Reconciling two views of cryptography (The computational soundness of formal encryption)

Stéphanie Delaune

Laboratoire Spécification et Vérification
ENS Cachan

$\longrightarrow$ Ces transparents sont issus en grande partie d'une présentation faite par Steve Kremer

Motivation

Deux approches pour analyser les protocoles cryptographiques :

	Approche formelle	Approche calculatoire
Messages	idéalisé (termes)	exacte (bitstrings)
Cryptographie	idéalisé	exacte
Adversaire	idéalisé	machine de Turing PPT arbitraire
Preuves	automatisable	à la main avec risque d'erreur
Garanties de sécurité	pas claires	fortes

Lien entre ces deux approches ?

But : Prendre le meilleur des deux approches : avoir des preuves formelles qui impliquent les garanties plus fortes du modèle calculatoire

Ce cours

Étude du papier de Martín Abadi et Phillip Rogaway.

Reconciling two views of cryptography
(The computational soundness of formal encryption)

Un des premiers résultat dans ce domaine :

- adversaire : passif
- primitives cryptographiques : paire + chiffrement symétrique
- propriété de sécurité : équivalence

Plan

Indistinguabilité vs déduction

Dans certaines situations le secret (en tant que dérivabilité) n'est pas adéquat :

Par exemple, soit $S = \{\mathbf{0}, \mathbf{1}\}$

$$t_1 = \mathbf{0} \qquad\qquad t_2 = \mathbf{1}$$

L'ensemble des termes déductibles de $S \cup \{t_1\}$ et $S \cup \{t_2\}$ est le même. Pourtant, intuitivement, t_1 et t_2 sont distinguables.

$$t_1' = \{\mathbf{0}\}_k \qquad\qquad t_2' = \{\mathbf{1}\}_k$$

On s'attend à ce que t_1' et t_2' soient indistinguables.

Algèbre de termes

Dans la suite nous considérons l'algèbre de termes générée par la signature

$$\mathbf{enc}/2, \mathbf{pair}/2$$

ainsi que des constantes dans **Bool** et **Keys** où

$$\mathbf{Bool} = \{\mathbf{0}, \mathbf{1}\} \qquad \mathbf{Keys} = \{k, k_1, k_2, \ldots, k', k'', \ldots\}$$

De plus nous supposons que le symbole **enc** ne prend en deuxième argument que des constantes dans **Keys**. Les termes sont donc générés par la grammaire suivante :

$$\begin{array}{lll} M, N ::= & & \text{termes} \\ & K & K \in \mathbf{Keys} \\ & 0, 1 & \mathbf{Bool} \\ & \langle M, N \rangle & \mathbf{pair} \\ & \{M\}_K & \mathbf{enc}\ (K \in \mathbf{Keys}) \end{array}$$

On étend également $\mathcal{I}_{DY}$ par les règles $\dfrac{}{\mathbf{0}}$ et $\dfrac{}{\mathbf{1}}$.

Patterns

On utilise le symbole $\square$ pour un chiffré pour lequel l'intrus ne connaît pas la clé. On définit ainsi les patterns

$$
\begin{array}{lll}
P, Q ::= & & \text{patterns} \\
& K & K \in \mathbf{Keys} \\
& 0, 1 & \mathbf{Bool} \\
& \langle P, Q \rangle & \mathbf{pair} \\
& \{P\}_K & \mathbf{enc}\ (K \in \mathbf{Keys}) \\
& \square &
\end{array}
$$

Patterns

On utilise le symbole $\Box$ pour un chiffré pour lequel l'intrus ne connaît pas la clé. On définit ainsi les patterns

$$
\begin{array}{lll}
P, Q ::= & & \text{patterns} \\
 & K & K \in \textbf{Keys} \\
 & 0, 1 & \textbf{Bool} \\
 & \langle P, Q \rangle & \textbf{pair} \\
 & \{P\}_K & \textbf{enc}\ (K \in \textbf{Keys}) \\
 & \Box &
\end{array}
$$

On définit la fonction $p(M, C)$ qui étant donné un terme M et un ensemble de clés C (connues par l'intrus) associe à un terme un pattern :

$$
\begin{array}{rcll}
p(K, C) & = & K & K \in \textbf{Keys} \\
p(b, C) & = & b & b \in \textbf{Bool} \\
p(\langle M, N \rangle, C) & = & \langle p(M, C), p(N, C) \rangle & \\
p(\{M\}_K, C) & = & \{p(M, C)\}_K & \text{si } K \in C \\
p(\{M\}_K, C) & = & \Box & \text{si } K \notin C
\end{array}
$$

Patterns (2)

Maintenant on définit le pattern d'un terme par rapport aux clés déductibles de ce terme

$$pat(M) = p(M, \{K \in \mathbf{Keys} \mid M \vdash_{\mathcal{I}_{DY}} K\})$$

Example

$$\begin{array}{rcl} pat(\langle \mathbf{0}, \mathbf{1} \rangle) & = & \\ pat(\langle \{\mathbf{0}\}_{K_1}, \langle \{\mathbf{1}\}_{K_2}, K_1 \rangle \rangle) & = & \\ pat(\langle \{\{K_1\}_{K_2}\}_{K_3}, K_3 \rangle) & = & \end{array}$$

Patterns (2)

Maintenant on définit le pattern d'un terme par rapport aux clés déductibles de ce terme

$$pat(M) = p(M, \{K \in \mathbf{Keys} \mid M \vdash_{\mathcal{I}_{DY}} K\})$$

Example

$$\begin{array}{rcl}
pat(\langle \mathbf{0}, \mathbf{1} \rangle) & = & \langle \mathbf{0}, \mathbf{1} \rangle \\
pat(\langle \{\mathbf{0}\}_{K_1}, \langle \{\mathbf{1}\}_{K_2}, K_1 \rangle \rangle) & = & \\
pat(\langle \{\{K_1\}_{K_2}\}_{K_3}, K_3 \rangle) & = &
\end{array}$$

Patterns (2)

Maintenant on définit le pattern d'un terme par rapport aux clés déductibles de ce terme

$$pat(M) = p(M, \{K \in \mathbf{Keys} \mid M \vdash_{\mathcal{I}_{DY}} K\})$$

Example

$$\begin{array}{rcl} pat(\langle \mathbf{0}, \mathbf{1} \rangle) & = & \langle \mathbf{0}, \mathbf{1} \rangle \\ pat(\langle \{\mathbf{0}\}_{K_1}, \langle \{\mathbf{1}\}_{K_2}, K_1 \rangle \rangle) & = & \langle \{\mathbf{0}\}_{K_1}, \langle \Box, K_1 \rangle \rangle \\ pat(\langle \{\{K_1\}_{K_2}\}_{K_3}, K_3 \rangle) & = & \end{array}$$

Patterns (2)

Maintenant on définit le pattern d'un terme par rapport aux clés déductibles de ce terme

$$pat(M) = p(M, \{K \in \mathbf{Keys} \mid M \vdash_{\mathcal{I}_{DY}} K\})$$

Example

$$\begin{array}{rcl} pat(\langle \mathbf{0}, \mathbf{1} \rangle) & = & \langle \mathbf{0}, \mathbf{1} \rangle \\ pat(\langle \{\mathbf{0}\}_{K_1}, \langle \{\mathbf{1}\}_{K_2}, K_1 \rangle \rangle) & = & \langle \{\mathbf{0}\}_{K_1}, \langle \Box, K_1 \rangle \rangle \\ pat(\langle \{\{K_1\}_{K_2}\}_{K_3}, K_3 \rangle) & = & \langle \{\Box\}_{K_3}, K_3 \rangle \end{array}$$

Equivalence de termes

Définition (Equivalence)

Deux termes M et N sont équivalents, noté $M \equiv N$ ssi $pat(M) = pat(N)$.

Problème :

Intuitivement, deux clés (aléatoires) sont équivalentes, mais on a que $k_1 \not\equiv k_2$.

Equivalence de termes

Définition (Equivalence)

Deux termes M et N sont équivalents, noté $M \equiv N$ ssi $pat(M) = pat(N)$.

Problème :

Intuitivement, deux clés (aléatoires) sont équivalentes, mais on a que $k_1 \not\equiv k_2$.

Définition (Equivalence à renommage près)

Deux termes M et N sont équivalents à renommage près, noté $M \cong N$ ssi il existe une bijection σ sur **Keys** telle que $M \equiv N\sigma$.

On a donc que $k_1 \cong k_2$ et $\langle k_1, k_2 \rangle \not\cong \langle k_3, k_3 \rangle$ (pas de bijection !)

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \quad & \mathbf{0} \\
\mathbf{0} & & \mathbf{1} \\
\{\mathbf{0}\}_K & & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K\rangle & & \langle K, \{\mathbf{1}\}_K\rangle \\
\langle K, \{\langle\{\mathbf{0}\}_{K'}, \mathbf{0}\rangle\}_K\rangle & & \langle K, \{\langle\{\mathbf{1}\}_{K'}, \mathbf{0}\rangle\}_K\rangle \\
\{\mathbf{0}\}_K & & \{K\}_K \\
\{\langle\langle \mathbf{0}, \mathbf{0}\rangle\langle \mathbf{0}, \mathbf{0}\rangle\rangle\}_K & & \{\mathbf{0}\}_K \\
\langle\{\mathbf{0}\}_K, \{\mathbf{0}\}_K\rangle & & \langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_K\rangle \\
\langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_K\rangle & & \langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'}\rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & & \mathbf{1} \\
\{\mathbf{0}\}_K & & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K\rangle & & \langle K, \{\mathbf{1}\}_K\rangle \\
\langle K, \{\langle\{\mathbf{0}\}_{K'}, \mathbf{0}\rangle\}_K\rangle & & \langle K, \{\langle\{\mathbf{1}\}_{K'}, \mathbf{0}\rangle\}_K\rangle \\
\{\mathbf{0}\}_K & & \{K\}_K \\
\{\langle\langle\mathbf{0}, \mathbf{0}\rangle\langle\mathbf{0}, \mathbf{0}\rangle\rangle\}_K & & \{\mathbf{0}\}_K \\
\langle\{\mathbf{0}\}_K, \{\mathbf{0}\}_K\rangle & & \langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_K\rangle \\
\langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_K\rangle & & \langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'}\rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K \rangle & & \langle K, \{\mathbf{1}\}_K \rangle \\
\langle K, \{\langle \{\mathbf{0}\}_{K'}, \mathbf{0} \rangle\}_K \rangle & & \langle K, \{\langle \{\mathbf{1}\}_{K'}, \mathbf{0} \rangle\}_K \rangle \\
\{\mathbf{0}\}_K & & \{K\}_K \\
\{\langle \langle \mathbf{0}, \mathbf{0} \rangle \langle \mathbf{0}, \mathbf{0} \rangle \rangle\}_K & & \{\mathbf{0}\}_K \\
\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle \\
\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & \cong & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K \rangle & & \langle K, \{\mathbf{1}\}_K \rangle \\
\langle K, \{\langle \{\mathbf{0}\}_{K'}, \mathbf{0} \rangle\}_K \rangle & & \langle K, \{\langle \{\mathbf{1}\}_{K'}, \mathbf{0} \rangle\}_K \rangle \\
\{\mathbf{0}\}_K & & \{K\}_K \\
\{\langle \langle \mathbf{0}, \mathbf{0} \rangle \langle \mathbf{0}, \mathbf{0} \rangle \rangle\}_K & & \{\mathbf{0}\}_K \\
\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle \\
\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & \cong & \{\mathbf{1}\}_K \\[1em]
\langle K, \{\mathbf{0}\}_K \rangle & \not\cong & \langle K, \{\mathbf{1}\}_K \rangle \\
\langle K, \{\langle \{\mathbf{0}\}_{K'}, \mathbf{0}\rangle\}_K \rangle & & \langle K, \{\langle \{\mathbf{1}\}_{K'}, \mathbf{0}\rangle\}_K \rangle \\
\{\mathbf{0}\}_K & & \{K\}_K \\
\{\langle\langle \mathbf{0}, \mathbf{0}\rangle \langle \mathbf{0}, \mathbf{0}\rangle\rangle\}_K & & \{\mathbf{0}\}_K \\
\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle \\
\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & \cong & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K \rangle & \not\cong & \langle K, \{\mathbf{1}\}_K \rangle \\
\langle K, \{\langle \{\mathbf{0}\}_{K'}, \mathbf{0} \rangle\}_K \rangle & \cong & \langle K, \{\langle \{\mathbf{1}\}_{K'}, \mathbf{0} \rangle\}_K \rangle \\
\{\mathbf{0}\}_K & & \{K\}_K \\
\{\langle \langle \mathbf{0}, \mathbf{0} \rangle \langle \mathbf{0}, \mathbf{0} \rangle \rangle\}_K & & \{\mathbf{0}\}_K \\
\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle \\
\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & \cong & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K \rangle & \not\cong & \langle K, \{\mathbf{1}\}_K \rangle \\
\langle K, \{\langle \{\mathbf{0}\}_{K'}, \mathbf{0} \rangle\}_K \rangle & \cong & \langle K, \{\langle \{\mathbf{1}\}_{K'}, \mathbf{0} \rangle\}_K \rangle \\
\{\mathbf{0}\}_K & \cong & \{K\}_K \\
\{\langle \langle \mathbf{0}, \mathbf{0} \rangle \langle \mathbf{0}, \mathbf{0} \rangle \rangle\}_K & & \{\mathbf{0}\}_K \\
\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle \\
\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & \cong & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K\rangle & \not\cong & \langle K, \{\mathbf{1}\}_K\rangle \\
\langle K, \{\langle\{\mathbf{0}\}_{K'}, \mathbf{0}\rangle\}_K\rangle & \cong & \langle K, \{\langle\{\mathbf{1}\}_{K'}, \mathbf{0}\rangle\}_K\rangle \\
\{\mathbf{0}\}_K & \cong & \{K\}_K \\
\{\langle\langle\mathbf{0}, \mathbf{0}\rangle\langle\mathbf{0}, \mathbf{0}\rangle\rangle\}_K & \cong & \{\mathbf{0}\}_K \\
\langle\{\mathbf{0}\}_K, \{\mathbf{0}\}_K\rangle & & \langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_K\rangle \\
\langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_K\rangle & & \langle\{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'}\rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & \cong & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K \rangle & \not\cong & \langle K, \{\mathbf{1}\}_K \rangle \\
\langle K, \{\langle \{\mathbf{0}\}_{K'}, \mathbf{0} \rangle\}_K \rangle & \cong & \langle K, \{\langle \{\mathbf{1}\}_{K'}, \mathbf{0} \rangle\}_K \rangle \\
\{\mathbf{0}\}_K & \cong & \{K\}_K \\
\{\langle \langle \mathbf{0}, \mathbf{0} \rangle \langle \mathbf{0}, \mathbf{0} \rangle \rangle\}_K & \cong & \{\mathbf{0}\}_K \\
\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle & \cong & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle \\
\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle & & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle
\end{array}
$$

Exemples d'équivalences

Exemple

$$
\begin{array}{rcl}
\mathbf{0} & \cong & \mathbf{0} \\
\mathbf{0} & \not\cong & \mathbf{1} \\
\{\mathbf{0}\}_K & \cong & \{\mathbf{1}\}_K \\
\langle K, \{\mathbf{0}\}_K \rangle & \not\cong & \langle K, \{\mathbf{1}\}_K \rangle \\
\langle K, \{\langle \{\mathbf{0}\}_{K'}, \mathbf{0} \rangle\}_K \rangle & \cong & \langle K, \{\langle \{\mathbf{1}\}_{K'}, \mathbf{0} \rangle\}_K \rangle \\
\{\mathbf{0}\}_K & \cong & \{K\}_K \\
\{\langle\langle \mathbf{0}, \mathbf{0} \rangle \langle \mathbf{0}, \mathbf{0} \rangle\rangle\}_K & \cong & \{\mathbf{0}\}_K \\
\langle \{\mathbf{0}\}_K, \{\mathbf{0}\}_K \rangle & \cong & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle \\
\langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_K \rangle & \cong & \langle \{\mathbf{0}\}_K, \{\mathbf{1}\}_{K'} \rangle
\end{array}
$$

Plan

Spécificités du modèle calculatoire

Rappel : On se concentre ici sur un modèle d'adversaire passif

- pas de description du protocole et de son exécution

Dans ce modèle

- Les données sont des chaînes de bits
- Les primitives cryptographiques sont des algorithmes polynomiaux
- L'adversaire est une machine de Turing polynomiale probabiliste arbitraire
- La sécurité est exprimée en termes de probabilités : *"La probabilité avec laquelle l'adversaire peut obtenir le secret doit être négligeable"*

Définitions préliminaires

Soit String $= \{0,1\}^*$ l'ensemble de toutes les chaînes de bits finies

On distingue dans String les ensembles

- Plaintext : l'ensemble des chaînes de bits représentant les textes clairs possibles ; on distingue un élément particulier noté $\mathbf{0}$
- Ciphertext : l'ensemble des chaînes de bits représentant les chiffrés possibles
- Key : l'ensemble des chaînes de bits représentant les clés possibles

Définitions préliminaires

Soit String $= \{0,1\}^*$ l'ensemble de toutes les chaînes de bits finies

On distingue dans String les ensembles

- Plaintext : l'ensemble des chaînes de bits représentant les textes clairs possibles ; on distingue un élément particulier noté $\mathbf{0}$
- Ciphertext : l'ensemble des chaînes de bits représentant les chiffrés possibles
- Key : l'ensemble des chaînes de bits représentant les clés possibles

On définit également :

- Coins $= \{0,1\}^\omega$: l'ensemble des chaînes de bits infinies, intuitivement la bande d'aléas
- Parameter $= 1^*$: l'ensemble des chaînes de 1 finies, le paramètre de sécurité (en unaire)

Schéma de chiffrement

Un schéma de chiffrement Π est un triplet d'algorithmes $\mathcal{K}, \mathcal{E}, \mathcal{D}$

- algorithme de génération de clés $\mathcal{K}$: Parameter $\times$ Coins $\rightarrow$ Key
- algorithme de chiffrement $\mathcal{E}$: Key $\times$ String $\times$ Coins $\rightarrow$ Ciphertext
- algorithme de déchiffrement $\mathcal{D}$: Key $\times$ String $\rightarrow$ Plaintext

On suppose que ces algorithmes sont calculables en temps polynomial en leur entrée (sans considérer la taille de l'entrée de l'argument dans Coins)

On utilisera la notation $\mathcal{E}_k(m, r)$ et $\mathcal{D}_k(m, r)$ pour $\mathcal{E}(k, m, r)$ et $\mathcal{D}(k, m, r)$

On omettra parfois Coins dans $\mathcal{E}$ et $\mathcal{K}$ pour dénoter la distribution correspondante ou le support de cette distribution (l'ensemble des chaînes de probabilité non nulle)

Pour tout $\eta \in$ Parameter, $k \in \mathcal{K}(\eta)$, $r \in Coins(\eta)$ on demande que

$$\mathcal{D}_k(\mathcal{E}_k(m)) = \begin{cases} m & \text{si } m \in \text{Plaintext} \\ \mathbf{0} & \text{si } m \notin \text{Plaintext} \end{cases}$$

Schéma de chiffrement

Un schéma de chiffrement Π est un triplet d'algorithmes $\mathcal{K}, \mathcal{E}, \mathcal{D}$

- algorithme de génération de clés $\mathcal{K}$: Parameter $\times$ Coins $\rightarrow$ Key
- algorithme de chiffrement $\mathcal{E}$: Key $\times$ String $\times$ Coins $\rightarrow$ Ciphertext
- algorithme de déchiffrement $\mathcal{D}$: Key $\times$ String $\rightarrow$ Plaintext

Intuitivement, le paramètre de sécurité détermine la longueur des clés

Schéma de chiffrement

Un schéma de chiffrement Π est un triplet d'algorithmes $\mathcal{K}, \mathcal{E}, \mathcal{D}$

- algorithme de génération de clés $\mathcal{K}$: Parameter $\times$ Coins $\to$ Key
- algorithme de chiffrement $\mathcal{E}$: Key $\times$ String $\times$ Coins $\to$ Ciphertext
- algorithme de déchiffrement $\mathcal{D}$: Key $\times$ String $\to$ Plaintext

Intuitivement, le paramètre de sécurité détermine la longueur des clés

Le chiffrement est probabiliste

Indistinguabilité calculatoire

Définition (Fonction négligeable)

Une fonction $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$ est négligeable si $\forall n > 0.\ \exists N_n.\ \epsilon(\eta) \leq \eta^{-n}$ pour $\eta \geq N_n$

Soit $D = \{D_\eta\}$ une famille de distributions sur String, une pour chaque $\eta \in$ Parameter.

Indistinguabilité calculatoire

Définition (Fonction négligeable)

Une fonction $\epsilon : \mathbb{N} \to \mathbb{R}$ est négligeable si $\forall n > 0.\ \exists N_n.\ \epsilon(\eta) \leq \eta^{-n}$ pour $\eta \geq N_n$

Soit $D = \{D_\eta\}$ une famille de distributions sur String, une pour chaque $\eta \in$ Parameter.

$x \xleftarrow{R} D$ dénote un tirage aléatoire dans D. $Pr[x \xleftarrow{R} D : E]$ dénote la probabilité de l'événement E sachant que x a été tiré aléatoirement dans D.

Indistinguabilité calculatoire

Définition (Fonction négligeable)

Une fonction $\epsilon : \mathbb{N} \rightarrow \mathbb{R}$ est négligeable si $\forall n > 0.\ \exists N_n.\ \epsilon(\eta) \leq \eta^{-n}$ pour $\eta \geq N_n$

Soit $D = \{D_\eta\}$ une famille de distributions sur String, une pour chaque $\eta \in$ Parameter.

$x \stackrel{R}{\longleftarrow} D$ dénote un tirage aléatoire dans D. $Pr[x \stackrel{R}{\longleftarrow} D : E]$ dénote la probabilité de l'événement E sachant que x a été tiré aléatoirement dans D.

Définition (Indistinguabilité)

Soient $D = \{D_\eta\}$ et $D' = \{D'_\eta\}$ deux familles de distributions. D et D' sont indistinguables, noté $D \approx D'$, si pour tout adversaire polynomial probabiliste $\mathcal{A}$ la fonction

$$Adv^{\mathrm{IND}}(\eta) = Pr[x \stackrel{R}{\longleftarrow} D_\eta : \mathcal{A}(\eta, x) = 1] - Pr[x \stackrel{R}{\longleftarrow} D'_\eta : \mathcal{A}(\eta, x) = 1]$$

est négligeable.

Définition (Sécurité de type-0)

Soient $\Pi = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ un schéma de chiffrement, $\eta \in$ Parameter. On définit l'avantage d'un adversaire $\mathcal{A}$ comme

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

Le schéma de chiffrement Π est sémantiquement sûr si pour tout adversaire probabiliste polynomial $\mathcal{A}$, $Adv_{\Pi,\eta}(\mathcal{A})$ est une fonction négligeable (en η).

$\mathcal{A}^{\mathcal{O}}$ dénote une machine de Turing $\mathcal{A}$ (ici l'adversaire) avec accès à un (ou plusieurs) oracle(s) $\mathcal{O}$ (ici des oracles de chiffrement).

$\mathcal{E}_k(\cdot)$ est un oracle de chiffrement qui prend un argument m et renvoie $c \xleftarrow{R} \mathcal{E}_k(m)$

$\mathcal{E}_k(\mathbf{0})$ est un oracle de chiffrement qui prend un argument m et renvoie $c \xleftarrow{R} \mathcal{E}_k(\mathbf{0})$ (qui est donc indépendant de m)

Les cycles de chiffrement

Remarque

Une propriété étrange des schémas de chiffrement sémantiquement sûrs :

il existe des schémas de chiffrement sémantiquement sûrs qui peuvent être cassés si on donne à l'adversaire un seul chiffrement $c \xleftarrow{R} \mathcal{E}_k(k)$

On appelle $\mathcal{E}_k(k)$ un cycle de chiffrement de taille 1

$(\mathcal{E}_{k_1}(k_2), \mathcal{E}_{k_2}(k_1))$ est un cycle de chiffrement de taille 2 et pose des problèmes dans les preuves de sécurité

Plan

Interdire les cycles de clés

Pour obtenir un résultat de correction il faudra interdire les cycles de chiffrement dans les termes.

Définition (Cycle de chiffrement)

Soient $K, K' \in \mathbf{Keys}$. On dit que K chiffre K' dans un terme M noté $K \succ_M K'$ si $\{N\}_K \in st(M)$ et $K' \in st(N)$.
Un terme M est acyclique ssi la relation $\succ_M$ est acyclique.

Exemples

Interdire les cycles de clés

Pour obtenir un résultat de correction il faudra interdire les cycles de chiffrement dans les termes.

Définition (Cycle de chiffrement)

Soient $K, K' \in \mathbf{Keys}$. On dit que K chiffre K' dans un terme M noté $K \succ_M K'$ si $\{N\}_K \in st(M)$ et $K' \in st(N)$.
Un terme M est acyclique ssi la relation $\succ_M$ est acyclique.

Exemples

- Soit $M = \langle \{\{K_1\}_{K_2}\}_{K_3}, \mathbf{0} \rangle$. $\succ_M$ est défini par $K_3 \succ_M K_2 \succ_M K_1$. M est donc acyclique.

Interdire les cycles de clés

Pour obtenir un résultat de correction il faudra interdire les cycles de chiffrement dans les termes.

Définition (Cycle de chiffrement)

Soient $K, K' \in \mathbf{Keys}$. On dit que K chiffre K' dans un terme M noté $K \succ_M K'$ si $\{N\}_K \in st(M)$ et $K' \in st(N)$.

Un terme M est acyclique ssi la relation $\succ_M$ est acyclique.

Exemples

- Soit $M = \langle \{\{K_1\}_{K_2}\}_{K_3}, \mathbf{0} \rangle$. $\succ_M$ est défini par $K_3 \succ_M K_2 \succ_M K_1$. M est donc acyclique.
- Soit $M = \{K\}_K$. On a que $K \succ_M K$. M contient un cycle de taille 1.

Interdire les cycles de clés

Pour obtenir un résultat de correction il faudra interdire les cycles de chiffrement dans les termes.

Définition (Cycle de chiffrement)

Soient $K, K' \in \mathbf{Keys}$. On dit que K chiffre K' dans un terme M noté $K \succ_M K'$ si $\{N\}_K \in st(M)$ et $K' \in st(N)$.
Un terme M est acyclique ssi la relation $\succ_M$ est acyclique.

Exemples

- Soit $M = \langle \{\{K_1\}_{K_2}\}_{K_3}, \mathbf{0} \rangle$. $\succ_M$ est défini par $K_3 \succ_M K_2 \succ_M K_1$. M est donc acyclique.
- Soit $M = \{K\}_K$. On a que $K \succ_M K$. M contient un cycle de taille 1.
- Soit $M = \langle \{K_1\}_{K_2}, \{K_2\}_{K_1} \rangle$. On a que $K_1 \succ_M K_2$ et $K_2 \succ_M K_1$. M contient un cycle de taille 2.

Implémentation des termes

On donne une implémentation aux termes formels. Soit Π un schéma de chiffrement et $\eta \in$ Parameter. On associe au terme M une distribution $[\![M]\!]_{\Pi,\eta}$ et donc une famille de distributions $[\![M]\!]_{\Pi}$.

Initialize$_\eta(M)$
  for $K \in Keys(M)$ do $\tau(K) \stackrel{R}{\longleftarrow} \mathcal{K}(\eta)$

Convert(M)
  if $M = K$ ($K \in$ **Keys**) then return $(\tau(K)$, "key")
  if $M = b$ ($b \in$ **Bool**) then return (b,"bool")
  if $M = \langle M_1, M_2 \rangle$ then return (Convert(M_1), Convert(M_2), "pair")
  if $M = \{M_1\}_K$ then
    $x \stackrel{R}{\longleftarrow}$ Convert(M_1); $y \stackrel{R}{\longleftarrow} \mathcal{E}_{\tau(K)}(x)$; return($y$, "ciphertext")

Implémentation des termes

On donne une implémentation aux termes formels. Soit Π un schéma de chiffrement et $\eta \in \text{Parameter}$. On associe au terme M une distribution $[\![M]\!]_{\Pi,\eta}$ et donc une famille de distributions $[\![M]\!]_{\Pi}$.

$$
\begin{array}{l}
\text{Initialize}_\eta(M) \\
\quad \text{for } K \in \mathit{Keys}(M) \text{ do } \tau(K) \stackrel{R}{\longleftarrow} \mathcal{K}(\eta) \\
\text{Convert}(M) \\
\quad \text{if } M = K \ (K \in \mathbf{Keys}) \text{ then return } (\tau(K), \text{“key”}) \\
\quad \text{if } M = b \ (b \in \mathbf{Bool}) \text{ then return } (b, \text{“bool”}) \\
\quad \text{if } M = \langle M_1, M_2 \rangle \text{ then return } (\text{Convert}(M_1), \text{Convert}(M_2), \text{“pair”}) \\
\quad \text{if } M = \{M_1\}_K \text{ then} \\
\qquad x \stackrel{R}{\longleftarrow} \text{Convert}(M_1); \quad y \stackrel{R}{\longleftarrow} \mathcal{E}_{\tau(K)}(x); \quad \text{return}(y, \text{“ciphertext”})
\end{array}
$$

- on génère toutes les clés de M (noté $\mathit{Keys}(M)$) en appelant $\mathcal{K}$ et on les sauve dans un tableau τ

Implémentation des termes

On donne une implémentation aux termes formels. Soit Π un schéma de chiffrement et $\eta \in$ Parameter. On associe au terme M une distribution $[\![M]\!]_{\Pi,\eta}$ et donc une famille de distributions $[\![M]\!]_{\Pi}$.

Initialize$_\eta(M)$
  for $K \in Keys(M)$ do $\tau(K) \stackrel{R}{\longleftarrow} \mathcal{K}(\eta)$

Convert(M)
  if $M = K$ $(K \in \mathbf{Keys})$ then return $(\tau(K)$, "key")
  if $M = b$ $(b \in \mathbf{Bool})$ then return $(b$,"bool")
  if $M = \langle M_1, M_2 \rangle$ then return (Convert(M_1), Convert(M_2), "pair")
  if $M = \{M_1\}_K$ then
    $x \stackrel{R}{\longleftarrow}$ Convert(M_1); $y \stackrel{R}{\longleftarrow} \mathcal{E}_{\tau(K)}(x)$; return$(y$, "ciphertext")

- on génère toutes les clés de M (noté $Keys(M)$) en appelant $\mathcal{K}$ et on les sauve dans un tableau τ
- on suppose qu'il existe une implantation des constantes **0** et **1**

Implémentation des termes

On donne une implémentation aux termes formels. Soit Π un schéma de chiffrement et $\eta \in$ Parameter. On associe au terme M une distribution $[\![M]\!]_{\Pi,\eta}$ et donc une famille de distributions $[\![M]\!]_{\Pi}$.

$$
\begin{array}{l}
\mathsf{Initialize}_{\eta}(M) \\
\quad \text{for } K \in Keys(M) \text{ do } \tau(K) \xleftarrow{R} \mathcal{K}(\eta) \\
\mathsf{Convert}(M) \\
\quad \text{if } M = K \ (K \in \mathbf{Keys}) \text{ then return } (\tau(K), \text{“key”}) \\
\quad \text{if } M = b \ (b \in \mathbf{Bool}) \text{ then return } (b, \text{“bool”}) \\
\quad \text{if } M = \langle M_1, M_2 \rangle \text{ then return } (\mathsf{Convert}(M_1), \mathsf{Convert}(M_2), \text{“pair”}) \\
\quad \text{if } M = \{M_1\}_K \text{ then} \\
\qquad x \xleftarrow{R} \mathsf{Convert}(M_1); \quad y \xleftarrow{R} \mathcal{E}_{\tau(K)}(x); \quad \text{return}(y, \text{“ciphertext”})
\end{array}
$$

- on génère toutes les clés de M (noté $Keys(M)$) en appelant $\mathcal{K}$ et on les sauve dans un tableau τ
- on suppose qu'il existe une implantation des constantes **0** et **1**
- pour éviter des ambiguités on utilise des tags

Équivalence formelle implique l'indistinguabilité

Théorème (Correction calculatoire de l'équivalence formelle)

Soit M et N deux termes acycliques et Π un schéma de chiffrement de type-0. Si $M \cong N$ alors $[\![M]\!] \approx [\![N]\!]$.

Ce théorème permet d'utiliser des techniques formelles automatisables pour obtenir des garanties de sécurité dans le modèle calculatoire.

Preuve : renommage

La première étape de la preuve consiste à renommer les clés.

Soit $Keys(M)$ l'ensemble des clés dans M.

$$\begin{array}{rcl} recoverable(M) & = & \{K \in Keys(M) \mid M \vdash K\} \\ hidden(M) & = & Keys(M) \setminus recoverable(M) \end{array}$$

Soit $\mu = \mid recoverable(M) \mid$ et $m = \mid hidden(M) \mid$.

On renomme les clés dans $recoverable(M)$ vers $J_1, \ldots, J_\mu$.

Comme M est acyclique on peut renommer les clés dans $hidden(M)$ vers $K_1, \ldots, K_m$ tel que $K_i \succ_M K_j$ implique $i > j$.

Une clé "plus profonde" a un indice plus petit

Exemple

Soit le terme M (on omet les paires pour la lisibilité)

$$\{0\}_{K_6}\ \{K_1 1\}_{K_4}\ K_2\ \{0\}_{K_3}\ \{K_6\}_{K_4}\ \{K_1 K_3\}_{K_4}\ \{111\}_{K_5}\ 0\ \{K_1\}_{K_6}\ \{K_5\}_{K_2}$$

$$\begin{aligned} \mathit{Keys}(M) &= \\ \mathit{recoverable}(M) &= \\ \mathit{hidden}(M) &= \end{aligned}$$

Preuve : renommage

Exemple

Soit le terme M (on omet les paires pour la lisibilité)

$$\{0\}_{K_6}\ \{K_1 1\}_{K_4}\ K_2\ \{0\}_{K_3}\ \{K_6\}_{K_4}\ \{K_1 K_3\}_{K_4}\ \{111\}_{K_5}\ 0\ \{K_1\}_{K_6}\ \{K_5\}_{K_2}$$

$$\begin{array}{rcl} Keys(M) & = & \{K_1, K_2, K_3, K_4, K_5, K_6\} \\ recoverable(M) & = & \{K_2, K_5\} \\ hidden(M) & = & \{K_1, K_3, K_4, K_6\} \end{array}$$

La relation $\succ_M$ (restreint à $hidden(M)$) est défini par

Preuve : renommage

Exemple

Soit le terme M (on omet les paires pour la lisibilité)

$$\{0\}_{K_6}\ \{K_1 1\}_{K_4}\ K_2\ \{0\}_{K_3}\ \{K_6\}_{K_4}\ \{K_1 K_3\}_{K_4}\ \{111\}_{K_5}\ 0\ \{K_1\}_{K_6}\ \{K_5\}_{K_2}$$

$$\begin{array}{rcl} Keys(M) & = & \{K_1, K_2, K_3, K_4, K_5, K_6\} \\ recoverable(M) & = & \{K_2, K_5\} \\ hidden(M) & = & \{K_1, K_3, K_4, K_6\} \end{array}$$

La relation $\succ_M$ (restreint à $hidden(M)$) est défini par
$K_4 \succ_M K_1 \quad K_4 \succ_M K_3 \quad K_4 \succ_M K_6 \quad K_6 \succ_M K_1$

On peut renommer

Preuve : renommage

Exemple

Soit le terme M (on omet les paires pour la lisibilité)

$$\{0\}_{K_6}\ \{K_1 1\}_{K_4}\ K_2\ \{0\}_{K_3}\ \{K_6\}_{K_4}\ \{K_1 K_3\}_{K_4}\ \{111\}_{K_5}\ 0\ \{K_1\}_{K_6}\ \{K_5\}_{K_2}$$

$$\begin{array}{rcl} Keys(M) & = & \{K_1, K_2, K_3, K_4, K_5, K_6\} \\ recoverable(M) & = & \{K_2, K_5\} \\ hidden(M) & = & \{K_1, K_3, K_4, K_6\} \end{array}$$

La relation $\succ_M$ (restreint à $hidden(M)$) est défini par
$K_4 \succ_M K_1 \quad K_4 \succ_M K_3 \quad K_4 \succ_M K_6 \quad K_6 \succ_M K_1$

On peut renommer $\{K_1 \to K_1, K_2 \to J_1, K_3 \to K_2, K_4 \to K_4, K_5 \to J_2, K_6 \to K_3\}$ et obtenir M'

$$\{0\}_{K_3}\ \{K_1 1\}_{K_4}\ J_1\ \{0\}_{K_2}\ \{K_3\}_{K_4}\ \{K_1 K_2\}_{K_4}\ \{111\}_{J_2}\ 0\ \{K_1\}_{K_3}\ \{J_2\}_{J_1}$$

Preuve : renommage

Comme $M \cong N$ on a que $pat(M) = pat(N\sigma)$ et donc $recoverable(M) = recoverable(N\sigma)$.

Par acyclicité de N on renomme les clés de $hidden(N)$ vers $\{K_1, \ldots K_n\}$ où $n = \mid hidden(N) \mid$.

On peut donc construire un renommage σ' tel que $N' = N\sigma'$, $M' \equiv N'$, $recoverable(M') = recoverable(N') = \{J_1, \ldots, J_\mu\}$, $hidden(N') = \{K_1, \ldots K_n\}$ et $K_i \succ_N K_j$ implique $i > j$.

Exemple

Soit le terme N

$$\{11\}_{K_2}\ \{K_3\}_{K_2}\ K_1\ \{K_3\}_{K_2}\ \{K_8\}_{K_2}\ \{1\}_{K_5}\ \{111\}_{K_3}\ 0\ \{00\}_{K_8}\ \{K_3\}_{K_1}$$

Preuve : renommage

Comme $M \cong N$ on a que $pat(M) = pat(N\sigma)$ et donc $recoverable(M) = recoverable(N\sigma)$.

Par acyclicité de N on renomme les clés de $hidden(N)$ vers $\{K_1, \ldots K_n\}$ où $n =\mid hidden(N) \mid$.

On peut donc construire un renommage σ' tel que $N' = N\sigma'$, $M' \equiv N'$, $recoverable(M') = recoverable(N') = \{J_1, \ldots, J_\mu\}$, $hidden(N') = \{K_1, \ldots K_n\}$ et $K_i \succ_N K_j$ implique $i > j$.

Exemple

Soit le terme N

$$\{11\}_{K_2}\ \{K_3\}_{K_2}\ K_1\ \{K_3\}_{K_2}\ \{K_8\}_{K_2}\ \{1\}_{K_5}\ \{111\}_{K_3}\ 0\ \{00\}_{K_8}\ \{K_3\}_{K_1}$$

On a que $recoverable(M) = \{K_1, K_3\},\ hidden(M) = \{K_2, K_5, K_8\}$. On renomme $\{K_1 \rightarrow J_1, K_2 \rightarrow K_3, K_3 \rightarrow J_2, K_5 \rightarrow K_1, K_8 \rightarrow K_2\}$ et obtient N'

$$\{11\}_{K_3}\ \{J_2\}_{K_3}\ J_1\ \{J_2\}_{K_3}\ \{K_2\}_{K_3}\ \{1\}_{K_1}\ \{111\}_{J_2}\ 0\ \{00\}_{K_2}\ \{J_2\}_{J_1}$$

Preuve : patterns hybrides

Dans cette phase de la preuve on introduit des patterns afin de former une chaîne

$$M' = M_m, \ldots, M_1, M_0 = N_0, N_1, \ldots, N_n = N'$$

où

$$M_i = p(M', recoverable(M') \cup \{K_1, \ldots, K_i\}) \qquad 0 \leq i \leq m$$

et

$$N_i = p(N', recoverable(N') \cup \{K_1, \ldots, K_i\}) \qquad 0 \leq i \leq n$$

Intuitivement M_i respectivement N_i est la vue de l'adversaire s'il connaissait les clés cachées $\{K_1, \ldots, K_i\}$

On a en effet que $M_0 = pattern(M') = pattern(N') = N_0$ car $M' \equiv N'$.

Preuve : patterns hybrides (exemple)

Exemple

$$
\begin{array}{llllllllllll}
M' \\
= \\
M_4: & \{0\}_{K_3} & \{K_1 1\}_{K_4} & J_1 & \{0\}_{K_2} & \{K_3\}_{K_4} & \{K_1 K_2\}_{K_4} & \{111\}_{J_2} & 0 & \{K_1\}_{K_3} & \{J_2\}_{J_1} \\
M_3: & \{0\}_{K_3} & \Box & J_1 & \{0\}_{K_2} & \Box & \Box & \{111\}_{J_2} & 0 & \{K_1\}_{K_3} & \{J_2\}_{J_1} \\
M_2: & \Box & \Box & J_1 & \{0\}_{K_2} & \Box & \Box & \{111\}_{J_2} & 0 & \Box & \{J_2\}_{J_1} \\
M_1: & \Box & \Box & J_1 & \Box & \Box & \Box & \{111\}_{J_2} & 0 & \Box & \{J_2\}_{J_1} \\
M_0: & \Box & \Box & J_1 & \Box & \Box & \Box & \{111\}_{J_2} & 0 & \Box & \{J_2\}_{J_1} \\
=
\end{array}
$$

Preuve : patterns hybrides (exemple)

Exemple

$$
\begin{array}{lcccccccccc}
M' \\
= \\
M_4 : & \{0\}_{K_3} & \{K_1 1\}_{K_4} & J_1 & \{0\}_{K_2} & \{K_3\}_{K_4} & \{K_1 K_2\}_{K_4} & \{111\}_{J_2} & 0 & \{K_1\}_{K_3} & \{J_2\}_{J_1} \\
M_3 : & \{0\}_{K_3} & \square & J_1 & \{0\}_{K_2} & \square & \square & \{111\}_{J_2} & 0 & \{K_1\}_{K_3} & \{J_2\}_{J_1} \\
M_2 : & \square & \square & J_1 & \{0\}_{K_2} & \square & \square & \{111\}_{J_2} & 0 & \square & \{J_2\}_{J_1} \\
M_1 : & \square & \square & J_1 & \square & \square & \square & \{111\}_{J_2} & 0 & \square & \{J_2\}_{J_1} \\
M_0 : & \square & \square & J_1 & \square & \square & \square & \{111\}_{J_2} & 0 & \square & \{J_2\}_{J_1} \\
= \\
N_0 : & \square & \square & J_1 & \square & \square & \square & \{111\}_{J_2} & 0 & \square & \{J_2\}_{J_1} \\
N_1 : & \square & \square & J_1 & \square & \square & \{1\}_{K_1} & \{111\}_{J_2} & 0 & \square & \{J_2\}_{J_1} \\
N_2 : & \square & \square & J_1 & \square & \square & \{1\}_{K_1} & \{111\}_{J_2} & 0 & \{00\}_{K_2} & \{J_2\}_{J_1} \\
N_3 : & \{11\}_{K_3} & \{J_2\}_{K_3} & J_1 & \{J_2\}_{K_3} & \{K_2\}_{K_3} & \{1\}_{K_1} & \{111\}_{J_2} & 0 & \{00\}_{K_2} & \{J_2\}_{J_1} \\
= \\
N'
\end{array}
$$

Preuve : associer des distributions aux patterns

Comme pour les termes on associera une famille de distributions à chaque pattern

Idée : le symbole $\Box$ est implanté par un chiffrement de $\mathbf{0}$ avec une clé fraîche

On rajoute dans **Initialize**$_\eta(M)$ la ligne

$$\tau(K_0) \xleftarrow{R} \mathcal{K}(\eta)$$

et dans **Convert**(M) la ligne

$$\begin{array}{l} \text{if } M = \Box \text{ then} \\ \quad y \xleftarrow{R} \mathcal{E}_{\tau(K_0)}(\mathbf{0}) \\ \quad \text{return}(y, \text{“ciphertext”}) \end{array}$$

Preuve : par contradiction

On a que

$$[\![M]\!]_\Pi = [\![M']\!]_\Pi \qquad [\![N]\!]_\Pi = [\![N']\!]_\Pi$$

car M et M' (resp. N et N') ne diffèrent que par un renommage des clés

Notre but est donc de montrer que $[\![M']\!]_\Pi \approx [\![N']\!]_\Pi$

Par contradiction, nous supposons qu'il existe un adversaire PPT $\mathcal{A}$ qui distingue $[\![M']\!]_\Pi$ et $[\![N']\!]_\Pi$

$$\lambda(\eta) = Pr[y \xleftarrow{R} [\![M']\!]_\Pi : \ \mathcal{A}(\eta, y) = 1] - Pr[y \xleftarrow{R} [\![N']\!]_\Pi : \ \mathcal{A}(\eta, y) = 1]$$

n'est pas négligeable

Preuve : par contradiction

On a que

$$[\![M]\!]_\Pi = [\![M']\!]_\Pi \qquad [\![N]\!]_\Pi = [\![N']\!]_\Pi$$

car M et M' (resp. N et N') ne diffèrent que par un renommage des clés

Notre but est donc de montrer que $[\![M']\!]_\Pi \approx [\![N']\!]_\Pi$

Par contradiction, nous supposons qu'il existe un adversaire PPT $\mathcal{A}$ qui distingue $[\![M']\!]_\Pi$ et $[\![N']\!]_\Pi$

$$\lambda(\eta) = Pr[y \xleftarrow{R} [\![M']\!]_\Pi :\ \mathcal{A}(\eta, y) = 1] - Pr[y \xleftarrow{R} [\![N']\!]_\Pi :\ \mathcal{A}(\eta, y) = 1]$$

n'est pas négligeable

Il exsite i tel que :

$$\lambda(\eta) = Pr[y \xleftarrow{R} [\![M_i]\!]_\Pi :\ \mathcal{A}(\eta, y) = 1] - Pr[y \xleftarrow{R} [\![M_{i-1}]\!]_\Pi :\ \mathcal{A}(\eta, y) = 1]$$

n'est pas négligeable (ou sur N_i)

Un adversaire contre le schéma de chiffrement

À partir de l'adversaire $\mathcal{A}$ on définit un adversaire $\mathcal{A}_0$ qui essaie de casser le schéma de chiffrement

algorithm $\mathcal{A}_0^{f,g}$
  for $K \in Keys(M')$ do $\tau(K) \xleftarrow{R} \mathcal{K}(\eta)$
  $y \xleftarrow{R}$ **Convert2**(M')
  $b \xleftarrow{R} \mathcal{A}(\eta, y)$

Convert2(M^*)
  if $M^* = K$ ($K \in$ **Keys**) then return $(\tau(K)$, "key")
  if $M^* = b$ ($b \in$ **Bool**) then return (b,"bool")
  if $M^* = \langle M_1^*, M_2^* \rangle$ then return (Convert(M_1^*), Convert2(M_2^*), "pair")
  if $M^* = \{M_1^*\}_K$ then
    if $K \in \{J_1, \ldots, J_\mu, K_1, \ldots, K_{i-1}\}$ then
      $x \xleftarrow{R}$ Convert2(M_1^*); $y \xleftarrow{R} \mathcal{E}_{\tau(K)}(x)$; return($y$, "ciphertext")
    if $K = K_i$ then
      $x \xleftarrow{R}$ Convert2(M_1^*); $y \xleftarrow{R} f(x)$; return(y, "ciphertext")
    if $K \in \{K_{i+1}, \ldots, K_m\}$ then
      $y \xleftarrow{R} g(\mathbf{0})$; return($y$, "ciphertext")

Un adversaire contre le schéma de chiffrement

Par construction on a que

$$\begin{array}{rcl} Pr[y \xleftarrow{R} [\![M_i]\!]_\Pi : \ \mathcal{A}(\eta, y) = 1] & = & Pr[k_i, k_0 \xleftarrow{\mathcal{K}} (\eta) : \mathcal{A}_0^{\mathcal{E}_{\boldsymbol{\kappa_i}}(\cdot), \mathcal{E}_{\boldsymbol{\kappa_0}}(\cdot)}(\eta) = 1] \\ Pr[y \xleftarrow{R} [\![M_{i-1}]\!]_\Pi : \ \mathcal{A}(\eta, y) = 1] & = & Pr[k_0 \xleftarrow{\mathcal{K}} (\eta) : \mathcal{A}_0^{\mathcal{E}_{\boldsymbol{\kappa_0}}(\mathbf{0}), \mathcal{E}_{\boldsymbol{\kappa_0}}(\mathbf{0})}(\eta) = 1] \end{array}$$

Un adversaire contre le schéma de chiffrement

Par construction on a que

$$\begin{array}{rcl} Pr[y \xleftarrow{R} [\![M_i]\!]_\Pi : \mathcal{A}(\eta, y) = 1] & = & Pr[k_i, k_0 \xleftarrow{\mathcal{K}} (\eta) : \mathcal{A}_0^{\mathcal{E}_{\mathbf{K_i}}(\cdot), \mathcal{E}_{\mathbf{K_0}}(\cdot)}(\eta) = 1] \\ Pr[y \xleftarrow{R} [\![M_{i-1}]\!]_\Pi : \mathcal{A}(\eta, y) = 1] & = & Pr[k_0 \xleftarrow{\mathcal{K}} (\eta) : \mathcal{A}_0^{\mathcal{E}_{\mathbf{K_o}}(\mathbf{0}), \mathcal{E}_{\mathbf{K_0}}(\mathbf{0})}(\eta) = 1] \end{array}$$

On a donc que :

$Adv_{\Pi,\eta}$ n'est donc pas une fonction négligeable ce qui contredit l'hypothèse de sécurité sémantique et conclut la preuve.