$\langle K, \{\mathbf{1}\}_K \rangle$
$\langle K, \{\{\mathbf{0}\}_{K'}, \mathbf{0}\}_K \rangle$	$\langle K, \{\{\mathbf{1}\}_{K'}, \mathbf{0}\}_K \rangle$
$\{\mathbf{0}\}_K$	$\{K\}_K$
$\{\langle \mathbf{0}, \mathbf{0} \rangle \langle \mathbf{0}, \mathbf{0} \rangle\}_K$	$\{\mathbf{0}\}_K$
$\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle$	$\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle$
$\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle$	$\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle$

**Exercice 2** Cycle de clefs

Les cycles de clefs posent des problèmes dans les résultats de type « soundness ». Considérons un schéma de chiffrement  $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  sémantiquement sûr, i.e. de type-0. Construire un schéma de chiffrement  $\Pi' = (\mathcal{K}', \mathcal{E}', \mathcal{D}')$  de type-0 tel que :

$$\llbracket \{k\}_k \rrbracket_{\Pi, \eta} \not\approx \llbracket \{0^{|k|}\}_k \rrbracket_{\Pi, \eta}$$

**Exercice 3** Exercice posé à l'examen de l'an dernier

1. Soient les termes  $T_1 = \langle \{K_1\}_{K_3}, \{K_2\}_{K_3} \rangle$  et  $T_2 = \langle \{\mathbf{0}\}_{K_1}, \{K_2\}_{K_3} \rangle$ . Quels sont les *patterns* de  $T_1$  et  $T_2$ . Est-ce que ces deux termes sont formellement indistinguables ?

2. La preuve de correction cryptographique en présence d'un attaquant passif vue au cours suppose la définition de sécurité d'un schéma de chiffrement suivante.

*Un schéma de chiffrement  $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$  est sémantiquement sûr si pour toute machine de Turing probabiliste polynomiale  $\mathcal{A}$  l'avantage*

$$Adv_{\Pi, \eta}(\mathcal{A}) = Pr[k, k' \xleftarrow{R} \mathcal{K}(\eta) : \mathcal{A}^{\mathcal{E}_k(\cdot), \mathcal{E}_{k'}(\cdot)}(\eta) = 1] - Pr[k \xleftarrow{R} \mathcal{K}(\eta) : \mathcal{A}^{\mathcal{E}_k(\mathbf{0}), \mathcal{E}_k(\mathbf{0})}(\eta) = 1]$$

*est une fonction négligeable en  $\eta$ .*

Nous redéfinissons la sécurité avec la fonction d'avantage suivante :

$$Adv_{\Pi, \eta}(\mathcal{A}) = Pr[k \xleftarrow{R} \mathcal{K}(\eta) : \mathcal{A}^{\mathcal{E}_k(\cdot)}(\eta) = 1] - Pr[k \xleftarrow{R} \mathcal{K}(\eta) : \mathcal{A}^{\mathcal{E}_k(\mathbf{0})}(\eta) = 1]$$

Expliquez pourquoi cette définition est plus faible et pourquoi le résultat de correction vu au cours n'est plus correcte. Vous pouvez baser votre explication sur l'exemple des termes  $T_1$  et  $T_2$  ci-dessus.