Initial state: The intruder knows the handles $\mathsf{h}(\mathsf{n}_1, \mathsf{k}_1)$, $\mathsf{h}(\mathsf{n}_2, \mathsf{k}_2)$; n_1 has the attributes sensitive, extract and whereas n_2 has the attribute extract set. The intruder also knows $\{\!|\mathsf{k}_3|\!\}_{\mathsf{k}_2}$.

Trace:

$$
\begin{array}{lrcl}
\mathsf{Set\_unwrap}: & \mathsf{h}(\mathsf{n}_2, \mathsf{k}_2) & \rightarrow & \mathsf{unwrap}(\mathsf{n}_2, \quad) \\
\mathsf{Unwrap}: & \mathsf{h}(\mathsf{n}_2, \mathsf{k}_2), \{\!|\mathsf{k}_3|\!\}_{\mathsf{k}_2} & \xrightarrow{\text{new } \mathsf{n}_3} & \mathsf{h}(\mathsf{n}_3, \mathsf{k}_3) \\
\mathsf{Unwrap}: & \mathsf{h}(\mathsf{n}_2, \mathsf{k}_2), \{\!|\mathsf{k}_3|\!\}_{\mathsf{k}_2} & \xrightarrow{\text{new } \mathsf{n}_4} & \mathsf{h}(\mathsf{n}_4, \mathsf{k}_3) \\
\mathsf{Set\_wrap}: & \mathsf{h}(\mathsf{n}_3, \mathsf{k}_3) & \rightarrow & \mathsf{wrap}(\mathsf{n}_3, \quad) \\
\mathsf{Wrap}: & \mathsf{h}(\mathsf{n}_3, \mathsf{k}_3), \mathsf{h}(\mathsf{n}_1, \mathsf{k}_1) & \rightarrow & \{\!|\mathsf{k}_1|\!\}_{\mathsf{k}_3} \\
\mathsf{Set\_decrypt}: & \mathsf{h}(\mathsf{n}_4, \mathsf{k}_3) & \rightarrow & \mathsf{decrypt}(\mathsf{n}_4, \quad) \\
\mathsf{Decrypt}: & \mathsf{h}(\mathsf{n}_4, \mathsf{k}_3), \{\!|\mathsf{k}_1|\!\}_{\mathsf{k}_3} & \rightarrow & \mathsf{k}_1
\end{array}
$$

Fig. 6. Re-import attack 2