J'ai trouvé deux erreurs dans les lois algébriques énoncées jusqu'à maintenant pour C2QL.
La première est probablement une erreur d'étourderie au moment d'écrire la loi.
La deuxième, par contre, est une erreur dans la condition d'application de la loi.

Loi (3), page 30 de la thèse

Ce qui est écrit dans la thèse

$$\pi_{a_1} \circ \cdots \circ \pi_{a_n} \equiv \pi_{a_1,\ldots,a_n}$$

Contre-exemple

Si on considère la relation r suivante

a_1	a_2
a	1
b	2

son image par π_{a_2} est

a_2
1
2

dont l'image par π_{a_1} est la table vide

Ainsi, l'image de r par $\pi_{a_1} \circ \pi_{a_2}$ est la table vide.

Par contre, l'image de r par π_{a_1,a_2} est la table r elle-même, qui est différente de la table vide.

Correction

La composition des projections correspond à la projection sur *l'intersection*, et non pas à une projection sur l'union.

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

Lois (14) et (15) de l'article A Language for the Composition of Privacy-Enforcement Techniques

Ce qui est écrit dans l'article

$$\sigma_p \circ decrypt_{\mathsf{s},a} \equiv decrypt_{\mathsf{s},a} \circ \sigma_p \quad \text{if } dom(p) \notin \mathscr{P}(a) \quad (14)$$
$$\sigma_p \circ decrypt_{\mathsf{s},a} \equiv decrypt_{\mathsf{s},a} \circ \sigma_{\mathsf{s}_p} \quad \text{if } dom(p) \in \mathscr{P}(a) \quad (15)$$

Contre-exemple

Le chiffrement pris pour l'exemple est artificiel, pour privilégier la simplicité de l'exemple.

On prend pour prédicat p

$$p : a_1 + a_2 < 10$$

pour fonction de chiffrement s

$$s : n \mapsto n + 50$$

et pour ensemble des attributs chiffrés a

$$a = a_1$$

Le domaine de p est alors $\{a_1, a_2\}$ qui n'est pas une partie de a. On est donc dans les hypothèses mentionnées dans l'article pour la loi (14)

On s'intéresse à la relation r

a_1	a_2
51	2

L'image de r par $\sigma_p \circ \text{decrypt}_{\mathtt{s},a_1}$ est la relation

a_1	a_2
1	2

L'image de r par $\text{decrypt}_{\mathtt{s},a_1} \circ \sigma_p$ est la relation vide.

Ainsi donc, la relation (14) dans l'article est fausse car la condition donnée n'est pas assez restrictive.

Correction possible

Ce problème est résolu si on s'intéresse à l'intersection entre $\text{dom}(p)$ et a .

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

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