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

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

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

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

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' .

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

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

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

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

Lois de composition des protections

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

$$\text{id} \circ \text{f} \equiv \text{f} \circ \text{id} \equiv \text{f} \tag{17}$$

$$\text{frag}_\delta \circ \text{decrypt}_{\alpha,\mathtt{c}} \equiv (\text{decrypt}_{\alpha,\mathtt{c}}, \text{id}) \circ \text{frag}_\delta \qquad \text{si } \alpha \in \delta' \tag{18}$$

$$\text{frag}_\delta \circ \text{decrypt}_{\alpha,\mathtt{c}} \equiv (\text{id}, \text{decrypt}_{\alpha,\mathtt{c}}) \circ \text{frag}_\delta \qquad \text{si } \alpha \notin \delta' \tag{19}$$

$$\text{decrypt}_{\alpha,\mathtt{c}} \circ \text{defrag} \equiv \text{defrag} \circ (\text{decrypt}_{\alpha,\mathtt{c}}, \text{id}) \qquad \text{si } \alpha \in \delta' \tag{20}$$

$$\text{decrypt}_{\alpha,\mathtt{c}} \circ \text{defrag} \equiv \text{defrag} \circ (\text{id}, \text{decrypt}_{\alpha,\mathtt{c}}) \qquad \text{si } \alpha \notin \delta' \tag{21}$$

$$\text{frag}_\delta \circ \text{crypt}_{\alpha,\mathtt{c}} \equiv (\text{crypt}_{\alpha,\mathtt{c}}, \text{id}) \circ \text{frag}_\delta \qquad \text{si } \alpha \in \delta' \tag{22}$$

$$\text{frag}_\delta \circ \text{crypt}_{\alpha,\mathtt{c}} \equiv (\text{id}, \text{crypt}_{\alpha,\mathtt{c}}) \circ \text{frag}_\delta \qquad \text{si } \alpha \notin \delta' \tag{23}$$

Lois que je propose de rajouter

Commutation de defrag et crypt

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

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

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

Lois évidentes

$$\text{crypt}_{\alpha,\mathtt{c}} \circ \text{crypt}_{\beta,\mathtt{s}} \equiv \text{crypt}_{\beta,\mathtt{s}} \circ \text{crypt}_{\alpha,\mathtt{c}} \qquad \text{si } \alpha \neq \beta \tag{26}$$

A priori, chiffrer une donnée déjà chiffrée semble une mauvaise idée de tous points de vue.

$$\text{decrypt}_{\alpha,\mathtt{c}} \circ \text{decrypt}_{\beta,\mathtt{s}} \equiv \text{decrypt}_{\beta,\mathtt{s}} \circ \text{decrypt}_{\alpha,\mathtt{c}} \qquad \text{si } \alpha \neq \beta \tag{27}$$

A priori, déchiffrer une donnée déjà déchiffrée semble une mauvaise idée de tous points de vue.

Lois d'agrégation

$$\mathrm{group}_\delta \circ \pi_{\delta'} \equiv \pi_{\delta'} \circ \mathrm{group}_\delta \qquad \text{si } \delta \subset \delta' \tag{28}$$

$$\mathrm{group}_\delta \circ \sigma_p \equiv \sigma_p \circ \mathrm{group}_\delta \qquad \text{si } \mathrm{dom}(p) \subset \delta \tag{29}$$

$$\text{group ne commute pas avec lui-même} \tag{30}$$

Lois de jonction

Lorsque les compositions de fonctions considérées à continuations prennent plusieurs arguments, on appelle, de gauche à droite, $\delta_1, \delta_2, \delta_3, \ldots$ leurs schémas relationnels respectifs.

Pour join et defrag

$$\bowtie \circ(\mathrm{defrag}, \mathrm{id}) \equiv \mathrm{defrag} \circ(\mathrm{id}, \bowtie) \qquad \text{si } \delta_1 \cap (\delta_2 \cup \delta_3) = \emptyset \tag{31}$$

Pour join et decrypt

$$\mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \bowtie \equiv \bowtie \circ(\mathrm{decrypt}_{\alpha,\mathtt{c}}, \mathrm{id}) \qquad \text{si } \alpha \in \delta_1 \tag{32}$$

$$\mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \bowtie \equiv \bowtie \circ(\mathrm{id}, \mathrm{decrypt}_{\alpha,\mathtt{c}}) \qquad \text{si } \alpha \in \delta_2 \tag{33}$$

Pour join et join on a envie d'écrire

$$\bowtie \circ(\bowtie, \mathrm{id}) \equiv \bowtie \circ(\mathrm{id}, \bowtie) \tag{34}$$

La correction de cette formule est à vérifier.

Join et group

$$\mathrm{group}_\delta \circ \bowtie \equiv \bowtie \circ(\mathrm{group}_\delta, \mathrm{group}_\delta) \qquad \text{si } \delta = \delta_1 \cap \delta_2 \tag{35}$$

Lois du fold

$$\mathrm{fold}_{\alpha,f,z} \circ \pi_\delta \equiv \pi_\delta \circ \mathrm{fold}_{\alpha,f,z} \qquad \text{si } \alpha \in \delta \tag{36}$$

$$\mathrm{fold}_{\alpha,f,z} \circ \pi_\delta \equiv \pi_\delta \qquad \text{si } \alpha \notin \delta \tag{37}$$

$$\pi_\delta \circ \mathrm{fold}_{\alpha,f,z} \equiv \pi_\delta \qquad \text{si } \alpha \notin \delta \tag{38}$$

$$\sigma_p \circ \mathrm{fold}_{\alpha,f,z} = \mathrm{fold}_{\alpha,f,z} \circ \sigma_p \qquad \text{si } \alpha \notin \mathrm{dom}(p) \tag{39}$$

On appelle δ' le schéma relationnel du premier argument.

$$\mathrm{fold}_{\alpha,f,z} \circ \mathrm{defrag} = \mathrm{defrag} \circ(\mathrm{fold}_{\alpha,f,z}, \mathrm{id}) \qquad \text{si } \alpha \in \delta' \tag{40}$$

$$\mathrm{fold}_{\alpha,f,z} \circ \mathrm{defrag} = \mathrm{defrag} \circ(\mathrm{id}, \mathrm{fold}_{\alpha,f,z}) \qquad \text{si } \alpha \notin \delta' \tag{41}$$

$$\mathrm{fold}_{\alpha,f,z} \circ \mathrm{decrypt}_{\beta,\mathtt{c}} = \mathrm{decrypt}_{\beta,\mathtt{c}} \circ \mathrm{fold}_{\alpha,f,z} \qquad \text{si } \alpha \neq \beta \tag{42}$$

$$\mathrm{fold}_{\alpha,f,z} \circ \mathrm{decrypt}_{\alpha,\mathtt{c}} = \mathrm{decrypt}_{\alpha,\mathtt{c}} \circ \mathrm{fold}_{\alpha,\mathtt{c}\Rightarrow f,\mathtt{c}\Rightarrow z} \qquad \text{si } \mathtt{c} \text{ est compatible avec } f \tag{43}$$