En fait, l'erreur que j'énonce ci-dessous est résolue dans la thèse. Je m'en était pas aperçu au moment de faire ce document.

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

Ce qui est écrit dans l'article

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

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 $\sigma_p \circ \mathrm{decrypt}_{\mathsf{s},a_1}$ est la relation

a_1	a_2
1	2

L'image de r par $\mathrm{decrypt}_{\mathsf{s},a_1} \circ \sigma_p$ 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 $\mathrm{dom}(p)$ et a .

$$\sigma_p \circ \mathrm{decrypt}_{\mathsf{c},a} \equiv \mathrm{decrypt}_{\mathsf{c},a} \circ \sigma_p \qquad \text{si } \mathrm{dom}(p) \cap a = \emptyset$$
$$\sigma_p \circ \mathrm{decrypt}_{\mathsf{c},a} \equiv \mathrm{decrypt}_{\mathsf{c},a} \circ \sigma_{\mathsf{c} \Rightarrow p} \qquad \text{si } p \text{ est compatible avec } \mathsf{c}$$