Lois déjà présentes dans la thèse et/ou l'article

Lois locales

$$\pi_{\delta_1} \circ \cdots \circ \pi_{\delta_n} \equiv \pi_{\delta_1 \cap \cdots \cap \delta_n} \tag{1}$$

$$\sigma_{p_1} \circ \cdots \circ \sigma_{p_n} \equiv \sigma_{p_1 \wedge \cdots \wedge p_n} \tag{2}$$

$$\pi_\delta \circ \sigma_p \equiv \sigma_p \circ \pi_\delta \qquad \text{si } \mathrm{dom}(p) \subset \delta \tag{3}$$

Lois identité

$$\mathrm{id} \equiv \mathrm{defrag} \circ \mathrm{frag}_\delta \tag{4}$$

$$\mathrm{id} \equiv \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \mathrm{crypt}_{\alpha,\mathtt{c}} \tag{5}$$

Lois de projection

$$\pi_\delta \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} \equiv \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \pi_\delta \qquad \text{si } \alpha \in \delta \tag{6}$$

$$\pi_\delta \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} \equiv \pi_\delta \qquad \text{si } \alpha \notin \delta \tag{7}$$

$$\pi_\delta \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\pi_{\delta \cap \delta'}, \pi_{\delta \setminus \delta'}) \quad \text{où } \delta' \text{ est le schéma relationnel du premier fragment} \tag{8}$$

Lois de sélection

Lorsqu'une défragmentation est effectuée, on supposera que le schéma relationnel du fragment de gauche s'appelle δ' .

$$\sigma_p \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} \equiv \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \sigma_p \qquad \text{si } \mathrm{dom}(p) \cap \alpha = \emptyset \tag{9}$$

$$\sigma_p \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} \equiv \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \sigma_{\mathtt{c} \Rightarrow p} \qquad \text{si } p \text{ est compatible avec } \mathtt{c} \tag{10}$$

$$\sigma_p \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\sigma_p, \mathrm{id}) \qquad \text{si } dom(p) \subset \delta' \tag{11}$$

$$\sigma_p \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{id}, \sigma_p) \qquad \text{si } dom(p) \subset \Delta \setminus \delta' \tag{12}$$

Lois d'agrégation

Pour tout chiffrement `c`, on appellera `c'` le chiffrement qui agit sur une liste en appliquant `c` à chacun des éléments de la liste. Lorsqu'une défragmentation est effectuée, on supposera que le schéma relationnel du fragment de gauche s'appelle δ' .

$$\mathrm{group}_\delta \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} \equiv \mathrm{decrypt}_{\alpha,\mathtt{c'}} \circ \mathrm{group}_\delta \qquad \text{Si } \alpha \notin \delta \tag{13}$$

$$\mathrm{group}_\delta \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} \equiv \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \mathrm{group}_\delta \qquad \text{Si } \mathtt{c} \text{ est compatible avec l'égalité} \tag{14}$$

$$\mathrm{group}_\delta \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{group}_\delta, \mathrm{group}_{\{\mathrm{id}\}}) \qquad \text{Si } \delta \subset \delta' \tag{15}$$

$$\mathrm{group}_\delta \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{group}_{\{\mathrm{id}\}}, \mathrm{group}_\delta) \qquad \text{Si } \delta \cap \delta' = \emptyset \tag{16}$$

Lois de composition des protections

Lorsqu'une défragmentation est effectuée, on supposera que le schéma relationnel du fragment de gauche s'appelle δ' .

$$\mathrm{id} \circ \mathrm{f} \equiv \mathrm{f} \circ \mathrm{id} \equiv \mathrm{f} \tag{17}$$
$$\mathrm{frag}_\delta \circ \mathrm{decrypt}_{\alpha,\mathsf{c}} \equiv (\mathrm{decrypt}_{\alpha,\mathsf{c}}, \mathrm{id}) \circ \mathrm{frag}_\delta \qquad \text{si } \alpha \in \delta' \tag{18}$$
$$\mathrm{frag}_\delta \circ \mathrm{decrypt}_{\alpha,\mathsf{c}} \equiv (\mathrm{id}, \mathrm{decrypt}_{\alpha,\mathsf{c}}) \circ \mathrm{frag}_\delta \qquad \text{si } \alpha \notin \delta' \tag{19}$$
$$\mathrm{decrypt}_{\alpha,\mathsf{c}} \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{decrypt}_{\alpha,\mathsf{c}}, \mathrm{id}) \qquad \text{si } \alpha \in \delta' \tag{20}$$
$$\mathrm{decrypt}_{\alpha,\mathsf{c}} \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{id}, \mathrm{decrypt}_{\alpha,\mathsf{c}}) \qquad \text{si } \alpha \notin \delta' \tag{21}$$
$$\mathrm{frag}_\delta \circ \mathrm{crypt}_{\alpha,\mathsf{c}} \equiv (\mathrm{crypt}_{\alpha,\mathsf{c}}, \mathrm{id}) \circ \mathrm{frag}_\delta \qquad \text{si } \alpha \in \delta' \tag{22}$$
$$\mathrm{frag}_\delta \circ \mathrm{crypt}_{\alpha,\mathsf{c}} \equiv (\mathrm{id}, \mathrm{crypt}_{\alpha,\mathsf{c}}) \circ \mathrm{frag}_\delta \qquad \text{si } \alpha \notin \delta' \tag{23}$$

Lois que je propose de rajouter

Lois avec fold

A FAIRE

Commutation de defrag et crypt

Lorsqu'une défragmentation est effectuée, on supposera que le schéma relationnel du fragment de gauche s'appelle δ' .

$$\mathrm{crypt}_{\alpha,\mathsf{c}} \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{crypt}_{\alpha,\mathsf{c}}, \mathrm{id}) \qquad \text{si } \alpha \in \delta' \tag{24}$$
$$\mathrm{crypt}_{\alpha,\mathsf{c}} \circ \mathrm{defrag} \equiv \mathrm{defrag} \circ (\mathrm{id}, \mathrm{crypt}_{\alpha,\mathsf{c}}) \qquad \text{si } \alpha \notin \delta' \tag{25}$$