Addendum to a Uniform Type Structure for Secure Information Flow (Subject Reduction with Inflation)

KOHEI HONDA
Queen Mary, University of London
and
NOBUKO YOSHIDA
Imperial College of Science, Technology and Medicine, University of London.

---

1. INTRODUCTION AND PRELIMINARIES

We here present the outline of the proof of subject reduction for the secure typing with inflation in the linear/affine π-calculus (π^{LA}). Before going into technical discussions, two points are worth noting.

—The inflation typing uses $\equiv$, which makes the reasoning difficult: however the use of labelled transition relation makes inductive reasoning possible.

—In fact the subject reduction is *not* an indispensable property of the secrecy typing, either with or without inflation and/or state. This is because the proof of noninterference reduces the secrecy typing into flow security: this flow security directly implies non-interference, hence the secrecy typing does not need such properties as the closure under reduction.

In spite of the second point, the proof has interest as an analysis of the structure of secrecy typing with inflation. For brevity we shall be only concerned with the calculus with unary, affine interaction (the cases for linear and/or branching prefixes are treated precisely by the same logic). The basic secrecy typing is given as:

$$\text{(Zero)}\ \frac{-}{\vdash \mathbf{0} \triangleright _}
\qquad
\text{(Par)}\ \frac{\vdash P_i \triangleright A_i \quad (i=1,2) \qquad A_1 \asymp A_2}{\vdash P_1|P_2 \triangleright A_1 \odot A_2}
\qquad
\text{(Res)}\ \frac{\vdash P \triangleright x:\tau,\ A \qquad \mathsf{md}(\tau) \in \mathcal{M}_{!} \cup \{\updownarrow\}}{\vdash (\boldsymbol{\nu}\, x)P \triangleright A}
\qquad
\text{(Weak)}\ \frac{\vdash P \triangleright A^{\text{-}x} \qquad \mathsf{md}(\tau) \in \mathcal{M}_{?} \cup \{\updownarrow\}}{\vdash P \triangleright x:\tau,\ A}$$

$$\text{(In}^{\downarrow_{\mathrm{A}}}\text{)}\ \boxed{s \sqsubseteq \mathsf{tamp}(A)}\ \frac{\vdash P \triangleright \vec{y}:\vec{\tau},\ \uparrow_{\mathrm{A}}?A^{\text{-}x}}{\vdash x(\vec{y}).P \triangleright x:(\vec{\tau})^{\downarrow_{\mathrm{A}}}_{s}, A}
\qquad
\text{(Out}^{\uparrow_{\mathrm{A}}}\text{)}\ \frac{\vdash P \triangleright \vec{y}:\vec{\tau}, ?A}{\vdash \overline{x}(\vec{y})P \triangleright x:(\vec{\tau})^{\uparrow_{\mathrm{A}}}_{s}, A}$$

$$\text{(In}^{!_{\mathrm{A}}}\text{)}\ \frac{\vdash P \triangleright \vec{y}:\vec{\tau},\ z:\rho,\ ?A^{\text{-}x}}{\vdash !\,x(\vec{y}z).P \triangleright x:(\vec{\tau})^{!_{\mathrm{A}}}, A}
\qquad
\text{(Out}^{?_{\mathrm{A}}}\text{)}\ \frac{\vdash P \triangleright \vec{y}:\vec{\tau},\ z:\rho,\ x:(\vec{\tau}\rho)^{?_{\mathrm{A}}}, \uparrow_{\mathrm{A}}?A}{\vdash \overline{x}(\vec{y}z)P \triangleright x:(\vec{\tau}\rho)^{?_{\mathrm{A}}},\ A}$$

Note we use a restricted form of output prefix typing. There is no loss of generality since up to $\equiv$ we obtain the original rules. The condition in the grey box in $(\mathrm{In}^{\downarrow_A})$ is the only addition from the non-secrecy typing.

To the basic typing, we add the inflation rules.

$$(\mathsf{Inf})\ \frac{\vdash_{\mathsf{sec}} P \triangleright \mathsf{inf}(A)}{\vdash_{\mathsf{sec}} P \triangleright A} \qquad (\mathsf{Str})\ \frac{\vdash_{\mathsf{sec}} P \triangleright A \quad P \equiv Q}{\vdash_{\mathsf{sec}} Q \triangleright A}$$

where we set $\mathsf{inf}(A) \stackrel{\text{def}}{=} A \sqcup \mathsf{tamp}(A)$. Without (Str), the rule is not closed under $\equiv$, so is not closed under $\longrightarrow$ either.

In the proof of the subject reduction, we shall be using the labelled transition. First, the untyped transition is given as follows.

$$(\mathsf{In})\ \frac{-}{x(\vec{y}).P \xrightarrow{x(\vec{y})} P}$$

$$(\mathsf{Rep})\ \frac{-}{!x(\vec{y}z).P \xrightarrow{x(\vec{y}z)} !x(\vec{y}z).P|P}$$

$$(\mathsf{Out})\ \frac{-}{\overline{x}(\vec{y})P \xrightarrow{\overline{x}(\vec{y})} P}$$

$$(\mathsf{Par})\ \frac{P \xrightarrow{l} P' \quad \mathsf{bn}(l) \cap \mathsf{fn}(Q) = \emptyset}{P|Q \xrightarrow{l} P'|Q}$$

$$(\mathsf{Res})\ \frac{P \xrightarrow{l} P' \quad \notin \mathsf{n}(l)}{(\boldsymbol{\nu}\, x)P \xrightarrow{l} (\boldsymbol{\nu}\, x)P'}$$

$$(\mathsf{Com})\ \frac{P \xrightarrow{l} P' \quad Q \xrightarrow{\overline{l}} Q'}{P|Q \xrightarrow{\tau} (\boldsymbol{\nu}\, \mathsf{bn}(l))(P'|Q')}$$

The induced transition is untyped: for typed processes, (apart from assuming processes in the antecedent and the left-hand processes in the conclusion are well-typed) we assume, in (Par), assuming $\vdash P \triangleright A$ and $\vdash Q \triangleright B$ with $A \asymp B$:

> *Either $l \neq \tau$ or, if not, if l is input (resp. output) then* $\mathsf{sbj}(l)$ *should be input (resp. output) in $A \odot B$.*

That is, the action to be done should follow the polarity in the type of the composite process.

2. PROOF

2.1 Main Results

The purpose of the rest of this addendum is to establish:

Proposition 2.1 *If $\vdash P \triangleright A$ and $P \longrightarrow P'$ then $\vdash P' \triangleright A$.*

To show Proposition 2.1, it suffices to prove:

Proposition 2.2 (main result) *If $\vdash P \triangleright A$ without using (Str) and $P \xrightarrow{\tau} P'$ then $\vdash P' \triangleright A$.*

because:

Lemma 2.3 $\longrightarrow\ =\ \stackrel{\tau}{\longrightarrow}\equiv$

Proof. Standard. $\Box$

and because:

Lemma 2.4 *If* $\vdash P \triangleright A$ *then* $\vdash P_0 \triangleright A$ *without using (Str) for some* $P_0 \equiv P$.

Proof. Since, for each rule, say (Some), we can always permute the sequence of application "(Str)(Some)" to "(Some)(Str)" (in the case of (Par) and (Com) we combine the use of (Str) for each sequent in the antecedent into one). $\Box$

Proposition 2.2 is much more tractable than Proposition 2.1 since both $\stackrel{l}{\longrightarrow}$ and the typing without (Str) follows the structure of syntax.

2.2 Proof of Proposition 2.2

For the proof of Proposition 2.2, we first note:

Lemma 2.5 (Inf permutation)

(1) *The use of (Inf) immediately before some rule can always be rolled forward, except for (Par) and (Out*$^{\uparrow_{\mathrm{A}}}$*).*

(2) *The use of (Inf) immediately after some rule can always be rolled back, except for (Zero), (Res), (Par) and (Out*$^{\uparrow_{\mathrm{A}}}$*),*

Proof. (1) is because, in all rules except for (Par) and (Out$^{\uparrow_{\mathrm{A}}}$), the tamper level of the process in conclusion is ensured to be the same as, or higher than, the process(es) in the antecedent. (2) is because, in all rules except for (Res), (Par) and (Out$^{\uparrow_{\mathrm{A}}}$), the tamper level of the process in conclusion is ensured to be the same as, or lower than, the process(es) in the antecedent. $\Box$

Further the application of (Weak) can always be rolled back to just after (Zero), the only axiom. We can thus safely assume, for each process which is typed:

—$x(\vec{y}).P$ is inferred by (In$^{\downarrow_{\mathrm{A}}}$).
—$\overline{x}(\vec{y})P$ is inferred by either (Out$^{\uparrow_{\mathrm{A}}}$) or (Inf).
—$!x(\vec{y}).P$ is inferred by (In$^{!_{\mathrm{A}}}$).
—$\overline{x}(\vec{y}z)P$ with x of mode $?_{\mathrm{A}}$ is inferred by (Out$^{?_{\mathrm{A}}}$).

Under these assumptions, we now inspect each generating transition rule.

Lemma 2.6 (affine input) *Let* $\vdash x(\vec{y}).P \triangleright x : (\vec{\tau})^{\downarrow_{\mathrm{A}}}_{s}, A$ *and* $x(\vec{y}).P \stackrel{x(\vec{y})}{\longrightarrow} P$. *Then* $\vdash P \triangleright \vec{y}:\vec{\tau}\,,\ \uparrow_{\mathrm{A}}?A^{-x}$.

Proof. Immediate. $\Box$

Lemma 2.7 (affine output)

(1) *Let* $\vdash \overline{x}(\vec{y})P \triangleright x:(\vec{\tau})^{\uparrow_{\mathrm{A}}}_{s}, A$ *by the application of (Out*$^{\uparrow_{\mathrm{A}}}$*). Then* $\vdash P \triangleright \vec{y}:\vec{\tau}, ?A$.

(2) Let $\vdash \overline{x}(\vec{y})P \triangleright x:(\vec{\tau})^{\uparrow_{\mathrm{A}}}_{s}, A$ *by the application of (Inf), with* $s \sqsupseteq \mathsf{tamp}(\vec{\tau})$*. Then* $\vdash P \triangleright \vec{y}:\vec{\tau} \sqcup s, ?A \sqcup s$*.*

Proof. Both are easy induction. □

Lemma 2.8 (replication) *Let* $\vdash x(\vec{y}).P \triangleright x:(\vec{\tau})^{!_{\mathrm{A}}},\ A$ *and* $!x(\vec{y}).P \xrightarrow{x(\vec{y})} !x(\vec{y}).P|P$*. Then* $\vdash P \triangleright \vec{y}:\vec{\tau},\ ?A^{-x}$*, hence* $\vdash !x(\vec{y}).P \xrightarrow{x(\vec{y})} |P \triangleright \vec{y}:\vec{\tau}, x:(\vec{\tau})^{!_{\mathrm{A}}},\ A$*.*

Proof. Immediate. □

Lemma 2.9 (replicated output) *Let* $\vdash \overline{x}(\vec{y})P \triangleright x:(\vec{\tau}\rho)^{?}, A$*. Then* $\vdash P \triangleright \vec{y}:\vec{\tau}, x:(\vec{\tau})^{?_{\mathrm{A}}}, \uparrow_{\mathrm{A}}?A$*.*

We note one basic property of inflated secure typing.

Lemma 2.10 *If* $\vdash P \triangleright A$ *then* $\vdash P \triangleright A \sqcup s$ *for arbitrary* s*.*

Proof. By rule induction on the typing rules. □

We can now prove:

Lemma 2.11 (affine communication) *Let* $P|Q \xrightarrow{\tau} (\boldsymbol{\nu}\,\vec{y})(P'|Q')$ *from* $P \xrightarrow{x(\vec{y})} P'$ *and* $Q \xrightarrow{\overline{x}(\vec{y})} Q'$ *where* x *is typed affine. Then if* $\vdash P|Q \triangleright E$ *without using (Str) then* $\vdash (\boldsymbol{\nu}\,\vec{y})(P'|Q') \triangleright E$*.*

Proof. First we can set, for reduction contexts C_P and C_Q: $P \stackrel{\text{def}}{=} C_P[x(\vec{y}).P']$ and $Q \stackrel{\text{def}}{=} C_Q[\overline{x}(\vec{y})Q']$. Assume further we have $\vdash P \triangleright A, x:\tau^{\downarrow_{\mathrm{A}}}$ and $\vdash Q \triangleright B, x:\overline{\tau}^{\uparrow_{\mathrm{A}}}$ such that $E = A \odot B, x:\updownarrow$, and let $s = \mathsf{tamp}(\overline{\tau})$ (the case when the last rule is (Inf) is essentially the same). Let R be:

$$R \stackrel{\text{def}}{=} C_P[(\boldsymbol{\nu}\,\vec{y})(P' \,|\, Q')] \,|\, C_Q[\mathbf{0}]$$

Let $\vdash x(\vec{y}).P' \triangleright A', C', x:\tau$ and $\vdash \overline{x}(\vec{y})Q' \triangleright B', C', x:\overline{\tau}$ in the derivation for P and Q, respectively, with $\mathsf{fn}(A') \cap \mathsf{fn}(B') = \emptyset$. By Lemmas 2.6 and 2.7 and applying Lemma 2.10, we can infer:

$$\vdash P' \triangleright A', C, \vec{y}:\vec{\rho}, \qquad\qquad \vdash Q' \triangleright ?_{\mathrm{A}}(B', C') \sqcup s,\ \ (\vec{y}:\overline{\vec{\rho}}) \sqcup s,$$

Since $\mathsf{tamp}(A') \sqsupseteq s$, we also have $\vdash P' \triangleright A',\ C' \sqcup s,\ (\vec{y}:\vec{\rho}) \sqcup s$. Noting the tampering levels of all these types do not exceed s, we obtain:

$$\vdash (\boldsymbol{\nu}\,\vec{y})(P' \,|\, Q') \triangleright A', C', ?B'$$

so that we conclude:

$$\vdash C_P[(\boldsymbol{\nu}\,\vec{y})(P' \,|\, Q')] \triangleright A. \tag{1}$$

Noting $\vdash \mathbf{0} \triangleright C$ and $\mathsf{tamp}(\tau, C) \sqsubseteq \mathsf{tamp}(C)$, we have

$$\vdash C_Q[\mathbf{0}] \triangleright B. \tag{2}$$

By (1) and (2), we obtain $\vdash R \triangleright E, x:\updownarrow$. Noting $R \equiv (\boldsymbol{\nu}\,\vec{y})(P'|Q')$ we are done. □

Lemma 2.12 (replicated communication) *Let* $P|Q \xrightarrow{\tau} (\boldsymbol{\nu}\,\vec{y})(P'|Q')$ *from* $P \xrightarrow{x(\vec{y}z)} P'$ *and* $Q \xrightarrow{\overline{x}(\vec{y}z)} Q'$ *where* x *is replicated. Then if* $\vdash P|Q \triangleright E$ *without using (Str) then* $\vdash (\boldsymbol{\nu}\,\vec{y}z)(P'|Q') \triangleright E$.

PROOF. As before, we set, for reduction contexts C_P and C_Q: $P \stackrel{\text{def}}{=} C_P[!x(\vec{y}z).P']$ and $Q \stackrel{\text{def}}{=} C_Q[\overline{x}(\vec{y}z)Q']$. Assume further we have $\vdash P \triangleright A, x:\tau^{!_A}$ and $\vdash Q \triangleright B, x:\overline{\tau}^{?_A}$ such that $E = A \odot B, x:\tau$. Let R be:

$$R \stackrel{\text{def}}{=} C_P[!x(\vec{y}z).P'] \mid C_Q[(\boldsymbol{\nu}\,\vec{y}z)(P' \mid Q')]$$

Let $\vdash !x(\vec{y}z).P' \triangleright A'$ and $\vdash \overline{x}(\vec{y}z)Q' \triangleright B'$ in the derivation for P and Q, respectively. By Lemmas 2.8 and 2.9, we know

$$\vdash C_P[(\boldsymbol{\nu}\,\vec{y}z)(P' \mid Q')] \triangleright B'$$

Hence we have $\vdash R \triangleright E, x:\tau$. Noting $R \equiv (\boldsymbol{\nu}\,\vec{y}z)(P'|Q')$ we are done. $\square$