Noninterference Proofs through Flow Analysis

Kohei Honda and Nobuko Yoshida

August 9, 2002

1 Introduction

This note proves noninterference results (NI) for the secrecy analyses for π^{LA} and π^{LAM} presented in [1], using the inductive information flow analysis. This flow analysis is related to the secrecy typing in [1] in that, while the latter *ensures* safety of information flow, the former *extracts* flow of information. The presentation and study of flow analysis is restricted to its use in NI proofs: further study of the presented flow analysis and its extensions are left for future. Technically the note refers to [1] for π^{LA} and π^{LAM} as well as the secrecy typing in them. For lucid presentation all technical development is done in the following setting.

1. We only use unary types (except for reference types in π^{LAM}). This does not lose generality since affine unary types already have non-trivial information flow and branching types are incorporated in the same way, both in construction and in reasoning.

2. We restrict processes to those with bound output, which results in no loss of generality via the standard translation. While the rules themselves can be presented for free output with the same effect, each rule becomes arguably simpler with bound output.

The remainder of the note is organised as follows. Section 2 introduces basic ideas through examples. Section 3 proves NI for the basic secrecy typing for π^{LA}. Section 4 lists the additional cases needed for the secrecy typing with inflation. Section 5 discusses the NI proof for π^{LAM}.

2 Basic Ideas

The flow analysis we shall use is given as a typing system which is superimposed on $\pi^{\mathsf{LA}}/\pi^{\mathsf{LAM}}$-typing. Since our interest lies in its correspondence with secrecy analysis, we use channel types with secrecy level annotations.

The sequent has the form $\vdash P^A \blacktriangleright \Psi$, which we usually write $\vdash P \blacktriangleright \Psi$, leaving A implicit for legibility. Here Ψ is a finite set of *causal maps*, each of

which has the form $\Gamma \rightsquigarrow x^{\tau}$, where Γ is a finite set of typed names, each of form y^{ρ}. In $\Gamma \rightsquigarrow x^{\tau}$, Γ is a *source* while x^{τ} is a *target*. Sometimes a typed channel in Γ is also called a source. We assume target names are pairwise distinct in each Ψ. Intuitively $\Gamma \rightsquigarrow x^{\tau}$ says interactions at Γ are needed to produce information which is emitted from x.

2.1 Example (1): copy-cat

To illustrate the idea of flow analysis, we first extract a flow of a copy-cat $\vdash !x(c).\overline{y}(e).\overline{c} \triangleright x : ()_s^{\uparrow_{\mathrm{A}}})^{!_{\mathrm{A}}} \otimes y : ()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}$. We use the simplified sequent, assuming the underlying π^{LA}-typing at each step.

$$\dfrac{\dfrac{\dfrac{\dfrac{-}{\vdash \overline{c} \blacktriangleright \emptyset \rightsquigarrow c^{()^{\uparrow_{\mathrm{A}}}}}\,(\mathsf{BOut})}{\vdash e.\overline{c} \blacktriangleright e^{()_s^{\downarrow_{\mathrm{A}}}} \rightsquigarrow c^{()_s^{\uparrow_{\mathrm{A}}}}}\,(\mathsf{In}^{\downarrow_{\mathrm{A}}})}{\vdash \overline{y}(e).\overline{c} \blacktriangleright y^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}} \rightsquigarrow c^{()_s^{\uparrow_{\mathrm{A}}}}}\,(\mathsf{BOut})}{\vdash !x(c).\overline{y}(e).\overline{c} \blacktriangleright y^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}} \rightsquigarrow x^{(()_s^{\uparrow_{\mathrm{A}}})^{!_{\mathrm{A}}}}}\,(\mathsf{In}^{!_{\mathrm{A}}})$$

Note the action of y actually depends on y: so, from an intuitive idea of causality, one may as well consider there is a flow from x to y, rather than y to x. However the extracted flow $y^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}} \rightsquigarrow x^{(()_s^{\uparrow_{\mathrm{A}}})^{!_{\mathrm{A}}}}$ does capture the flow of this typed π^{LA}-term: as discussed elsewhere, the replicated type of x has a non-trivial information content, which *depends on* the interaction starting at y.

2.2 Example (2): composition

The following simple example shows how we can extract information flow from a parallel composition of processes. Given a term $\vdash \overline{x}(c)c.\overline{w} \triangleright x{:}(()^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}} \otimes w{:}()^{\uparrow_{\mathrm{A}}}$, we can extract its flow as:

$$\vdash \overline{x}(c)c.\overline{w} \blacktriangleright x{:}(()^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}} \rightsquigarrow w{:}()^{\uparrow_{\mathrm{A}}}$$

Then we compose it with the copy-cat we discussed in Example (1), as follows.

$$(\mathsf{Par})\ \dfrac{\begin{array}{c}\vdash !x(c).\overline{y}(e).\overline{c} \blacktriangleright y^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}} \rightsquigarrow x^{(()_s^{\uparrow_{\mathrm{A}}})^{!_{\mathrm{A}}}} \\ \vdash \overline{x}(c)c.\overline{w} \blacktriangleright x^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}} \rightsquigarrow w^{()_{s'}^{\uparrow_{\mathrm{A}}}}\end{array}}{\vdash !x(c).\overline{y}(e).\overline{c} \mid \overline{x}(c)c.\overline{w} \blacktriangleright \{\, y^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}} \rightsquigarrow x^{(()_s^{\uparrow_{\mathrm{A}}})^{!_{\mathrm{A}}}},\ y^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}} \rightsquigarrow w^{()_{s'}^{\uparrow_{\mathrm{A}}}} \,\}}$$

In the inference for parallel composition, $x^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}}$ in the antecedent is replaced by $y^{(()_s^{\downarrow_{\mathrm{A}}})^{?_{\mathrm{A}}}}$. This is because the complement of an output at x is already supplied (as shown by the fact that the resulting action type has $x{:}(()_s^{\uparrow_{\mathrm{A}}})^{!_{\mathrm{A}}}$), and because it depends on y. In this way the resulting typed names should conform to the resulting action type.

2.3 Example (3): Unused Types

We consider the following typed term in π^{LA}, with secrecy annotation on types:

$$\vdash x(y_1y_2).\overline{y_1}(e)e.\overline{f} \triangleright x{:}(((){}^{\downarrow_{\mathsf{A}}}_{L})^{?_{\mathsf{A}}}(()^{\downarrow_{\mathsf{A}}}_{H})^{?_{\mathsf{A}}})^{\downarrow_{\mathsf{L}}} \otimes f{:}()^{\uparrow_{\mathsf{A}}}_{L}$$

This process is secure: to output a low-level f, it is suppressed by e carried by y_1, but this e is again a low-level, so no insecure flow takes place. The flow analysis presented in the next section represents the information flow of this process as follows.

$$\vdash x(y_1y_2).\overline{y_1}(e)e.\overline{f} \blacktriangleright x{:}(((){}^{\downarrow_{\mathsf{A}}}_{L})^{?_{\mathsf{A}}})^{\downarrow_{\mathsf{L}}} \rightsquigarrow f{:}()^{\uparrow_{\mathsf{A}}}_{L}$$

Here, in the causal map $x{:}(((){}^{\downarrow_{\mathsf{A}}}_{L})^{?_{\mathsf{A}}})^{\downarrow_{\mathsf{L}}} \rightsquigarrow f{:}()^{\uparrow_{\mathsf{A}}}_{L}$, the type of x does not contain the type of the channel which is not used (here y_2). Thus, if we calculate the level of input and that of output, we can see the process inputs at L and outputs L, which is indeed secure.

3 π^{LA} (1): Basic Secrecy Analysis

3.1 Preliminaries

First we write $\tau \prec \tau'$ if τ is "part of" τ'. Formally we define $\prec$ from:

$$(\vec{\tau}_1\vec{\tau}_2)^p_s \prec (\vec{\tau}_1\rho\vec{\tau}_2)^p_s$$

and closing it under type formation. Second we write $\Psi \vdash y{:}\tau \rightsquigarrow x{:}\rho$ when $\Gamma \rightsquigarrow x{:}\rho \in \Psi$ such that $y{:}\tau \in \Gamma$. We also write $\Psi \vdash \emptyset \rightsquigarrow x{:}\rho$ when $\emptyset \rightsquigarrow x{:}\rho \in \Psi$. Note the collection of such "unit chains" in Ψ completely determines Ψ. Based on these definitions, we define $\Psi_1 \asymp \Psi_2$ and $\Psi_1 \odot \Psi_2$ (which are analogous to $A_1 \asymp A_2$ and $A_1 \odot A_2$) as follows. Below we say Ψ *conforms to* A if for each $x{:}\tau$ we have $A(x) = \tau'$ such that $\tau \prec \tau'$.

Definition 3.1 Assume $A_1 \asymp A_2$, to which the modes of channels in Ψ_1 and Ψ_2 respectively conform. Then $\Psi_1 \asymp \Psi_2$ iff the following two conditions hold.

(1) If Ψ_1 has a source channel y^{ρ}, and its compensating channel is in A_2, then it should also occur in Ψ_2 as a target y^{τ} such that $\rho \prec \overline{\tau}$; and the symmetric case.

(2) If x^{ρ_1} occurs in Ψ_1 and x^{ρ_2} occurs in Ψ_2 except for (a), then $\rho_1 = \rho_2$.

Definition 3.2 Assume $\Psi_{1,2}$ such that $\Psi_1 \asymp \Psi_2$, with the underlying action types A_1 and A_2. Then $\Psi_1 \odot \Psi_2$ is given as follows:

(1) If $\Psi_1 \cup \Psi_2 \vdash x_{i+1}{:}\tau_{i+1} \rightsquigarrow x_i{:}\tau_i$ for $1 \leq i \leq n-1$ such that each x_i is distinct and, moreover, $\mathsf{md}(\tau_n) = \mathsf{md}((A_1 \odot A_2)(x_n))$, then $\Psi_1 \odot \Psi_2 \vdash x_n{:}\tau_n \rightsquigarrow x_1{:}\tau_1$.

$$\frac{}{\vdash \mathbf{0} \blacktriangleright \emptyset}\ (\mathsf{Zero}) \qquad \frac{\vdash P_i \blacktriangleright \Psi_i\ (i=1,2) \quad \Psi_1 \asymp \Psi_2}{\vdash P_1|P_2 \blacktriangleright \Psi_1 \odot \Psi_2}\ (\mathsf{Par}) \qquad \frac{\vdash P \blacktriangleright \Psi}{\vdash (\boldsymbol{\nu}\, x)P \blacktriangleright \Psi/x}\ (\mathsf{Res})$$

$$\frac{\vdash P \blacktriangleright \Psi_i}{\vdash P \blacktriangleright \bigcup_i \Psi_i}\ (\mathsf{Union}) \qquad \frac{\vdash P \blacktriangleright \Psi' \supset \Psi}{\vdash P \blacktriangleright \Psi}\ (\mathsf{Subset})$$

$$\frac{\vdash P \blacktriangleright \Gamma \rightsquigarrow w^{\sigma} \quad \vec{\rho} = \Gamma(\vec{y})}{\vdash x(\vec{y}).P \blacktriangleright \Gamma/\vec{y} \cdot x^{(\vec{\rho})^{\downarrow_{\mathrm{L}}}} \rightsquigarrow w^{\sigma}}\ (\mathsf{In}^{\downarrow_{\mathrm{L}}}) \qquad \frac{\vdash P_i \blacktriangleright \Gamma_i \rightsquigarrow y_i^{\rho_i}}{\vdash \overline{x}(\vec{y})(\Pi_i P_i) \blacktriangleright \odot \Gamma_i \rightsquigarrow x^{(\vec{\rho})^{\uparrow_{\mathrm{L}}}}}\ (\mathsf{BOut}^{\uparrow_{\mathrm{L}}})$$

$$\frac{\vdash P \blacktriangleright \Gamma \rightsquigarrow w^{\sigma}}{\vdash x(\vec{y}).P \blacktriangleright \Gamma/\vec{y} \cdot x^{()_s^{\downarrow_{\mathrm{A}}}} \rightsquigarrow w^{\sigma}}\ (\mathsf{In}^{\downarrow_{\mathrm{A}}}) \qquad \frac{\vdash P_i \blacktriangleright \Gamma_i \rightsquigarrow y_i^{\rho_i}}{\vdash \overline{x}(\vec{y})(\Pi_i P_i) \blacktriangleright \emptyset \rightsquigarrow x^{()_s^{\uparrow_{\mathrm{A}}}}}\ (\mathsf{BOut}^{\uparrow_{\mathrm{A}}})$$

$$\frac{\vdash P \blacktriangleright \Gamma \rightsquigarrow z^{\sigma} \quad p \in \{!_{\mathrm{L}}, !_{\mathrm{A}}\}}{\vdash !\, x(\vec{y}z).P \blacktriangleright \Gamma/\vec{y}z \rightsquigarrow x^{(\sigma)^{!_{\mathrm{L}}}}}\ (\mathsf{In}^{!_{\mathrm{L}},!_{\mathrm{A}}})\ p \in \{!_{\mathrm{L}}, !_{\mathrm{A}}\} \qquad \frac{\vdash P_i \blacktriangleright \Psi_i \quad \vdash Q \blacktriangleright z^{\rho} \cdot \Gamma \rightsquigarrow w^{\sigma}}{\vdash \overline{x}(\vec{y}z)(\Pi P_i|Q) \blacktriangleright \Gamma \cdot x^{(\rho)^{p}} \rightsquigarrow w^{\sigma}}\ (\mathsf{BOut}^{?_{\mathrm{L}},?_{\mathrm{A}}})\ p \in \{?_{\mathrm{L}}, ?_{\mathrm{A}}\}$$

Figure 1: Flow Analysis for π^{LA}

(2) If $\Gamma \rightsquigarrow x{:}\tau \in \Psi_i$ and for no y we have $\Psi_1 \odot \Psi_2 \vdash y{:}\rho \rightsquigarrow x{:}\tau$ by (1) above, then we have $\Psi_1 \odot \Psi_2 \vdash \emptyset \rightsquigarrow x{:}\tau$.

Note $\Psi_1 \asymp \Psi_2$ says we do not leave **?** or $\downarrow$-moded channels in the resulting source if these channels are eliminated at the level of the action type. Taking only part of it for compensation is to deal with the situation discussed in §2.3.

3.2 Inductive Flow Analysis

The rules are given in Figure 1, each rule superimposed with the corresponding π^{LA}-typing rule (thus we in fact have the rule for (Weak) which weakens the action type but does not change the causal map, which we omit). The rules use at most one causal map except for (Par), (Union) and (Subset). Brief illustration of the typing rules follows.

1. (Par) connects causal chains so that modes of the source match the resulting (implicit) action type. It may need more than one causal maps for compensating multiple sources in accordance with the action types.

(Zero), (Weak) and (Res) need no illustration except they assume the manipulation of underlying action types (as all other rules do). (Subset) and (Union) bridge (Par) and other rules.

2. In $(\mathrm{In}^{\downarrow_{\mathrm{L}}})$ we extract part of the carried types used for producing the result. $(\mathrm{BOut}^{\uparrow_{\mathrm{L}}})$ carries all causality information from its abstracted names. In $(\mathrm{In}^{\downarrow_{\mathrm{A}}})$ we cancel all carried types, unlike $(\mathrm{In}^{\downarrow_{\mathrm{L}}})$, since this action directly receives information. Dually $(\mathrm{BOut}^{\uparrow_{\mathrm{A}}})$ throws away all information on source, since this immediately tampering action takes place without depending on any other actions.

3. In $(\mathrm{In}^{!_{\mathrm{L}},!_{\mathrm{A}}})$, we do not record the incoming abstracted sources (keeping them leads to refined analysis, though this is unnecessary for the present purpose). Dually, in $(\mathrm{BOut}^{?_{\mathrm{L}},?_{\mathrm{A}}})$, the process receives information at z in the antecedent, which is registered as the type of x.

The analysis extracts a causal chain from the source to the target.

3.3 Flow Analysis and Noninterference

In this subsection we show that our secrecy typing ensures that a causal chain is non-existent in secure processes if the source has a higher or incompatible level in comparison with the target, except for semantically innocuous "cancelable" indirections. Combined with behavioural properties associated with such chains, we can establish the noninterference property. To relate secrecy analysis and causality analysis, we need some preparations. First we define those types which are essentially non-affecting due to linearity.

Definition 3.3 Let τ have mode $?_{\mathrm{L}}$ or $\downarrow_{\mathrm{L}}$. Then τ is *cancelable* when:

1. $\tau = (\rho'^{\downarrow_{\mathrm{L}}})^{?_{\mathrm{L}}}$ such that ρ' is cancelable.
2. $\tau = (\rho_1..\rho_n)^{\downarrow_{\mathrm{L}}}$ such that each ρ_i is cancelable.

If we have branching, cancelable types do not include branching linear input, since it does receive non-trivial information. Using cancelable types we can precisely specify the level of reception of information in interaction.

Definition 3.4 (receiving level) The *receiving level of* τ, denoted $\mathsf{receive}(\tau)$, is given by the following equations: $\mathsf{receive}(\tau) = \mathsf{tamp}(\overline{\tau})$ if τ is not cancelable, and $\mathsf{receive}(\tau) = \bot$ if else.

In the definition of receiving levels, the exceptional treatment for cancelable types is necessary because these types are better to be considered as types for which "we don't care secrecy levels", due to the inductive lack of immediate information flow.

We can now relate the flow analysis and secrecy typing.

Proposition 3.5 *Assume below (a)* $\vdash_{\mathsf{sec}} P \triangleright A$*; (b)* $\vdash P \blacktriangleright \Gamma \rightsquigarrow x^{\sigma}$ *is derived following the derivation of* $\vdash_{\mathsf{sec}} P \triangleright A$ *and (c)* $y \in \mathtt{dom}(\Gamma)$*.*

1. *If* $\Gamma(y) = \tau$ *then* $\mathsf{receive}(\tau) \sqsubseteq \mathsf{tamp}(\sigma)$ *for each* τ_i*.*
2. *If* $\Gamma(y) = \tau$ *such that* $\mathsf{md}(\tau) \in \{?_{\mathrm{A}}, \downarrow_{\mathrm{A}}\}$*, then* $\mathsf{receive}(A(y)) \sqsubseteq \mathsf{tamp}(\sigma)$*.*
3. *If* $\Gamma(y) = \tau$ *and* $\mathsf{receive}(A(y)) \not\sqsubseteq \mathsf{tamp}(\sigma)$ *then* τ *is cancelable.*

Proof: (1) is by rule induction, noting the causal analysis uses only part of channel types which are really used for suppressing the final tampering output. (2) is immediate by the definition of receiving levels. For (3) let us say τ is *immediately receiving* if $\overline{\tau}$ is immediately tampering. Note if the immediately receiving type in (2) is included in the source then $\mathsf{receive}(A(y)) \not\sqsubseteq \mathsf{tamp}(\sigma)$ is not possible. By induction of the immediately receiving type, the resulting receiving type can only be cancelable. ■

The flow analysis allows us to inductively prove the behavioural property associated with noninterference as follows. We use the following notion, which is a term mediating an observable type to the canonical observable type.

Definition 3.6 Let $\mathsf{md}(\tau), \mathsf{md}(\rho) \in \mathcal{M}_{!,\uparrow}$. Then we say P is a *mediator from* $x{:}\tau$ *to* $y{:}\rho$ if it is typed as $\vdash P \triangleright x{:}\overline{\tau} \otimes y{:}\rho$.

For example, $\overline{w}(e).\overline{z}$ is a mediator from $w{:}((\,)^{\uparrow_{\mathrm{A}}})^{!_{\mathrm{L}}}$ to $z{:}(\,)^{\uparrow_{\mathrm{A}}}$. We can now prove the behavioural property. Below a process P *compensates* A if $\vdash P \triangleright \overline{A_0}$ where A_0 is the subset of A with names of modes in $\mathcal{M}_{?,\downarrow}$. Further $A \restriction \vec{y}$ projects A onto $\vec{y}$ while $A/\vec{y}$ takes off $\vec{y}$ from A.

Proposition 3.7 *Assume* $\vdash P \blacktriangleright \Gamma \rightsquigarrow w^{\tau}$ *following* $\vdash P \triangleright A$*, with* $\vec{y} = \mathsf{fn}(\Gamma)$*. Further assume (1)* R *compensates* $A \restriction \vec{y}$*, (2)* $S_{1,2}$ *compensates* $A/\vec{y}w$*, and (3)* T *is a mediator from* $w : \tau$ *to a fresh* $z : (\,)^{\uparrow_{\mathrm{A}}}$*. Then* $P|R|T|S_1 \Downarrow_z$ *iff* $P|R|T|S_2 \Downarrow_z$*.*

Proof: By induction of the rules in Figure 1.

(Zero) Vacuous.

(Res) Assume we infer $\vdash (\boldsymbol{\nu}\, x)P \blacktriangleright y{:}\tau\Gamma/x$ from $\vdash P \blacktriangleright y{:}\tau\Gamma$. First assume $x \notin \mathsf{fn}(\Gamma)$. If, for R, S_i and T as above, we have $((\boldsymbol{\nu}\, x)P)|R|S_1|T \Downarrow_z$, then we also have $P|R|S_1|T \Downarrow_z$. Since S_1 compensates $A/\vec{y}wx$ by the type of x (which is of mode either $\updownarrow$ or *modeset*$!$, we have $P|R|S_2|T \Downarrow_z$, that is $(\boldsymbol{\nu}\, x)P|R|S_2|T \Downarrow_z$, as required.

(Sub) Immediate.

(Union) Immediate.

(Par) We show the special case when we compose $\vdash P \blacktriangleright x:\tau y:\rho$ (following $\vdash P \triangleright A$) and $\vdash Q \blacktriangleright y:\rho' u:\delta$ (following $\vdash Q \triangleright B$). The general case is by the same reasoning (in fact any parallel composition can be decomposed into parallel composition of connected processes). Let $C = A \odot B$ and assume the names compensated for in C/xz are $\vec{v}\vec{w}$ where, for simplicity, we assume $\vec{v}$ are in A and $\vec{w}$ are in B (the case when names are overlapped can be treated similarly). Let R, S_i and T be as above. Since types say terms are either replicated or linear outputs, we can decompose S_1 into $V_1^{\vec{v}}$ and $W_1^{\vec{w}}$. Similarly we decompose S_2 into $V_2^{\vec{v}}$ and $W_2^{\vec{w}}$. Now assume $(P|Q)|S_1^{\vec{v}\vec{w}}|R^u|T^{xz} \Downarrow_z$, that is $P|V_1|(\boldsymbol{\nu}\, u)(Q|R)|(\boldsymbol{\nu}\, \vec{w})(W_1|T) \Downarrow_z$. By the induction hypothesis on P we have: $P|V_2|(\boldsymbol{\nu}\, u)(Q|R)|(\boldsymbol{\nu}\, \vec{w})(W_1|T) \Downarrow_z$, that is $Q|W_1|R|V_2|(\boldsymbol{\nu}\, x)(P|T) \Downarrow_z$. By the induction hypothesis on Q we have: $Q|W_2|R|V_2|(\boldsymbol{\nu}\, x)(P|T) \Downarrow_z$, as required.

(In$^{\downarrow_{\mathrm{L}}}$) Assume given the inference

$$\frac{\vdash P \blacktriangleright \Gamma \rightsquigarrow w^{\sigma} \quad \vec{\rho} = \Gamma(\vec{y})}{\vdash x(\vec{y}).P \blacktriangleright \Gamma/\vec{y} \cdot x^{(\vec{\rho})^{\downarrow_{\mathrm{L}}}} \rightsquigarrow w^{\sigma}}$$

following appropriate linear/affine typing. Assume given appropriate $S_{1,2}$, R and T as stated. Then by applying extended reduction at x we have, $x(\vec{y}).P|S_i \cong (\boldsymbol{\nu}\, \vec{y})(P|S_i')$ where S_i' is in an appropriate form for P. Thus if $(x(\vec{y}).P)|S_1|R|T^{wz} \Downarrow_z$ then $P|S_1'|R|T \Downarrow_z$ hence $P|S_2'|R|T \Downarrow_z$ that is $(x(\vec{y}).P)|S_2|R|T^{wz} \Downarrow_z$ hence as required.

Other prefix rules are similar. ■

As a special case of Proposition 3.7 (setting $\Gamma = \emptyset$), we obtain:

Corollary 3.8 *Let* $\vdash P \blacktriangleright \emptyset \rightsquigarrow x^{\uparrow_{\mathrm{A}}}$ *following* $\vdash P \triangleright A$. *Let* $B = \overline{A/x}$ *and* $\vdash R_{1,2} \triangleright B$. *Then* $P|R_1 \Downarrow_x$ *iff* $P|R_2 \Downarrow_x$.

We can now establish the key property related with noninterference in π^{LA}.

Proposition 3.9 *Let* $\vdash P \blacktriangleright \Gamma \rightsquigarrow x^{\uparrow_{\mathrm{A}}}$ *following* $\vdash P \triangleright A$ *with each type in* Γ *cancelable. Let* $B = \overline{A/x}$ *and* $\vdash R_{1,2} \triangleright B$. *Then* $P|R_1 \Downarrow_x$ *iff* $P|R_2 \Downarrow_x$.

Proof: By induction on the structure of cancelable types we check that, in $P|R_i$ as above, there is a unique P' for both $i = 1, 2$ such that $P|R_i \cong P'|R_i'$ and the interface Γ is all cancelled. This is because, by the liveness properties [2], we can always force the interaction via $!_{\mathrm{L}}$-$?_{\mathrm{L}}$ channels and unary $\downarrow_{\mathrm{L}}$-$\uparrow_{\mathrm{L}}$ channels regardless of the shape of the process in the environment (i.e. the compensating actions of the other party is uniquely determined by its type). Thus the statement is reduced to Corollary 3.8. ■

We can now prove the noninterference. Below the side condition for A given at the top does not lose generality since if $\overline{A}$ (hence R) contains replication they can be distributed by the replication theorem.

Proposition 3.10 *Assume* $\mathsf{md}(\overline{A}) \subset \mathcal{M}_{?,\downarrow}$.

1. *Let* $\vdash_{\mathsf{sec}} R \triangleright \overline{A} \otimes x : ()^{\uparrow_{\mathrm{A}}}_{s}$ *such that* $\mathsf{tamp}(A) \not\sqsubseteq s$ *and* $\vdash R \blacktriangleright \Gamma \rightsquigarrow x^{()^{\uparrow_{\mathrm{A}}}_{s}}$ *following the derivation of* $\vdash_{\mathsf{sec}} R \triangleright \overline{A} \otimes x : ()^{\uparrow_{\mathrm{A}}}_{s}$. *Then for each* $y \in \mathtt{dom}(\Gamma)$, $\Gamma(y)$ *is cancelable.*

2. *Let* $\vdash_{\mathsf{sec}} P_{1,2} \triangleright A$ *and* $\vdash_{\mathsf{sec}} R \triangleright \overline{A} \otimes x : ()^{\uparrow_{\mathrm{A}}}_{s}$ *with* $\mathsf{tamp}(A) \not\sqsubseteq s$. *Then* $(\boldsymbol{\nu}\, \mathsf{fn}(A))(P_1|R) \Downarrow_s$ *iff* $(\boldsymbol{\nu}\, \mathsf{fn}(A))(P_2|R) \Downarrow_s$.

3. (noninterference) *If* $\vdash_{\mathsf{sec}} P_{1,2} \triangleright A$ *then* $\mathsf{tamp}(A) \not\sqsubseteq s$ *then* $\vdash_{\mathsf{sec}} P_1 \cong_s P_2 \triangleright A$.

Proof: (1) is direct from Prop. 3.5 (1) and (3). For (2), by (1) above and by induction on the number of such forced reduction steps, we can reduce A to that which contains only $?_{\mathrm{A}}$ or $\downarrow_{\mathrm{A}}$-channels. We can now appeal to Proposition 3.9, to obtain (2). Finally (3) is from the context lemma give and (2) above, hence as required. ■

4 π^{LA} (2): Inflation

For inflation, we assume the rule in which we change the secrecy annotation of typed names in the flow analysis following the change in action types. Formally, using the full sequent, we add the following rule (with $\Psi \sqcup s$ defined as for action types):

$$(\mathsf{Inf})\frac{\vdash P^{\mathsf{inf}(A)} \blacktriangleright \Psi \sqcup \mathsf{tamp}(A)}{\vdash P^{A} \blacktriangleright \Psi}$$

Now assume $\vdash P \blacktriangleright \Gamma \rightsquigarrow x : \tau$ is the antecedent of the above rule, with the conclusion $\vdash P \blacktriangleright \Gamma' \rightsquigarrow x : \tau'$. Clearly $\mathsf{tamp}(\tau') = \mathsf{tamp}(\tau)$ and, for each y_i in $\mathsf{fn}(\Gamma)$, $\mathsf{receive}(\Gamma'(y_i)) \sqsubseteq \mathsf{receive}(\Gamma(y_i))$. Further cancelable types in Γ' are precisely those in Γ. Thus we obtain:

Proposition 4.1 *The same properties as stated in Proposition 3.5 hold for the secrecy analyse with inflation.*

The rest is the same as Section 3.

5 π^{LAM}

In this section we consider the secrecy analysis on π^{LAM} with inflation. The rule for the flow analysis of inflation is already given in §4. The causality analysis in π^{LAM} is more complex than that in π^{LA} in that we have more possibility of causal relations, together with more "observable" actions. Among others it uses "part of" reference types depending on their use in producing information. The key insight is that reference types (and mutable types in general) have the property that they as well as their duals have non-trivial tampering levels, unlike stateless replicated types. Part of reference types is written using the following notation.

(In$^{!_{\mathrm{M}}}$-1)
$$\frac{\vdash P \blacktriangleright \Gamma \rightsquigarrow z^{\sigma} \quad z \in \{\vec{y}\}}{\vdash !x(\vec{y}).P \blacktriangleright \Gamma/\vec{y} \rightsquigarrow x^{(\sigma)_s^{!_{\mathrm{M}}}}}$$

(In$^{!_{\mathrm{M}}}$-2)
$$\frac{\vdash P \blacktriangleright \Gamma \rightsquigarrow z^{\sigma} \quad z \notin \{\vec{y}\}}{\vdash !x(\vec{y}).P \blacktriangleright (\Gamma/\vec{y}) \cdot x^{()_s^{!_{\mathrm{M}}}} \rightsquigarrow z^{\sigma}}$$

(BOut$^{?_{\mathrm{M}}}$-1)
$$\frac{\vdash P_i \blacktriangleright \Psi_i \quad \vdash Q \blacktriangleright \Psi}{\vdash \overline{x}(\vec{y}z)(\Pi_i P_i | Q) \blacktriangleright \emptyset \rightsquigarrow x^{()_s^{?_{\mathrm{M}}}}}$$

(BOut$^{?_{\mathrm{M}}}$-2)
$$\frac{\vdash P_i \blacktriangleright \Psi_i \quad \vdash Q \blacktriangleright z^{\rho} \cdot \Gamma \rightsquigarrow u^{\sigma}}{\vdash \overline{x}(\vec{y}z)(\Pi_i P_i | Q) \blacktriangleright x^{(\rho)_s^{?_{\mathrm{M}}}} \cdot \Gamma \rightsquigarrow u^{\sigma}}$$

(BOut$^{?_{\mathrm{M}}}$-3)
$$\frac{\vdash P_i \blacktriangleright \Psi_i \quad \Psi_j = \Gamma \cdot y_j^{\rho} \rightsquigarrow u^{\sigma} \quad \vdash Q \blacktriangleright \Psi}{\vdash \overline{x}(\vec{y}z)(\Pi_i P_i | Q) \blacktriangleright (\Gamma/y_j) \cdot x^{(\rho)_s^{?_{\mathrm{M}}}} \rightsquigarrow u^{\sigma}}$$

(Ref-1)
$$\frac{-}{\vdash \mathsf{Ref}\langle xy \rangle \blacktriangleright y^{\overline{\tau}} \rightsquigarrow x^{\mathsf{refL}_s\langle\tau\rangle}}$$

(Ref-2)
$$\frac{\tau \text{ mutable}}{\vdash \mathsf{Ref}\langle xy \rangle \blacktriangleright x^{\mathsf{ref}_s\langle\tau\rangle} \rightsquigarrow y^{\overline{\tau}}}$$

(Read-1)
$$\frac{\vdash P^c \blacktriangleright \Gamma \cdot c^{(\vec{\rho})^{\downarrow_{\mathrm{L}}}} \rightsquigarrow z^{\sigma}}{\vdash \overline{x}\mathtt{inl}(c)P \blacktriangleright \Gamma \cdot x^{\overline{\mathsf{refL}_s\langle\vec{\rho}\rangle}} \rightsquigarrow z^{\sigma}}$$

(Read-2)
$$\frac{\vdash P^c \blacktriangleright \Psi \quad \tau \text{ mutable}}{\vdash \overline{x}\mathtt{inl}(c)P \blacktriangleright \emptyset \rightsquigarrow x^{\overline{\mathsf{ref}_s\langle\varepsilon\rangle}}}$$

(Write-1)
$$\frac{\vdash P^v \blacktriangleright \Psi \quad \vdash Q^c \blacktriangleright \Psi'}{\vdash \overline{x}\mathtt{inr}(vc)(P|Q) \blacktriangleright \emptyset \rightsquigarrow x^{\overline{\mathsf{ref}_s\langle\varepsilon\rangle}}}$$

(Write-2)
$$\frac{\vdash P^v \blacktriangleright \Gamma \cdot v^{\rho} \rightsquigarrow u^{\sigma} \quad \vdash Q^c \blacktriangleright \Psi'}{\vdash \overline{x}\mathtt{inr}(vc)(P|Q) \blacktriangleright \Gamma \cdot x^{\overline{\mathsf{refR}_s\langle\rho\rangle}} \rightsquigarrow u^{\sigma}}$$

(Write-3)
$$\frac{\vdash P^v \blacktriangleright \Psi \quad \vdash Q^c \blacktriangleright \Gamma \cdot c^{()^{\downarrow_{\mathrm{L}}}} \rightsquigarrow u^{\sigma}}{\vdash \overline{x}\mathtt{inr}(vc)(P|Q) \blacktriangleright \Gamma \cdot x^{\overline{\mathsf{ref}_s\langle\varepsilon\rangle}} \rightsquigarrow u^{\sigma}}$$

Figure 2: Flow Analysis for Stateful Actions

1. $\mathsf{refL}_s\langle\vec{\tau}\rangle$ stands for $[(\vec{\tau})^{\uparrow_{\mathrm{L}}} \& ()^{\uparrow_{\mathrm{L}}}]_s^{!_{\mathrm{L}}}$.
2. Symmetrically $\mathsf{refR}_s\langle\vec{\tau}\rangle$ stands for $[()^{\uparrow_{\mathrm{L}}} \& \overline{\vec{\tau}}()^{\uparrow_{\mathrm{L}}}]_s^{!_{\mathrm{L}}}$.

where, in fact, we only treat the case $\vec{\tau}$ is a vector of length zero or one. Note these types are *not* mutating: these are used when a channel is used as a source of information, not as a target. The grammar of cancelable types adds those

of form $\mathsf{refL}_s\langle\varepsilon\rangle$ as well as closing under the new syntax of types (so if τ is cancelable then so is $\overline{\mathsf{refL}_s\langle\tau\rangle}$). We observe:

Proposition 5.1 $\mathsf{tamp}(\mathsf{ref}_s\langle\tau\rangle) = \mathsf{tamp}(\overline{\tau})\sqcap\mathsf{tamp}(\tau)$, $\mathsf{tamp}(\mathsf{refL}_s\langle\tau\rangle) = \mathsf{tamp}(\tau)$, $\mathsf{tamp}(\mathsf{refR}_s\langle\tau\rangle) = \mathsf{tamp}(\overline{\tau})$, *and* $\mathsf{tamp}(\overline{\mathsf{ref}_s\langle\varepsilon\rangle}) = s$.

We list the additional rules for stateful actions in Figure 2, writing P^c when P is an input prefixed term with subject c. In addition to these rules, linear/affine output rules for stateless actions should also have the counterpart of (Write-3), which are omitted since the treatment is the same. (Write-3) and related rules introduce a typed channel to a source when the dual of the type can have a non-trivial tampering level. Below we observe the construction of reference types add a new collection of cancelable types since they are linearly replicated.

Proposition 5.2 *The same properties as stated in Proposition 3.5 hold for the secrecy analyse for π^{LAM} with inflation.*

Proof: By inspecting each rule as before. In detail:

(In$^{!_{\mathbb{M}}}$-1) Because the receiving levels of the source and the tampering level of the target do not change (except some names are taken off).

(In$^{!_{\mathbb{M}}}$-2) Because z is tampering its level is the same as, or higher than, s.

(Out$^{?_{\mathbb{M}}}$-1) Trivial.

(Out$^{?_{\mathbb{M}}}$-2) Because no change takes place in receiving levels in the source and the tampering level in the target.

(Out$^{?_{\mathbb{M}}}$-3) Same as above except some names are taken off.

(Ref-1) By Proposition 5.1.

(Ref-2) By structural security.

(Read-1) If $\vec{\rho}$ is null then the type of x is cancelable hence done. If $\vec{\rho} = \tau$ then we use Proposition 5.1.

(Read-2) Immediate.

(Write-1) Immediate.

(Write-2) By Proposition 5.1.

(Write-3) Because the type at x is cancelable.

(Inf) has already been reasoned in §4. Thus we have exhausted all cases. ■

Instead of Proposition 3.10 (2), we use the following operational property which suits the form of context lemma for π^{LAM}. The proof is essentially the same.

Corollary 5.3 *Let* $\vdash_{\mathsf{sec}} R \triangleright \overline{A} \otimes B$ *such that* $\mathsf{tamp}(A) \not\sqsubseteq s$ *and, for each* $x{:}\tau \in B$, $\mathsf{tamp}(\tau) \sqsubseteq s$. *Then, for each* $y \in \mathsf{fn}(B)$, *whenever* $\vdash R \blacktriangleright \Gamma \rightsquigarrow y^{\rho}$ *and* $z \in \mathsf{fn}(\Gamma)$, *either* $z \notin \mathsf{fn}(A)$ *or, if not,* $\Gamma(z)$ *is cancelable.*

We now prove the noninterference.

Proposition 5.4 (noninterference for secrecy analysis in π^{LAM}) *If* $\vdash_{\mathsf{sec}} P_{1,2} \triangleright A$ *in the secrecy analysis for* π^{LAM}, *we have* $\vdash_{\mathsf{sec}} P_1 \cong_s P_2 \triangleright A$ *where* $\cong_s$ *is the reduction-based secrecy sensitive congruence.*

In the following proof we consistently ignore $\updownarrow$-channels (assume they are hidden immediately after composition) and cancelable types, both of which lose no generality. Further we ignore edges in action types which are irrelevant in the proof.

PROOF: We show the closure of the following relation under parallel composition satisfies the context lemma for π^{LAM}.

$$\vdash_{\mathsf{sec}} P_1 \mathcal{R} P_2 \triangleright A \stackrel{\mathrm{def}}{\Leftrightarrow} \vdash_{\mathsf{sec}} P_{1,2} \triangleright A,\ \forall x{:}\tau \in A.\mathsf{tamp}(\tau) \not\sqsubseteq s.$$

Since $\mathsf{tamp}(A) \not\sqsubseteq s$ implies $\mathsf{tamp}(\tau) \not\sqsubseteq s$ for each $x{:}\tau \in A$, this suffices. Suppose $\vdash_{\mathsf{sec}} P \mathcal{R} Q \triangleright A$ as above and, moreover, $\vdash_{\mathsf{sec}} R \triangleright B$ such that $A \asymp B$. For simplicity we assume $B = \overline{A} \otimes C$ (this does not lose any generality since by mode-closure we should compensate all linear/affine/?-channels) and further assume, again w.l.o.g. $\mathsf{md}(C) \subset \mathcal{M}_!$ and $\mathsf{md}(A) \subset \mathcal{M}_! \cup \mathcal{M}_?$. Let $C = C_1 \otimes C_2$ such that (1) $\mathsf{tamp}(\tau_1) \not\sqsubseteq s$ for each $z{:}\tau$ in C_1 and (2) $\mathsf{tamp}(\tau_1) \sqsubseteq s$ for each $z{:}\tau$ in C_2. Let R_1 and R_2 are parts of R which contain all replicated processes and reference agents which correspond to C_1 and C_2, respectively. By Corollary 5.3 there are no mediating names between R_1 and $_2$, so that we can write $R \stackrel{\mathrm{def}}{=} R_1 | R_2$ for R_1 and R_2 which have, again using Corollary 5.3, the following typings:

$$\vdash_{\mathsf{sec}} R_1 \triangleright C_1 \otimes \overline{A} \otimes C_2' \qquad \vdash_{\mathsf{sec}} R_2 \triangleright C_2 \otimes C_1' \otimes A'$$

where C_2' compensates part of C_2 by reading (including non-stateful ?-actions), C_1' compensates part of C_1 by stateful writing and A' compensates part of A by writing. Now suppose $P|R \longrightarrow P'$. The interaction with P can take place only with R_1 by their types. Hence we can write this reduction as either $P|R \longrightarrow (\boldsymbol{\nu}\, \vec{y})(P'|R_1')|R_2$ or $P|R \longrightarrow P_1|R_1|R_2'$.

1. If $P|R \longrightarrow (\boldsymbol{\nu}\, \vec{y})(P'|R_1')|R_2$, then $Q|R$ simulates this by non-action. Indeed, since both $P|R_1$ and $Q|R_1$ has type $E \stackrel{\mathrm{def}}{=} C_1 \otimes (A \odot \overline{A}) \otimes C_2'$ for which $\mathsf{tamp}(\tau) \not\sqsubseteq s$ for each τ in E, we have $(\boldsymbol{\nu}\, \vec{y})(P'|R_1')\mathcal{R}Q|R_1$ so that the resulting pair are again in the $|$-closure of $\mathcal{R}$.
2. If $P|R \longrightarrow P|R_1|R_2'$, then $Q|R$ simulates this by $Q|R \longrightarrow Q|R_1|R_2'$, which is again in the $|$-closure of $\mathcal{R}$.

This concludes the proof of reduction-closure. The convergence is established by the same reasoning. By context lemma for state we are done. ■

References

[1] Honda, K. and Yoshida, N. A Uniform Type Structure for Secure Information Flow. Typescript, 72 pages, 2002.

[2] Yoshida, N., Type-Based Liveness Guarantee in the Presence of Nontermination and Nondeterminism, April 2002. MCS Technical Report, 2002-20, University of Leicester. Available at www.mcs.le.ac.uk/~yoshida.