Static Analysis for the $\pi$-Calculus with Applications to Security

Chiara Bodei and Pierpaolo Degano
Dipartimento di Informatica, Università di Pisa, Corso Italia, 40, I-56125 Pisa, Italy
E-mail: [chiara, degano]@di.unipi.it

and

Flemming Nielson and Hanne Riis Nielson
Informatics and Mathematicse Modelling, The Technical University of Denmark, Richard Petersens Plads, blg 321, DK 2800 Kongens Lyngby, Denmark
E-mail: nielson@imm.dtu.dk, riis@imm.dtu.dk

October 14, 1998; received January 15, 2000

Control Flow Analysis is a static technique for predicting safe and computable approximations to the set of values that the objects of a program may assume during its execution. We present an analysis for the $\pi$-calculus that shows how names will be bound to actual channels at run time. The result of our analysis establishes a super-set of the set of channels to which a given name may be bound and of the set of channels that may be sent along a given channel. Besides a set of rules that permits one to validate a given solution, we also offer a constructive procedure that builds solutions in low polynomial time. Applications of our analysis include establishing two simple security properties of processes. One example is that $P$ has no leaks: $P$ offers communication to the external environment through public channels only and confines its secret channels within itself. The other example is connected to the no read-up/no write-down property of Bell and LaPadula: once processes are given levels of security clearance, we check that a process at a high level never sends channels to processes at a lower level.

1. INTRODUCTION

Program analysis aims at verifying properties of a program that hold in all executions—regardless of the actual data upon which the program operates and regardless of the specific environment in which it executes. Traditionally, program analysis has been used in compilers for “optimizing” the implementation of programming languages. More recently, program analysis has been used for validating security and safety issues for concurrent and distributed systems.

Program analysis provides automatic and decidable methods for analysing properties of programs. Since most properties implicitly involve questions about termination, the methods are intended to “err on the safe side.” For each analysis an ordering is imposed on the properties, for example stipulating that a property is larger than another if more values satisfy the former than the latter. The properties are then interpreted in such a way that an analysis remains correct even when it produces a larger property than ideally possible. This corresponds to producing a valid inference in a program logic for partial correctness. However, program analysis is generally more efficient than program verification, and for that reason more approximate, because the focus is on the fully automatic processing of large programs.

We wish to study these issues for concurrent languages. To investigate them in a pure form we shall use the $\pi$-calculus which is a model of concurrent communicating processes based on name passing. Names may represent both data and channels that processes exchange. For example, if $a$ is the name of a link to some information on the web home page of a user, then another user can access this information through $a$, by performing a communication. We propose in Section 3 a Control Flow Analysis for the $\pi$-calculus that requires only minor additions to the syntax: assigning explicit “channels” to the names occurring in restrictions and assigning explicit “binders” to the names occurring in input prefixes. This may be compared to the approach of [41], where processes are required to be on a special form. Roughly, channels can be seen as representatives of semantic values that names may have, and binders as the
actual placeholders in input prefixes. We review in Section 2 the syntax and the early semantics of the \(\pi\)-calculus, and we introduce our annotations.

The result of our control flow analysis establishes a super-set of the set of channels to which a given name may be bound and of the set of channels that may be sent along a given channel. These super-sets give rise to solutions \((\rho, \kappa)\) and we formulate the control flow analysis as a specification of the correctness of a candidate solution. This takes the form of a Flow Logic with judgements \((\rho, \kappa) \models_{\text{me}} P\) (where \(\text{me}\) is an auxiliary function that associates channels or binders with the free names of the process \(P\)), and a set of clauses that operate on them. We show that best solutions always exist and we establish the semantic correctness of solutions in the form of a subject-reduction result. In Section 4 we then present a procedure that generates solutions by inducing on the structure of processes, and operates in \(O(N^3)\) time with respect to the size \(N\) of the process under analysis.

We apply our analysis for statically checking two simple security properties. The first property is in Section 5 and considers channels as divided into "secret" and "public" channels. Then, the dynamic security requirement is that secret information may only be communicated over secret channels; in other words, a process has no leaks of secret information. With simple checks on a solution, we obtain a static test (called confinement) for a given process having no leaks, and we prove it safe with respect to the dynamic notion (called no leaks).

The second property presented in Section 6 is the simple security property ("no read-up/no write-down") of Bell and LaPadula [5]. Processes are given levels of security clearance, and the dynamic property demands that those at high level never send information to those at low level, while communication in any other direction is permitted. A little extension to our machinery is sufficient to define a static check (called discreetness) for when a process respects the classification hierarchy, and to prove it safe with respect to the dynamic notion (called nru/nwd).

Finally, we briefly discuss in Section 7 some related work on static analysis and security properties, and in Section 8 we discuss some other uses of control flow analysis for concurrent processes.

2. THE \(\pi\)-CALCULUS

Syntax

In this section we briefly recall the \(\pi\)-calculus [29], a model of concurrent communicating processes based on the notion of name passing.

**Definition 2.1.** Let \(\mathcal{N}\) be an infinite set of names ranged over by \(a, b, \ldots, x, y, \ldots\) and let \(\tau\) be a distinguished element such that \(\mathcal{N} \cap \{\tau\} = \emptyset\). Processes are built from names according to the syntax

\[
P :: \emptyset \mid \mu.P \mid P + P \mid P \mid (\nu x)P \mid [x = y]P \mid !P,
\]

where \(\mu\) may either be \(x(y)\) for input, or \(\bar{x}y\) for output or \(\tau\) for silent moves. Hereafter, the trailing \(\emptyset\) will be omitted (i.e., we write \(\mu\) instead of \(\mu.\emptyset\)). We assume that + has lower precedence than \(\mid\) which again has lower precedence than the other operators.

The prefix \(\mu\) is the first atomic action that the process \(\mu.P\) can perform. The input prefix \(x(y)\) binds the name \(y\) in the prefixed process. Intuitively, some name \(y\) is received along the link named \(x\). The output prefix \(\bar{x}y\) does not bind the name \(y\) which is sent along \(x\). The silent prefix \(\tau\) denotes an action which is invisible to an external observer of the system. Summation denotes nondeterministic choice, so \(P + Q\) behaves either as \(P\) or as \(Q\). The operator \(\mid\) describes parallel composition of processes. Intuitively, \(P\) and \(Q\) in \(P \mid Q\) act independently and can also communicate when one performs an input and the other an output on the same common link. The restriction operator \((\nu x)P\) acts as a declaration for the name \(x\) in the process \(P\) that it prefixes. In other words, \(x\) is a unique name in \(P\) which is different from all the external names. The agent \((\nu x)P\) behaves as \(P\) except that sending and receiving along \(\bar{x}\) and \(x\) is blocked. A distinguished feature of the \(\pi\)-calculus is to allow for an enlargement of the scope of a restriction; we will expand on this below. Matching \([x = y]P\) is an if–then operator: process \(P\) is activated if \(x = y\). Finally, replication \(!P\) behaves as \(P[P] \cdots\) as many times as needed.
The formulation of our analysis requires only a minor extension to the syntax of the \( \pi \)-calculus, namely annotating the binding occurrences of names within restrictions with “channels” \( \chi \), and the binding occurrences of names within input prefixes with “binders” \( \beta \). These syntactic extensions are needed because of the \( \alpha \)-conversion allowed by the structural congruence. They do not affect the dynamic semantics of the \( \pi \)-calculus; however, they heavily influence the way in which our static analysis of Section 3 operates. From the point of view of the analysis, annotations place all the names of a process in a finite set of equivalence classes. Through them, the analysis computes (a super-set of) the actual links that a name can denote.

**Definition 2.2.** Let \( B \) be a nonempty set of binders ranged over by \( \beta, \beta', \ldots; \) and let \( C \) be a nonempty set of channels ranged over by \( \chi, \chi', \ldots \) such that \( B \cap C = \emptyset \); moreover call \( B \cup C \) the set of markers. Then (annotated) processes, denoted by \( P, P_1, P_2, Q, R, \ldots \in \text{Proc} \) are built as in Definition 2.1, where the (annotated) input prefix \( xy^\beta \) replaces \( x(y) \) and the (annotated) restriction \( (vx^{xy})P \) replaces \( (vx)(y)P \).

**Semantics**

The \( \pi \)-calculus can be equipped with an early as well as a late semantics; in this paper we consider the *early* operational semantics defined in SOS style, because it is emerging as a standard for transitional semantics and appears to be more suitable for the security issues studied in the next sections. We follow [30], in particular for the distinction between free and bound input.

The labels of transitions are \( \tau \) for silent actions, \( xy \) for free input, \( \bar{x}y \) for free output, \( x(y^\beta) \) for bound input and \( \bar{x}(y^\beta) \) for bound output. Roughly speaking, the effect of a bound output is moving a \( (vx^\beta) \) operator from a process to a label, as in \( Q = (vy^\beta)x^\beta y^\beta.P \xrightarrow{\beta(y^\beta)} P \). The intuition behind this operation is to make the name \( y \), which is private to \( Q \), available to the external environment. The bound output then enlarges the scope of the declaration, and for this reason it is sometimes referred to as *scope extrusion* in the literature. When coupled with a bound input \( x(y^\beta) \), the extrusion originates a communication and reestablishes the removed restriction.

As usual, we will use \( \mu \) as a metavariable for the labels of transitions (although it is formally distinct from the metavariable for prefixes with which it has a few cases in common). We recall the notion of free names \( fn(\mu) \), bound names \( bn(\mu) \), and names \( n(\mu) = fn(\mu) \cup bn(\mu) \) of a label \( \mu \). The *subject* of an input or output action is the channel \( (x) \) used for the communication and the *object* is the entity \( (y) \) being transmitted.

<table>
<thead>
<tr>
<th>Kind</th>
<th>( \mu )</th>
<th>( fn(\mu) )</th>
<th>( bn(\mu) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Silent move</td>
<td>( \tau )</td>
<td>\emptyset</td>
<td>\emptyset</td>
</tr>
<tr>
<td>Free input and output</td>
<td>( xy, \bar{x}y )</td>
<td>{x, y}</td>
<td>\emptyset</td>
</tr>
<tr>
<td>Bound input and output</td>
<td>( x(y^\beta), \bar{x}(y^\beta) )</td>
<td>{x}</td>
<td>{y}</td>
</tr>
</tbody>
</table>

Functions \( fn \) and \( n \) are extended in the obvious way to processes.

**Congruence**

Below we shall need the *structural congruence* \( \equiv \) on processes, defined as in [30] to be the least congruence satisfying:

- if \( P \) and \( Q \) are \( \alpha \)-equivalent \( (P = \alpha Q) \) then \( P \equiv Q \); to be more precise: \( (vx^\beta)P \equiv (vy^\beta)(P[y/x]) \) if \( y \notin fn((vx^\beta)P) \), and \( x(y^\beta)P \equiv x(z^\beta)(P[z/y]) \) if \( z \notin fn(x(y^\beta)P) \);
- \( \text{Proc}_{+} \) and \( \text{Proc}_{-} \) are commutative monoids;
- \( (vx^\beta)(vy^\beta)P \equiv (vy^\beta)(vx^\beta)P \), if \( x \neq y \), \( (vx^\beta)(P_1 \parallel P_2) \equiv (vx^\beta)P_1 \parallel P_2 \) if \( x \notin fn(P_2) \), and \( (vx^\beta)P \equiv P \) if \( x \notin fn(P) \);
- \( !P \equiv P \parallel !P \).
Early Transition System for the $\pi$-Calculus

\[
\begin{array}{ll}
\text{Tauc: } \tau \cdot P \xrightarrow{\tau} P & \text{Out: } \vec{x} y \cdot P \xrightarrow{\vec{y}} P \\
\text{Freeleq: } x(y^\theta) \cdot P \xrightarrow{x\alpha} P \sub{w/y} & \text{Bound In: } x(y^\theta) \cdot P \xrightarrow{\alpha} P \\
\text{Par: } P_1 \parallel P_2 \xrightarrow{\mu} Q_1, \text{ free}(P_1) \cap \text{ free}(P_2) = \emptyset & \text{Sum: } P_1 \parallel P_2 \xrightarrow{\mu} Q_1 \parallel Q_2 \\
\text{Res: } P \xrightarrow{\pi \sigma} Q, x \notin \text{free}(\mu) & \text{Open: } P \xrightarrow{\pi \sigma} Q, y \notin x \\
\text{Close: } P \xrightarrow{\mu} Q & \text{Match: } P \xrightarrow{\mu} Q \stackrel{\pi x} \xrightarrow{\sigma} Q \\
\text{Var: } P = P \xrightarrow{\pi} Q = Q' & \text{Com: } P \xrightarrow{\mu} Q \stackrel{\pi x} \xrightarrow{\sigma} Q ' \\
\end{array}
\]

Note that $\alpha$-conversions do not affect markers. Also, we permit exchange restrictions only when the restricted names are different, because otherwise $(x\pi x)P \equiv (x\pi x)P$ and the marker then loses its identity.

Table 1 shows the (annotated) early transition system of the $\pi$-calculus defined in SOS style.

A different treatment of matching is presented in [7]. There, the structural congruence law $[x = x]P \equiv P$ is assumed and the transitional rule Match is removed from Table 1. This latter change requires an accurate handling of free names, otherwise applying the congruence rule from right to left may introduce new free names ad libitum. The need of handling similar kinds of low level details is a recurrent problem in congruence-based semantics, and in [7] we illustrate one of the techniques needed to deal with them.

We conclude this section with a straightforward fact that will be repeatedly used in the proofs later on.

**Fact 2.3.** If $P \xrightarrow{\mu} Q$ then

1. If $\mu = \tau$ then $\text{free}(P) \supseteq \text{free}(Q)$.
2. If $\mu = \vec{x} y$ then $\text{free}(P) \supseteq \{x, y\} \cup \text{free}(Q)$.
3. If $\mu = \vec{x}(\pi x)$, $xy, x(\pi x)$ then $\text{free}(P) \supseteq \{x\} \cup (\text{free}(Q) \setminus \{y\})$.

3. CONTROL FLOW ANALYSIS

The result of analysing a process $P$ is a pair $(\rho, \kappa)$. The first component, $\rho$, is an abstract environment which gives information about the set of channels to which names can be bound; the second component, $\kappa$, is an abstract channel environment which gives information about the set of channels that can flow over given channels.

One way to view the pair $(\rho, \kappa)$ is as a record of the actual communications taking place during it execution. Whenever a value $a_{val}$ is output on some channel $b_{chan}$, as in $b_{chan}a_{val}$, it must be duly recorded in the $\kappa$ component, intuitively by ensuring that $a_{val} \in \kappa(b_{chan})$. Similarly, whenever a variable $c_{var}$ inputs a value on some channel $b_{chan}$, as in $b_{chan}(c_{var})$, this must also be duly recorded in the $\rho$ component, intuitively by ensuring that $a_{val} \in \rho(c_{var})$ for all $a_{val} \in \kappa(b_{chan})$.

We now make this more precise (also paying attention to an additional marker environment $me$ for associating names with markers).

### 3.1. Validation

To validate the correctness of a proposed solution $(\rho, \kappa)$ we state a set of clauses operating upon judgments of the form:

$$(\rho, \kappa) \models me P$$

The purpose of $me$, $\rho$, and $\kappa$ is clarified by:
• \( me : \mathcal{N} \rightarrow (\mathcal{B} \cup \mathcal{C}) \) is the marker environment that maps a name (in particular the free names of a process) to the appropriate channel or binder used when the name was introduced; so \( me(x) \) will be the marker (in \( \mathcal{B} \) or \( \mathcal{C} \)) where the current name \( x \) is bound.

• \( \rho : \mathcal{B} \rightarrow \varphi(\mathcal{C}) \) is the abstract environment that maps a binder to the set of channels that it can be bound to; more precisely, \( \rho(\beta) \) must include the set of channels that \( \beta \) could evaluate to. We shall allow one to regard the abstract environment as a function \( \rho : (\mathcal{B} \cup \mathcal{C}) \rightarrow \varphi(\mathcal{C}) \) by setting \( \forall \chi \in \mathcal{C} : \rho(\chi) = \{ \chi \} \).

We write \( \bot \) for the function that maps everything to \( \emptyset \). However, we continue to assume that \( \forall \chi \in \mathcal{C} : \bot(\chi) = \{ \chi \} \).

• \( \kappa : \mathcal{C} \rightarrow \varphi(\mathcal{C}) \) is the abstract channel environment that maps a channel to the set of channels that can be communicated over it.

More precisely, \( \kappa(\chi) \) must include the set of channels that can be communicated over the channel \( \chi \). Also, here we write \( \bot \) for the function that maps everything to \( \emptyset \).

Note that we use a marker environment, because the identity of names is not preserved under \( \alpha \)-conversions (see the rule \( \text{Var} \)). Indeed, it would not suffice to “\( \alpha \)-rename the program apart” because this property is not preserved under reduction, in particular when scope extrusion is required. For example, the process \( (v a^x)(a(y)^\beta).a(c^\beta).z \mid !(v x^x)\bar{a}x \) performs a first communication, then \( \alpha \)-converts the name \( x \) to perform a second communication and becomes \( (v a^x)(v w^x)(v w^x)(\bar{e}w \mid !(v x^x)\bar{a}x) \).

A further comment on annotations may clarify their subsequent use. A typical schema for annotating each element of \( \mathcal{B} \) \( \text{proc} \) require that the components are validated, apart from the one for matching. Moreover, the input demands that the set of channels that can pass along \( x \) includes the channels to which \( \emptyset \) can evaluate. In the clause for restriction, we can simply update the marker environment as \( me(x \mapsto \chi) \) because \( \rho(\chi) = \{ \chi \} \) by definition. The condition for matching says that the continuation \( P \) needs to be validated if there is at least one channel to which both \( x \) and \( y \) can evaluate.

**Example 3.1.** Consider the following process

\[
P = a(x^\beta).((v b^\beta)(v x^x)(\bar{b}a.x.\bar{b}(x^\beta).\bar{b}c + \bar{c}d.\bar{a}c) \mid b(x^\beta).\bar{b}x) \mid d(x^\beta),
\]

the marker environment \( me \) such that \( me(a) = \chi_2 \) and \( me(d) = \chi_3 \), and the pair \( (\rho, \kappa) \) defined as follows, where \( i \in \{0, 1, 2, 3, 4\} \):

\[
\begin{align*}
\rho(\beta_i) &= \begin{cases} 
\{\chi_0, \chi_1, \chi_2, \chi_3, \chi_4\} & \text{if } i = 1, 2 \\
\{\chi_1, \chi_2, \chi_3, \chi_4\} & \text{if } i = 0 \\
\{\chi_1, \chi_2, \chi_3, \chi_4\} & \text{if } i \geq 1.
\end{cases} \\
\kappa(\chi_i) &= \begin{cases} 
\{\chi_0, \chi_1, \chi_2, \chi_3, \chi_4\} & \text{if } i = 0 \\
\{\chi_1, \chi_2, \chi_3, \chi_4\} & \text{if } i \geq 1.
\end{cases}
\end{align*}
\]

**TABLE 2**

<table>
<thead>
<tr>
<th>Rule</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>( (\rho, \kappa) \models_{me} \mathbf{0} )</td>
<td>( \text{iff } \text{true} )</td>
</tr>
<tr>
<td>( (\rho, \kappa) \models_{me} \tau.P )</td>
<td>( \text{iff } (\rho, \kappa) \models_{me} P )</td>
</tr>
<tr>
<td>( (\rho, \kappa) \models_{me} \bar{a}.P )</td>
<td>( \text{iff } (\rho, \kappa) \models_{me} P \land \forall \chi \in \rho(me(x)) : \rho(me(y)) \subseteq \kappa(\chi) )</td>
</tr>
<tr>
<td>( (\rho, \kappa) \models_{me} a(x^\beta).P )</td>
<td>( \text{iff } (\rho, \kappa) \models_{me(a)} P \land \forall \chi \in \rho(me(x)) : \chi(\chi) \subseteq \rho(\beta) )</td>
</tr>
<tr>
<td>( (\rho, \kappa) \models_{me} P_1 + P_2 )</td>
<td>( \text{iff } (\rho, \kappa) \models_{me} P_1 \land (\rho, \kappa) \models_{me} P_2 )</td>
</tr>
<tr>
<td>( (\rho, \kappa) \models_{me} (v x^x)P )</td>
<td>( \text{iff } (\rho, \kappa) \models_{me(v x^x)} P )</td>
</tr>
<tr>
<td>( (\rho, \kappa) \models_{me} [x = y]P )</td>
<td>( \text{iff } (\rho, \kappa) \models_{me(x = y)} P )</td>
</tr>
<tr>
<td>( (\rho, \kappa) \models_{me} \exists x.P )</td>
<td>( \text{iff } (\rho, \kappa) \models_{me} P )</td>
</tr>
</tbody>
</table>
A simple check shows that \((\rho, \kappa) \models_{me} P\). The objects \(x\) of the inputs on channels \(a\) and \(d\) are kept distinct for the analysis, because the annotations \(\beta_0\) and \(\beta_3\) place them in two different equivalence classes (but this does not influence the dynamic semantics). The reader may have noticed that \((\rho, \kappa)\) above is not the least solution, e.g., because of the presence of \(\chi_4\). This kind of useless channel may occur in solutions, although they do appear neither in annotations nor in the image of a marker environment—nor will they occur in the solutions constructed according to Section 4 (see also Theorem 3.4).

The formulation of our control flow analysis borrows from standard ideas for functional languages. Our current formulation is insensitive to flow and context [31], so terms can be rearranged without affecting the acceptability of a candidate solution; in effect, restrictions can be lifted to the top level, or to the nearest enclosing \(!\), and prefixing of actions can be replaced by their parallel composition. While more complex flow analyses can be devised, these are not necessary for the applications to security studied here.

### 3.2. Existence of Solutions

So far we have only considered a procedure for validating whether or not a proposed solution \((\rho, \kappa)\) is in fact acceptable. We now show that there always exists a least choice of \((\rho, \kappa)\) that is acceptable in the manner of Table 2.

**Definition 3.2.** The set of proposed solutions can be partially ordered by setting \((\rho, \kappa) \subseteq (\rho', \kappa')\) iff \(\forall \beta \in B: \rho(\beta) \subseteq \rho'(\beta)\) and \(\forall \chi \in C: \kappa(\chi) \subseteq \kappa'(\chi)\).

It is immediate that this suffices for making the set of proposed solutions into a complete lattice; using standard notation we write \((\rho, \kappa) \cup (\rho', \kappa')\) for the binary least upper bound (defined pointwise), \(\cap \mathcal{J}\) for the greatest lower bound of a set \(\mathcal{J}\) of proposed solutions (also defined pointwise), and \((\bot, \bot)\) for the least element.

**Definition 3.3.** A set \(\mathcal{J}\) of proposed solutions is a Moore family if and only if it contains \(\cap \mathcal{J}\) for all \(\mathcal{J} \subseteq \mathcal{J}\) (in particular for \(\mathcal{J} = \emptyset\) and for \(\mathcal{J} = \mathcal{J}\)).

This concept plays an important role in the theory of Abstract Interpretation [11, 31]; in other branches of computer science it is sometimes called the model intersection property. When \(\mathcal{J}\) is a Moore family it contains a greatest element \((\cap \emptyset)\) as well as a least element \((\cap \mathcal{J})\). The following theorem then guarantees that there always is a least solution to the specification in Table 2 (just take \((\hat{\rho}, \hat{\kappa}) = (\bot, \bot)\) in the statement below).

**Theorem 3.4.** For all \(me\), \(P\) and \((\bar{\rho}, \bar{\kappa})\) the set

\[
\{ (\rho, \kappa) \mid (\rho, \kappa) \models_{me} P \land (\rho, \kappa) \supseteq (\bar{\rho}, \bar{\kappa}) \}
\]

is a Moore family.

**Proof.** We proceed by structural induction on \(P\) (since Table 2 is defined by structural induction on \(P\)). Let

\[
\mathcal{J} \subseteq \{ (\rho, \kappa) \mid (\rho, \kappa) \models_{m} P \land (\rho, \kappa) \supseteq (\bar{\rho}, \bar{\kappa}) \}
\]

and let \(J\) and \((\rho_j, \kappa_j)\) be given such that \(\mathcal{J} = \{ (\rho_j, \kappa_j) \mid j \in J \}\). Next define

\[
(\rho', \kappa') = \cap \mathcal{J} = \cap \{ (\rho_j, \kappa_j) \mid j \in J \}
\]

and recall that the greatest lower bound is defined pointwise and hence that \((\rho', \kappa') \supseteq (\bar{\rho}, \bar{\kappa})\). It remains to check that \((\rho', \kappa') \models_{me} P\). For this we proceed by cases on \(P\) making use of the induction hypothesis. Most cases are straightforward and here we only consider two of the more interesting cases.

**The Case** \(x(\gamma^P)\). \(P\). Since \(\forall j \in J : (\rho_j, \kappa_j) \models_{me} x(\gamma^P)\). \(P\) we have

\[
\forall j \in J : (\rho_j, \kappa_j) \models_{me [\gamma^P]} P \quad \text{and} \quad \forall j \in J : \forall \chi \in \rho_j(me)(x) : \kappa_j(\chi) \subseteq \rho_j(\beta)
\]
Using the induction hypothesis and that $\rho'$ is defined in a pointwise manner, we then obtain

\[(\rho', \kappa') \models_{me[y \mapsto \beta]} P \quad \text{and} \quad \forall x \in \rho'(me(x)) : \kappa'(x) \subseteq \rho'(\beta)\]

thus establishing the desired $(\rho', \kappa') \models_{me} x(\nu^\beta).P$.

The Case $[x = y] P$. Since $\forall j \in J : (\rho_j, \kappa_j) \models_{me} [x = y] P$ we have $\forall j \in J : (\rho_j(me(x)) \cap \rho_j(me(y)) \neq \emptyset \Rightarrow (\rho_j, \kappa_j) \models_{me} P$.

Using the induction hypothesis and the pointwise definition of $\rho'$, we then obtain

\[(\rho'(me(x)) \cap \rho'(me(y)) \neq \emptyset \Rightarrow (\rho', \kappa') \models_{me} P\]

thus establishing the desired $(\rho', \kappa') \models_{me} [x = y] P$. ■

3.3. Correctness

We state now some auxiliary results that will allow us to establish the semantic correctness of our analysis; they are all independent of the operational semantics and only rely on Table 2.

**Lemma 3.5.** Assume that $\forall x \in fn(P) : me_1(x) = me_2(x)$; then $(\rho, \kappa) \models_{me_1} P$ if and only if $(\rho, \kappa) \models_{me_2} P$.

**Proof.** A straightforward structural induction on $P$.

**Lemma 3.6.** Assume that $me(y) = me(z)$; then $(\rho, \kappa) \models_{me} P$ if and only if $(\rho, \kappa) \models_{me} P[z/y]$.

**Proof.** The proof is by induction on the size of $P$. Most cases are straightforward using the fact that $\forall x : me(x) = me(x[z/y])$. This leaves us with the cases where the marker environment is modified and here we consider only a typical case.

The Case $P = u(v^\beta).Q$. If $v = y$ the result follows from the above remarks so assume that $v \neq y$. Let $w$ be a fresh name, i.e., let $w \notin fn(Q) \cup \{z, y\}$, in case $z = v$, and let $w = v$ in case $z \neq v$; in both cases $me[w \mapsto \beta](z) = me[w \mapsto \beta](y)$. Then

\[P[z/y] = u(z/y)(w^\beta)(Q[w/v][z/y])\]

and it follows that

\[(\rho, \kappa) \models_{me} P[z/y]\]

amounts to

\[(\rho, \kappa) \models_{me[w \mapsto \beta]} Q[w/v][z/y] \quad \text{and} \quad \forall \chi \in \rho(me(u[z/y])) : \kappa(\chi) \subseteq \rho(\beta)\]

and by the induction hypothesis this amounts to

\[(\rho, \kappa) \models_{me[w \mapsto \beta]} Q[w/v] \quad \text{and} \quad \forall \chi \in \rho(me(u)) : \kappa(\chi) \subseteq \rho(\beta),\]

which by Lemma 3.5 amounts to

\[(\rho, \kappa) \models_{me[w \mapsto \beta, v \mapsto \beta]} Q[w/v] \quad \text{and} \quad \forall \chi \in \rho(me(u)) : \kappa(\chi) \subseteq \rho(\beta)\]

so that by the induction hypothesis this amounts to

\[(\rho, \kappa) \models_{me[w \mapsto \beta, v \mapsto \beta]} Q \quad \text{and} \quad \forall \chi \in \rho(me(u)) : \kappa(\chi) \subseteq \rho(\beta),\]
which by Lemma 3.5 amounts to
\[(\rho, \kappa) \models_{\text{me}[w \rightarrow \beta]} Q \quad \text{and} \quad \forall \chi \in \rho(\text{me}(u)): \kappa(\chi) \subseteq \rho(\beta),\]
which again amounts to
\[(\rho, \kappa) \models_{\text{me}} P\]
as was to be shown. ■

**Corollary 3.7.** Assume that \( z \notin \text{fn}(P) \) and \( \eta \in B \cup C \); then \( (\rho, \kappa) \models_{\text{me}[y \rightarrow \eta]} P \) if and only if \( (\rho, \kappa) \models_{\text{me}[z \rightarrow \eta]} P[z/y] \).

**Proof.** By Lemma 3.6
\[(\rho, \kappa) \models_{\text{me}[y \rightarrow \eta, z \rightarrow \eta]} P \iff (\rho, \kappa) \models_{\text{me}[y \rightarrow \eta, z \rightarrow \eta]} P[z/y]\]
and by Lemma 3.5 and \( z \notin \text{fn}(P) \)
\[(\rho, \kappa) \models_{\text{me}[y \rightarrow \eta]} P \iff (\rho, \kappa) \models_{\text{me}[z \rightarrow \eta]} P[z/y]\]
as was to be shown. ■

**Lemma 3.8.** Assume that \( P \equiv Q \); then \( (\rho, \kappa) \models_{\text{me}} P \) if \( (\rho, \kappa) \models_{\text{me}} Q \).

**Proof.** The proof is by induction on the construction of \( P \equiv Q \) and here we only consider the two harder cases.

**The Case of \( \alpha \)-Equivalence.** Consider the subcase \((\nu x^x)P \equiv (\nu y^x)(P[y/x])\) where \( y \notin \text{fn}((\nu x^x)P) \). We calculate that
\[(\rho, \kappa) \models_{\text{me}} (\nu x^x)P\]
is equivalent to
\[(\rho, \kappa) \models_{\text{me}[x \rightarrow \chi]} P,\]
which by Corollary 3.7 is equivalent to
\[(\rho, \kappa) \models_{\text{me}[y \rightarrow \chi]} P[y/x]\]
(since either \( y \notin \text{fn}(P) \) or \( y = x \)), which is equivalent to
\[(\rho, \kappa) \models_{\text{me}} (\nu y^x)(P[y/x])\]
as was to be shown. The other subcase is similar.

**The Cases.** \((\nu x^x)(P_1 | P_2) \equiv (\nu x^x)P_1 | P_2 \) (if \( x \notin \text{fn}(P_2) \)) and \((\nu x^x)P \equiv (\nu x^x)(\nu y^x)P \) (if \( x \neq y \)) are easy consequences of Lemma 3.5 and the case \((\nu x^x)(\nu y^x)P \equiv (\nu y^x)(\nu x^x)P \) (if \( x \neq y \)) is straightforward. ■

**Lemma 3.9.** Assume that \( (\rho, \kappa) \models_{\text{me}} P \) and \( \text{me}(w) \in \rho(\text{me}(z)) \); then \( (\rho, \kappa) \models_{\text{me}} P[w/z] \).

**Proof.** The proof is by structural induction on \( P \). Most cases are straightforward using the fact
\[\forall x: \rho(\text{me}(x[w/z])) \subseteq \rho(\text{me}(x)).\]
Here we only consider the two harder cases.
The Case $P = u(v^\beta).Q$. By Lemma 3.8 (since $\alpha$-equivalence is part of the structural congruence) we may without loss of generality assume that $v$ is neither $w$ nor $z$. Then we may calculate that

$$(\rho, \kappa) \models_{me} u(v^\beta).Q$$

amounts to

$$(\rho, \kappa) \models_{me[v\mapsto\beta]} Q \quad \text{and} \quad \forall \chi \in \rho(me(u)) : \kappa(\chi) \subseteq \rho(\beta),$$

which, by the induction hypothesis and the fact stated above, imply that

$$(\rho, \kappa) \models_{me[v\mapsto\beta]} Q[w/z] \quad \text{and} \quad \forall \chi \in \rho(me(u[w/z])) : \kappa(\chi) \subseteq \rho(\beta),$$

which is equivalent to the required

$$(\rho, \kappa) \models_{me} (u(v^\beta)).Q[w/z].$$

The Case $P = [x = y].Q$. Our assumption $(\rho, \kappa) \models_{me} P$ amounts to

$$(\rho(me(x)) \cap \rho(me(y))) \neq \emptyset \Rightarrow (\rho, \kappa) \models_{me} Q$$

and our goal is to show

$$\rho(me(x[w/z])) \cap \rho(me(y[w/z])) \neq \emptyset \Rightarrow (\rho, \kappa) \models_{me} Q[w/z]$$

as this amounts to $(\rho, \kappa) \models_{me} P[w/z]$. By the induction hypothesis it suffices to show that

$$\rho(me(x[w/z])) \cap \rho(me(y[w/z])) \neq \emptyset \Rightarrow \rho(me(x)) \cap \rho(me(y)) \neq \emptyset$$

that is immediate using the fact stated at the beginning of the proof. □

Subject Reduction

To establish the semantic correctness of our analysis we rely on the definition of the early semantics in Table 1 as well as on the analysis in Table 2. The subject reduction result below applies to all the solutions of the analysis and hence in particular to the least. The operational semantics only rewrites processes at “top level” where it is natural to demand that all free names are bound to channels (rather than to binders); this is formalised by the condition $me[\text{fin}(-)] \subseteq \mathcal{C}$. In the statement below, we write $(\rho, \kappa) \models_{me}^C P$ as a shorthand for $(\rho, \kappa) \models_{me} P \land me[\text{fin}(P)] \subseteq \mathcal{C}$.

**Theorem 3.10.** If $(\rho, \kappa) \models_{me}^C P$ and $P \xrightarrow{\mu} Q$ we have:

1. If $\mu = \tau$ then $(\rho, \kappa) \models_{me} Q$;
2. If $\mu = \tilde{x}y$ then $(\rho, \kappa) \models_{me}^C Q$, and me(y) $\in \kappa(me(x))$;
3. If $\mu = \tilde{x}(y^\chi)$ then $(\rho, \kappa) \models_{me[y\mapsto\chi]}^C Q$, and $\chi \in \kappa(me(x))$;
4. If $\mu = xy$ and me(y) $\in \kappa(me(x))$ then $(\rho, \kappa) \models_{me}^C Q$;
5. If $\mu = x(y^\chi)$ and $\chi \in \kappa(me(x))$ then $(\rho, \kappa) \models_{me[y\mapsto\chi]}^C Q$.

**Proof.** The proof is by induction on the construction of $P \xrightarrow{\mu} Q$ and with subcases depending on whether case (1), (2a), (2b), (3a), or (3b) applies. Throughout assume that $me[\text{fin}(P)] \subseteq \mathcal{C}$, $(\rho, \kappa) \models_{me} P$ (i.e. $(\rho, \kappa) \models_{me}^C P$) and $P \xrightarrow{\mu} Q$. 
The Case (1). That \( me[fn(Q)] \subseteq C \) is immediate from Fact 2.3. It remains to show that \((\rho, \kappa) \models_m Q\).

In the case of \( Tau \) this is immediate; clearly the axioms \( Out, FreeIn, \) and \( Boundln \) do not apply. Thanks to Lemma 3.8 and the induction hypothesis (1), the property is preserved by the rules \( Var, Par, Sum, Res, \) and \( Match \); clearly the rule \( Open \) does not apply.

For suitable \( Q_1 \) and \( Q_2 \) such that \( Q = Q_1 \mid Q_2 \), in the case of rule \( Close \) the induction hypothesis (2b) ensures that

\[
(\rho, \kappa) \models_{me[y \mapsto \chi]} Q_1 \land \chi \in \kappa(me(x))
\]

and the induction hypothesis (3b) ensures that

\[
(\rho, \kappa) \models_{me[y \mapsto \chi]} Q_2
\]

thereby establishing the desired

\[
(\rho, \kappa) \models_{me} (\forall y)(Q_1 \mid Q_2).
\]

The case of rule \( Com \) is similar but uses the induction hypotheses (2a) and (3a).

The Case (2a). That \( me[fn(Q)] \subseteq C \) is immediate from Fact 2.3; furthermore \( \rho(me(x)) = \{me(x)\} \subseteq C \) and \( \rho(me(y)) = \{me(y)\} \subseteq C \). It remains to show that \((\rho, \kappa) \models_{me} Q \) and that \( me(y) \in \kappa(me(x)) \).

In the case of \( Out \) it follows from Table 2 that \((\rho, \kappa) \models_{me} Q \) and \( \forall \chi \in \rho(me(x)); \rho(me(y)) \subseteq \kappa(\chi) \), which amounts to \( me(y) \in \kappa(me(x)) \); the axioms \( Tau, FreeIn, \) and \( Boundln \) do not apply. Thanks to Lemma 3.8 and the induction hypothesis (2a) the property is preserved by the rules \( Var, Par, Sum, Res, \) and \( Match \); clearly the rules \( Open, Close, \) and \( Com \) do not apply.

The Case (2b). That \((me[y \mapsto \chi])[fn(Q)] \subseteq C \) is immediate from Fact 2.3; furthermore \( \rho(me(x)) = \{me(x)\} \subseteq C \). It remains to show that \((\rho, \kappa) \models_{me} Q \) and \( \chi \in \kappa(me(x)) \). None of the axioms \( Tau, Out, FreeIn, \) and \( Boundln \) nor any of the rules \( Close \) or \( Com \) can apply. Thanks to Lemma 3.8 and the induction hypothesis (2b) the property is preserved by the rules \( Var, Par, Sum, Res, \) and \( Match \).

The Case (3a). Here we also assume that \( me(y) \in \kappa(me(x)) \) so that \( me(y) \in C \). Then \( me[fn(Q)] \subseteq C \) is immediate from Fact 2.3 that also implies \( \rho(me(x)) = \{me(x)\} \subseteq C \); it remains to show that \((\rho, \kappa) \models_{me} Q \).

In the case of \( FreeIn \), \( P \) is on the form \( x(w^\beta) \). \( R \) and \( Q \) is \( R[y/w] \). By Lemma 3.8 (since \( \alpha \)-equivalence is part of the structural congruence) we may use rule \( Var \) to guarantee that \( w \neq y \). From \((\rho, \kappa) \models_{me} x(w^\beta).R \) we have that \((\rho, \kappa) \models_{me[w \mapsto \beta]} R \) and \( \kappa(me(x)) \subseteq \rho(\beta) \). It follows that \( me(y) \in \rho(\beta) \), which may be rewritten as \( (me[w \mapsto \beta])(y) \in \rho(\{me[w \mapsto \beta]\}(w)) \). From Lemma 3.9 we then get \((\rho, \kappa) \models_{me[w \mapsto \beta]} R[y/w] \) and the desired \((\rho, \kappa) \models_{me} R[y/w] \) follows, by Lemma 3.5.

Neither the axioms \( Tau, Out, \) and \( Boundln \), nor the rules \( Open, Close, \) or \( Com \) are applicable. Thanks to Lemma 3.8 and induction hypothesis (3a) the property is preserved by the rules \( Var, Par, Sum, Res, \) and \( Match \).

The Case (3b). Here we also assume that \( \chi \in \kappa(me(x)) \subseteq C \). From Fact 2.3 we have \( (me[y \mapsto \chi])[fn(Q)] \subseteq C \) and \( \rho(me(x)) = \{me(x)\} \subseteq C \) so that it remains to show that \((\rho, \kappa) \models_{me[y \mapsto \chi]} Q \).

The axiom \( Boundln \) applies in this case so \( P \) has the form \( x(y^\beta).Q \). Let now \( w \notin \{y\} \cup fn(Q) \) and note that \( x(w^\beta).R \equiv x(y^\beta).Q \) for \( R \equiv Q[w/y] \). Since \( Q \equiv R[y/w] \) it follows from Lemma 3.8 that it suffices to show that \((\rho, \kappa) \models_{me[y \mapsto \chi]} R[y/w] \). From \((\rho, \kappa) \models_{me} P \) and Lemma 3.8 it follows that \((\rho, \kappa) \models_{me} x(w^\beta).R \) and hence that \((\rho, \kappa) \models_{me[w \mapsto \beta]} R \) and \( \kappa(me(x)) \subseteq \rho(\beta) \). Using Lemma 3.5 it now follows that \((\rho, \kappa) \models_{me[w \mapsto \beta][y \mapsto \chi]} R \). As in the previous case we have \((me[w \mapsto \beta][y \mapsto \chi])(y) \in \rho(\{me[w \mapsto \beta]\}(w)) \) and Lemma 3.9 gives \((\rho, \kappa) \models_{me[w \mapsto \beta][y \mapsto \chi]} R[y/w] \). The desired \((\rho, \kappa) \models_{me[y \mapsto \chi]} R[y/w] \) follows by Lemma 3.5.

Neither the axioms \( Tau, Out, \) and \( FreeIn \), nor the rules \( Open, Close, \) or \( Com \) are applicable. Thanks to Lemma 3.8 and induction hypothesis (3b) the property is preserved by the rules \( Var, Par, Sum, Res, \) and \( Match \).
The inclusions occurring in the above items mildly constrain the environment where the process under validation operates. If one only considers closed systems, which can only perform τ moves, the inclusions become useless, as all names are bound; in essence we retain only item (1).

4. CONSTRUCTION OF SOLUTIONS

There is also a constructive procedure for obtaining the least solution which operates in $O(N^3)$ time in the size of processes (see [18, 31]). To describe it we shall concentrate on a process, $P_\ast$, of interest as well as a marker environment, $me_\ast$, giving the binders and channels of free names in the process. To obtain a finite algorithm we prefer to restrict our attention to a finite universe, $\mathcal{U}$, containing all the relevant binders and channels and the set $me[fn(P_\ast)] = \{ me(x) | x \in fn(P_\ast) \}$.

We shall say that the size, $N$, of $P_\ast$ is the maximum of the number of symbols in $P_\ast$ and the number of elements in $\mathcal{U}$. In case we take an annotation which has all markers different from each other and disjoint from the image of the marker environment, $N$ linearly depends on the size of $P_\ast$ only.

Validating a solution $(\rho, \kappa) \models_{me} P$ amounts to checking a number of individual constraints. We now define a function $G_C[P]_{me}$ for explicitly extracting the set of constraints to be checked. In doing so we shall make it clear that we are extracting the constraints in the form of syntax, and hence replace $\rho$ of Table 2 by $r$ and $\kappa$ by $k$.

**Definition 4.1.** We now define two classes of constraints.

- An **individual constraint** is on one of the forms $n_1 \subseteq n_2, \{ x \} \subseteq n_0$, or $n_1 \cap n_2 \neq \emptyset$, where each $n_i$ will be on one of the three forms $r(\beta), r(\chi)$ or $k(\chi)$.

- A **composite constraint** is on the form $ic_1, \ldots, ic_m \Rightarrow ic$ where $m \geq 0$, all $ic_i$ (on the left-hand side) are individual constraints on either form $\{ x \} \subseteq n_0$ or $n_1 \cap n_2 \neq \emptyset$, and $ic$ (on the right-hand side) is an individual constraint on the form $n_1 \subseteq r(\beta)$ or $n_1 \leq k(\chi)$.

The details of $G_C[P]_{me}$ are given in Table 3. In the clause for $[x = y]P$ we cannot decide whether or not $r(me(x)) \cap r(me(y)) \neq \emptyset$ and hence we ensure that the constraints subsequently generated will in fact explicitly test this. Technically, this is achieved by means of the subscript $C$ to the function $G_C[P]_{me}$: each constraint generated will be conditional on all of the constraints in the (initially empty) set $C$. Similarly, in the clauses for $\bar{x}y.P$ and $x(y^\beta).P$ we use the assumptions about the universe $\mathcal{U}$, in particular that $me[fn(P_\ast)] \subseteq \mathcal{U}$, to generate a sufficiently large set of constraints that then explicitly test for $\{ x \} \subseteq r(me(x))$.

The call $G_C[P]_{me}$ will give rise to at most $O(N)$ recursive calls, each call directly responsible for generating at most $O(N)$ constraints (see the clauses for input and output). The set of constraints $C$ occurring as index to the recursive calls $G_C[P]_{me}$ can have size at most $O(N^2)$ (see the clause for matching). Hence at most $O(N^3)$ constraints of size $O(N)$ will be produced.

**TABLE 3**

<table>
<thead>
<tr>
<th>Constraint Generation for the π-Calculus</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G_C[0]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}y.P]_{me}$</td>
</tr>
<tr>
<td>$G_C[x(y^\beta).P]_{me}$</td>
</tr>
<tr>
<td>$G_C[P_1 \uplus P_2]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}(x^\gamma).P]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}y.P]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}(x^\gamma).P]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}(x^\gamma).P]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}(x^\gamma).P]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}(x^\gamma).P]_{me}$</td>
</tr>
<tr>
<td>$G_C[\bar{x}(x^\gamma).P]_{me}$</td>
</tr>
</tbody>
</table>
The Semantics of the Constraints

To relate Tables 2 and 3 we need to interpret a set of constraints with respect to a proposed solution \((\rho, \kappa)\). First we define an evaluation function for left-hand sides:

**Definition 4.2.** We define \(V_{(\rho, \kappa)}[n] \vartriangleleft \rho(\beta)\) if \(n = r(\beta)\)

\[
V_{(\rho, \kappa)}[n] = \begin{cases} 
\rho(\beta) & \text{if } n = r(\beta) \\
\{\chi\} & \text{if } n = r(\chi) \\
\kappa(\chi) & \text{if } n = k(\chi).
\end{cases}
\]

Next we define a satisfaction relation.

**Definition 4.3.** We define \((\rho, \kappa) \models n_1 \subseteq n_2\) iff \(V_{(\rho, \kappa)}[n_1] \subseteq V_{(\rho, \kappa)}[n_2]\)

\((\rho, \kappa) \models \{\chi\} \subseteq n\) iff \(\chi \not\in V_{(\rho, \kappa)}[n]\)

\((\rho, \kappa) \models n_1 \cap n_2 \neq \emptyset\) iff \(V_{(\rho, \kappa)}[n_1] \cap V_{(\rho, \kappa)}[n_2] \neq \emptyset\)

and also

\((\rho, \kappa) \models \{i_1, \ldots, i_m\} \Rightarrow i_1 \iff \bigwedge_{i=1}^{m} (\rho, \kappa) \models i_1 \Rightarrow ((\rho, \kappa) \models i_1)\)

and finally

\((\rho, \kappa) \models \forall c \in C: (\rho, \kappa) \models cc\)

The relationship between Tables 2 and 3 is now given by the following result.

**Lemma 4.4.** \((\rho, \kappa) \models \exists_c \in C : (\rho, \kappa) \models cc\)

**Proof.** We proceed by structural induction on \(P\). Most cases are straightforward and here we only consider two of the more interesting cases.

**The Case** \(\exists y \beta).P\). We have that \((\rho, \kappa) \models \exists y \beta).P\) is equivalent to

\[
(\rho, \kappa) \models \exists y \beta).P_{me} \vartriangleleft \rho(\beta), P_{me} \vartriangleleft r(\rho(\beta)) |
\]

Using the induction hypothesis this is equivalent to

\[
((\rho, \kappa) \models C) \Rightarrow (\rho, \kappa) \models [\rho(\beta) \vartriangleleft r(\rho(\beta)), P_{me} \vartriangleleft r(\rho(\beta))]
\]

and given the assumptions about the universe \(\mathcal{U}\) this is equivalent to the desired \((\rho, \kappa) \models C) \Rightarrow (\rho, \kappa) \models x(\beta).P\).

**The Case** \([x = y] P\). We have that \((\rho, \kappa) \models [x = y] P\) is equivalent to

\[
(\rho, \kappa) \models [x = y] P_{me} \vartriangleleft \rho(\beta) \vartriangleleft r(\rho(\beta)) \vartriangleleft P_{me}
\]

Using the induction hypothesis and the definition of SAT this is equivalent to

\[
((\rho, \kappa) \models C \land (\rho, \kappa) \models (\rho(\beta) \vartriangleleft r(\rho(\beta)) \vartriangleleft \emptyset)) \Rightarrow (\rho, \kappa) \models P)
\]
which using the definition of sat may be rewritten as

\[(\rho, \kappa) \text{ SAT } C \land (\rho(me(x)) \land \rho(me(y)) \neq \emptyset) \Rightarrow ((\rho, \kappa) \models_{me} P)\]

that is equivalent to the desired \(((\rho, \kappa) \text{ SAT } C) \Rightarrow (\rho, \kappa) \models_{me} [x = y]P\).

\section*{Solving the Constraints}

We now demonstrate how to solve a set of constraints as might have been generated above. For our purposes, merely obtaining an algorithm running in \(O(N^5)\) time, it suffices to perform a simple iterative procedure upon a function \(f_C\) associated with the set of constraints \(C\).

\textbf{Definition 4.5.} Given a set \(C\) of constraints, the function \(f_C\) maps a proposed solution into another one as

\[f_C(\rho, \kappa) = (\rho', \kappa'),\]

where

\[
\rho'(\beta) = \bigcup_{(i_1, \ldots, i_m) \Rightarrow n(x) \in r(\beta) \in C} \begin{cases} V_{(\rho, \kappa)}[n_1] & \text{if } \bigwedge_{i=1}^m (\rho, \kappa) \text{ sat } i_i \\ \emptyset & \text{otherwise} \end{cases}
\]

and

\[
\kappa'(\chi) = \bigcup_{(i_1, \ldots, i_m) \Rightarrow n(x) \in k(\chi) \in C} \begin{cases} V_{(\rho, \kappa)}[n_1] & \text{if } \bigwedge_{i=1}^m (\rho, \kappa) \text{ sat } i_i \\ \emptyset & \text{otherwise} \end{cases}.
\]

A related function \(\hat{f}_C\) is given by

\[\hat{f}_C(\rho, \kappa) = (\rho, \kappa) \cup f_C(\rho, \kappa).\]

The relationship between the two functions, \(f_C\) and \(\hat{f}_C\), and satisfaction, \(\text{SAT }C\), of the set of constraints is given by the following result.

\textbf{Lemma 4.6.} \((\rho, \kappa) \text{ SAT } C \iff f_C(\rho, \kappa) \subseteq (\rho, \kappa) \iff \hat{f}_C(\rho, \kappa) = (\rho, \kappa)\) whenever \(C\) is a set of composite constraints.

\textbf{Proof.} The second “iff” is immediate so consider the first. A composite constraint in \(C\) has the form \([i_1, \ldots, i_m] \Rightarrow n_1 \subseteq n_2\); there are two possibilities for \(n_2\) and here we just consider the case where \(n_2\) is \(r(\beta)\). Then

\[(\rho, \kappa) \text{ sat } ([i_1, \ldots, i_m] \Rightarrow n_1 \subseteq r(\beta))\]

is equivalent to

\[
\left( \bigwedge_{i=1}^m (\rho, \kappa) \text{ sat } i_i \right) \Rightarrow V_{(\rho, \kappa)}[n_1] \subseteq \rho(\beta),
\]

which can be rewritten as

\[
\begin{cases} V_{(\rho, \kappa)}[n_1] & \text{if } \bigwedge_{i=1}^m (\rho, \kappa) \text{ sat } i_i \\ \emptyset & \text{otherwise} \end{cases} \subseteq \rho(\beta).
\]

It follows that

\[(\rho, \kappa) \text{ SAT } \{([i_1, \ldots, i_m] \Rightarrow n_1 \subseteq r(\beta')) \in C \mid \beta' = \beta\}\]
is equivalent to

$$\bigcup_{\{i_1, \ldots, ic_m\} \supseteq n_1 \forall (\beta') \in C \land \beta' = \beta} \left( \begin{array}{l} V_{(\rho, \kappa)}[n_1] \quad \text{if } \land_{i=1}^{m} (\rho, \kappa) \text{ sat } ic_i \\vdash \rho(\beta) \quad \text{otherwise} \end{array} \right)$$

and the desired result easily follows. ■

To prepare for the iteration we need the following standard result.

**Lemma 4.7.** $f_C$ is monotone and $\hat{f}_C$ is monotone and extensive whenever $C$ is a set of composite constraints.

**Proof.** It is immediate that $\hat{f}_C$ is extensive (meaning that $\forall (\rho, \kappa):(\rho, \kappa) \supseteq \hat{f}_C(\rho, \kappa)$ and that it is monotone (meaning that $\forall (\rho, \kappa) \subseteq (\rho', \kappa') : \hat{f}_C(\rho, \kappa) \supseteq \hat{f}_C(\rho', \kappa')$) if $f_C$ is. To see that $f_C$ is monotone let $(\rho, \kappa) \subseteq (\rho', \kappa')$ and consider a composite constraint $\{ic_1, \ldots , ic_m\} \Rightarrow n_1 \subseteq n_2$ in $C$; there are two possibilities for $n_2$ and here we just consider the case where $n_2$ is $r(\beta)$. It is immediate that $V_{(\rho, \kappa)}[n_1] \supseteq V_{(\rho', \kappa')}[n_1]$ and we also have $(\rho, \kappa) \text{ sat } ic_1 \Rightarrow (\rho', \kappa') \text{ sat } ic_1$ because $ic_1$ is either of the form $n_1' \cap n_2' \neq \emptyset$ or $\{\chi\} \subseteq n'$. This establishes the result. ■

Setting $C = G_{\emptyset}[P_*]_{me}$, it now follows that the least $(\rho, \kappa)$ (above a given $(\tilde{\rho}, \tilde{\kappa})$, typically $(\bot, \bot)$) that satisfies $(\rho, \kappa) \models_{me} P_*$ equals the least fixed point of $f_C$ (above $(\tilde{\rho}, \tilde{\kappa})$). Because of our assumptions about the universe, $U$, the set $C$ is finite and $f_C$ operates over a complete lattice of finite size. Standard fixed point theory then ensures that the desired $(\rho, \kappa)$ is obtained as $\hat{f}_C(\tilde{\rho}, \tilde{\kappa})$ upon stabilisation, i.e., for the least $j$ such that $\hat{f}_C^j(\tilde{\rho}, \tilde{\kappa}) = \hat{f}_C^{j+1}(\tilde{\rho}, \tilde{\kappa})$, where it is certain that such $j$ exists. We may summarise the development as follows.

**Theorem 4.8.** Writing $C = G_{\emptyset}[P_*]_{me}$, there is a least natural number $j$ such that $\hat{f}_C^j(\tilde{\rho}, \tilde{\kappa}) = \hat{f}_C^{j+1}(\tilde{\rho}, \tilde{\kappa})$; it satisfies

$$\hat{f}_C^j(\tilde{\rho}, \tilde{\kappa}) \models_{me} P_*$$

and that $\hat{f}_C^j(\tilde{\rho}, \tilde{\kappa}) \supseteq \bigcap \{ (\rho, \kappa) \mid (\rho, \kappa) \models_{me} P_*, (\rho, \kappa) \supseteq (\tilde{\rho}, \tilde{\kappa}) \}$.

The tuple $(\rho, \kappa)$ contains $O(N)$ elements taking values in a set of size $O(N)$. Hence at most $O(N^2)$ iterations of the function will be needed. Each iteration can be performed by considering each of the $O(N^2)$ constraints of form $\{ic_1, \ldots , ic_m\} \Rightarrow n_1 \subseteq n_2$, calculating $ic_1, \ldots, ic_m$ and $n_1$ in time $O(N)$ and then updating the entry for $n_2$ accordingly. Hence the desired solution can be obtained in time $O(N^5)$ and space $O(N^3)$.

**Example 4.9.** As an example suppose that $(\rho_1, \kappa_1)$ is the least solution for $P_1$ and that $(\rho_2, \kappa_2)$ is the least solution for $P_2$ (w.r.t. the same $me$). It follows that there also is a least solution $(\rho, \kappa)$ for $P_1 \mid P_2$ and since this is a solution for $P_1$ and for $P_2$ we have

$$(\rho_1, \kappa_1) \cup (\rho_2, \kappa_2) \subseteq (\rho, \kappa).$$

We therefore know that $(\rho, \kappa)$ equals

$$\hat{f}_C^j((\rho_1, \kappa_1) \cup (\rho_2, \kappa_2))$$

upon stabilisation.

To see that $j$ cannot always be taken to be $0$ consider the two processes $P_1 = x(y^\beta)(\nu x)\bar{x}x$ and $P_2 = (\nu x z^1)(\nu z^2)\bar{z}z$, the marker environment $me(x) = \chi_1$, and the following definitions of $\rho_i$ and $\kappa_i$:

<table>
<thead>
<tr>
<th>$i$</th>
<th>$\kappa_i(\chi_1)$</th>
<th>$\rho_i(\beta_0)$</th>
<th>$\ldots$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>${\chi_1}$</td>
<td>${\chi_1}$</td>
<td>$\ldots$</td>
</tr>
<tr>
<td>2</td>
<td>$\emptyset$</td>
<td>$\emptyset$</td>
<td>$\ldots$</td>
</tr>
</tbody>
</table>
Setting \((\rho', \kappa') = (\rho_1, \kappa_1) \cup (\rho_2, \kappa_2)\) we have \(\kappa'(\chi_1) = \{\chi_1, \chi_2\}\) and \(\rho'(\beta_0) = \{\chi_1\}\) and hence the constraint \(\kappa'(\chi_1) \subseteq \rho'(\beta_0)\) fails.

5. PREVENTING LEAKAGE

A common approach to system security is based on putting objects and subjects into security classes. We demonstrate that control flow analysis helps in statically detecting useful information on security. We consider in this section a static property ensuring that a channel, devised to be secret to a process \(P\), is never communicated to an external user. In the next section, we statically check another property that concerns how information flows between processes at different levels.

The \(\pi\)-calculus does not distinguish between data, that may be secret, and channels that can be seen as capabilities of accessing data. More refined calculi, notably the \(\textit{spi}\)-calculus \cite{spi}, make such a distinction and permit a finer description of security properties. We choose here a pure calculus of computations, without encryption and decryption primitives, in order to concentrate on the applicability of the control flow analysis to security issues. In fact, the scoping rules of the \(\pi\)-calculus are sufficient for a careful use of channels, because processes can generate and pass new names, making the channels they denote available for communication. In a sense, learning the name of a channel amounts to possessing the capability to communicate on it, and restriction governs the visibility of names.

A process \(P\) could have the security requirement of keeping secret (some of) its channels, i.e., not to communicate them to the external environment. A process matches this requirement if it never performs an extrusion of a secret channel, as made precise below. In the following, we assume that \(S\) is a set of secret channels given by a designated authority, e.g., the designer or the user of a process \(P\), who implicitly introduces also the set \(P\) of public channels as the complement of \(S\). A priori, binders are neither public nor secret; the actual solution of the analysis establishes which kind of channels can be bound to each binder.

**Definition 5.1.** The pair \(P, me\) is admissible for the set \(S \subseteq C\) of secret channels, if and only if \(me[fn(P)] \subseteq C\) and \(me[fn(P)] \cap S = \emptyset\). Then, the set of public channels is \(P = C \setminus S\).

Note that the condition of admissibility is equivalent to \(me[fn(P)] \subseteq P\); i.e., all free names are public channels.

**A Dynamic Notion**

Now, we characterize a process \(P\) that never discloses its secrets. We describe this property by saying that \(P\) has no leaks. Intuitively, \(P\) enjoys this property if neither it nor any of its derivatives can perform an extrusion of a name bound to a secret channel, as made precise below. For this to make sense it is important to assume that the environment (or an external user) cannot guess any secret channels. We formalise this by a constrained notion of computation called censored. Essentially, a computation is censored if no name \(y\), with \(me(y) \in S\), can be read from the environment through an input.

**Definition 5.2.** Given \(P, me, S\) a censored step \((P, me) \xrightarrow{\mu} (Q, me')\) is defined whenever the following conditions hold:

1. \(P \xrightarrow{\mu} Q\)
2. (a) if \(\mu = xy\), then \(me(y) \in P\)
   (b) if \(\mu = x(y^z)\), then \(\chi \in P\)

where \(me' = \begin{cases} me & \text{if } \mu = \tau, \tilde{x}y, xy \\ me[y \mapsto \chi] & \text{if } \mu = \tilde{x}(y^z), x(y^z) \end{cases}\).

A censored computation \((P, me) \xrightarrow{\star} (Q, me') \xrightarrow{\mu} (R, me'')\) is made of censored steps, whose labels are all immaterial, apart from the last one.
The following proposition shows that admissibility is preserved under censored computations, provided that there is no extrusion of a name marked secret. It also reveals the role played by the second condition of a censored step.

**Lemma 5.3.** Let $P$, $me$ be admissible for $S$ and $(P, me) \mu \mapsto (Q, me')$ be such that $\mu = \bar{x}(y^x)$ implies $\chi \in P$; then, $Q$, $me'$ are admissible for $S$.

**Proof.** The proof is by cases on $\mu$. If $\mu = \tau$ or $\mu = \bar{x}y$ then $me' = me$; from the hypotheses and Fact 2.3 we have that $me'[	ext{fn}(Q)] \subseteq P$. If $\mu = \bar{x}(y^x)$ we have that $me' = me[y \mapsto \chi]$; from the hypotheses and Fact 2.3 we get that $me'[	ext{fn}(Q)] \subseteq P$. If $\mu = xy$, $me(y) \in P$ (by censored step) and $me' = me$, therefore the hypotheses and Fact 2.3 ensure that $me'[	ext{fn}(Q)] \subseteq P$. If $\mu = x(y^x)$ we have that $\chi \in P$ (by censored step) and that $me' = me[y \mapsto \chi]$ so that the hypotheses together with Fact 2.3 ensure that $me'[	ext{fn}(Q)] \subseteq P$.

We are ready to define our dynamic notion of security for some $P$, $me$ that are admissible for the set $S$ of secret channels.

**Definition 5.4.** The process $P$ has no leaks with respect to $S$, $me$ if and only if $(P, me) \mapsto^* (Q, me')$ implies that there is no pair $(R, me'')$ such that $(Q, me') \mapsto^* (R, me'')$ with $\chi \in S$.

Of course when $P$ is stuck, it has no leaks. Note that if $P$ has no leaks, with respect to $S$, $me$, and $P$, $me$ are admissible for $S$, then for all $Q$ such that $(P, me) \mapsto^* (Q, me')$, $Q$, $me'$ are admissible for $S$, due to Lemma 5.3.

**A Static Notion**

The notion of no leaks above is dynamic. We now introduce a static notion, in order to predict at compile time if a process has no leaks. It is called confinement\(^1\) and we prove that it is a sufficient condition for a process to have no leaks.

**Definition 5.5.** Let $P$, $me$ be admissible for a given $S$. A process $P$ is confined with respect to $S$, $me$ if and only if there exists $(\rho, \kappa)$ such that

\[
\begin{align*}
(a) \quad (\rho, \kappa) \models_{me} P & \quad \text{and} \quad (b) \quad \kappa(\chi) = \mathcal{P} \quad \text{if} \quad \chi \in \mathcal{P}.
\end{align*}
\]

Hereafter, we will say that $P$ is confined via the confining solution $(\rho, \kappa)$.

Note that if a process $P$ is confined, by admissibility we also have that $me[\text{fn}(P)] \subseteq \mathcal{P}$. Intuitively, condition (b) above implies that only public information can be transmitted along a public channel, i.e., $\bigcup_{\chi \in \mathcal{P}} \kappa(\chi) \subseteq \mathcal{P}$; conversely, any channel, be it secret or public, can pass along secret channels, as no restriction is put on them. We now show that confinement is preserved by censored computations.

**Lemma 5.6 (Subject reduction for confinement).** Let $P$ be confined (w.r.t. $S$, $me$) and $(P, me) \mu \mapsto (Q, me')$; then $Q$ is confined (w.r.t. $S$, $me'$).

**Proof.** The proof is by cases on $\mu$ and considers the confining solution $(\rho, \kappa)$ for $P$. If $\mu = \tau$ or $\mu = \bar{x}y$ we have that $me' = me$; it follows from Theorem 3.10 that $(\rho, \kappa) \models_{me} Q$ and from Lemma 5.3 that $Q$, $me'$ is admissible for $S$. If $\mu = \bar{x}(y^x)$ we have $me' = me[y \mapsto \chi]$ and $x \in \text{fn}(P)$ (by Fact 2.3); it follows from Theorem 3.10 and confinement that $\rho, \kappa \models_{me} Q$ and that $\chi \in \kappa(me(x)) = \mathcal{P}$; then, by Lemma 5.3 it follows that $Q$, $me$ is admissible for $S$. If $\mu = xy$ or $\mu = x(y^x)$ we have $\chi \in \text{fn}(P)$ (because of Fact 2.3). In the first subcase $me' = me$ and $me(y) \in \mathcal{P} = \kappa(me(x))$ (by censored step and confinement); Theorem 3.10 guarantees that $\rho, \kappa \models_{me} Q$ and Lemma 5.3 that $Q$, $me'$ is admissible for $S$. In the second subcase $me' = me[y \mapsto \chi]$, $\chi \in \mathcal{P} = \kappa(me(x))$ (by censored step and confinement); Theorem 3.10 guarantees that $\rho, \kappa \models_{me} Q$ and Lemma 5.3 that $Q$, $me'$ is admissible for $S$.

We are finally ready to show that confinement is sufficient to guarantee that $P$ has no leaks.

**Theorem 5.7.** If $P$ is confined (with respect to $S$, $me$) then $P$ has no leaks (with respect to $S$, $me$).

---

\(^1\) In the literature on security, confinement is also used with different meanings.
Proof. By Lemma 5.6 it is enough to prove that \((P, me) \xrightarrow{\pi^{(\nu)}} (Q, me')\) implies \(\chi \in \mathcal{P}\). Since \(x \in \text{fin}(P)\) by Fact 2.3, we have that \(me(x) \in \mathcal{P}\) and \(\kappa(me(x)) = \mathcal{P}\) (by confinement). By Theorem 3.10, \(\chi \in \kappa(me(x))\) and hence \(\chi \in \mathcal{P}\) as was to be shown. \(\blacksquare\)

Example 5.8. We consider here an abstract version of the Wide Mouthed Frog protocol, adapted from [3]. Intuitively, two principals \(A\) and \(B\) wish to communicate using classical shared-key cryptography, and the first forwards a secret key, say \(c_{AB}\), to the second one, with the help of a server. The server shares the secret keys \(c_{AS}\) and \(c_{SB}\) with \(A\) and \(B\), respectively. So, the principal \(A\) passes its key \(c_{AB}\), encrypted with \(c_{AS}\), to the server. The server decrypts the message, encrypts it with \(c_{SB}\) and passes it to \(B\). Afterwards \(A\) sends the message \(M\), encrypted with \(c_{AB}\), to \(B\).

Here principals will be represented by processes and keys by secret channels, because the \(\pi\)-calculus has no cryptographic primitives. The specification follows:

- \(A = (vMxM)(vc_{AB}^{\chi AB})c_{AS}c_{AB}.c_{AB}M\)
- \(S = c_{AS}(x^\beta.).x_{SB}x\)
- \(B = c_{SB}(y^\beta.).y(z^\beta.)\)
- \(P = (vc_{AS}^{\chi AB})(vc_{SB}^{\chi SB})x(A|S|B)\)

The following solution is the least one:

\[
\rho(\beta) = \begin{cases} 
\{\chi AB\} & \text{if } \beta = \beta_x, \beta_y \\
\{\chi M\} & \text{if } \beta = \beta_z 
\end{cases}
\]

\[
\kappa(\chi) = \begin{cases} 
\{\chi M\} & \text{if } \chi = \chi AB \\
\{\chi AB\} & \text{if } \chi = \chi AS, \chi SB \\
\emptyset & \text{if } \chi = \chi M 
\end{cases}
\]

If we take \(S = \{\chi AB, \chi AS, \chi SB, \chi M\}\), for all choices of \(\mathcal{P}\) there is a solution confining \(P\) (with respect to \(S\)). Thus, secrecy of \(M\) is guaranteed.

Suppose to have a new name \(c_{AC}\), with \(me(c_{AC}) = \chi_c \in \mathcal{P}\). Let \(A\) be extended as follows

\(A = (vMxM)(vc_{AB}^{\chi AB})c_{AS}c_{AB}.c_{AC}M.x_{AC}c_{AB}.\)

Intuitively, \(A\) sends \(c_{AB}\) along \(c_{AC}\) after the completion of the protocol. For all solutions, it turns out that \(\kappa(\chi_{AC}) \supseteq \{\chi AB\} \not\subseteq \mathcal{P}\). Therefore, there is no solution confining \(P\) with respect to \(S\). Indeed, the analysis reveals the extrusion of \(c_{AB}\). With our specification in the \(\pi\)-calculus, this action does not affect the secrecy of \(M\), yet it signals a potential problem, as an extrusion represents the publication of the corresponding secret key. Indeed, if we take the \(spi\)-calculus, where encrypted messages are transmitted as cleartext, an enemy may intercept \(M\) encrypted, store it, and then decrypt it after \(c_{AB}\) has been extruded (this violates the so-called forward-secrecy property, see e.g., [2]).

It is immediate to see that confinement is not a necessary condition for \(P\) having no leaks. For instance the process \((v x^\gamma)\bar{y}x . \bar{y}x\) has no leaks but it is not confined with respect to \(S = \{\chi\}\) and \(me(y) \neq \chi\). Indeed not all deadlocks can be detected statically. So the extrusion of the name \(x\) along channel \(y\) is considered a possible violation of secrecy.

Checking the Static Condition

One approach to checking confinement of a process \(P\) with respect to \(S\), \(me\) is to use the polynomial time algorithm devised in the previous section. First, we check that \(P\), \(me\) (or \(P_*, me_*)\) is indeed admissible for the \(S\) given. Next, we construct sets of constraints \(C_a\) and \(C_b\) corresponding closely to the two conditions in Definition 5.5. For \(C_a\) we may simply use \(G_a[[P]]_{me}\). For \(C_b\) we generate constraints for half of the equality, namely for the inclusion “\(\supseteq\)” To be specific, write \(P_\times = P \cap \mathcal{U}_\times\) and let \(C_b\) consist of the constraints \(P_\times \subseteq \kappa(\chi)\) for all \(\chi \in P_\times\). (These constraints can be expanded into a form allowed by Definition 4.1 unlike what would be the case if we let \(C_b\) take care of the entire equality.) We then solve the set of constraints in polynomial time so as to get the least solution. Then \(P\) is confined if and only if the least solution has a \(\kappa\) component equal to the one displayed in Definition 5.5. This approach to determining whether or not \(P\) is confined (w.r.t. to \(S\), \(me\)) clearly operates in polynomial time.
6. MULTILEVEL SECURITY

Another way of enforcing security is by defining a hierarchy of levels for processes. The security requirement is that a process classified at a high level cannot write any value to a process at low level, while the converse is allowed; symmetrically a process at low level cannot read data from one of a high level. Sometimes this noninterference property is referred to as no read-up/no write-down [16]. These requirements amount to the simple security property that is part of the multilevel access control policy of [5, 14].

To study the no read-up/no write-down property we need an extension to the syntax of the π-calculus to assign security levels to processes. Accordingly, the operational semantics requires a little extension. Moreover, we will adapt the static analysis as well to take care of these levels.

In the following we will only introduce the necessary extensions to the setting of the previous sections.

Syntax

In order to simplify our presentation, we make here two assumptions that are common in the literature (see e.g., [43]). First, we consider only two levels of security clearance: \( L \) for low and \( H \) for high. So, we introduce the set \( L = \{ L, H \} \). The case with a hierarchy of levels is studied in [8]. Second, we assume to have systems made of processes in parallel, and only these top-level components are labelled by clearance levels.

The new syntax, defined below, imports the syntax in Definition 2.2 for processes.

**Definition 6.1.** Systems, denoted by \( S, S', S_1, S_2, \ldots \in \text{Sys} \) are built from processes according to the syntax

\[
S ::= (P)^l \mid (\nu x^x)S \mid S \mid !S,
\]

where \((P)^l\) expresses that \( P \) has level \( l \in L \).

The definition of free names is trivially extended by letting

\[
fn((P)^l) = fn(P) \quad fn((\nu x^x)S) = fn(S) \setminus \{x\}.
\]

**Semantics**

The structural congruence now takes care of systems, i.e.:

- \( S \equiv S' \) if \( S \) and \( S' \) are \( \alpha \)-equivalent;
- \( (0)^H \equiv (0)^L \) and \((\text{Sys} / =, \cdot, (0)^H)\) is a commutative monoid;
- \((\nu x^x)(\nu y^y)S \equiv (\nu y^y)(\nu x^x)S\), if \( x \neq y \), \((\nu x^x)(S_1 \mid S_2) \equiv (\nu x^x)S_1 \mid S_2\) if \( x \notin fn(S_2) \), and \((\nu x^x)S \equiv S\) if \( x \notin fn(S)\);
- \(!S \equiv S \mid !S\).

The operational semantics is defined in Table 4, and uses the transition relation defined in Table 1. The transitions have the form \( S \xrightarrow{l} S' \), with \( l \in L \cup \{\epsilon\} \). When different from \( \epsilon \), the additional level label \( l \) records the clearance of the system performing the transition. When a communication is derived the levels of the sender \( S_o \) and of the receiver \( S_i \) are discarded, leading to a transition of the form \( S_o \mid S_i \xrightarrow{\epsilon} S' \) (see the rules \( \text{ComS} \) and \( \text{CloseS} \) in Table 4).

**Analysis**

The solution of our new analysis is a triple \( (\rho, \kappa, \sigma) \) and the flow logic judgements are on either form

\[
(\rho, \kappa, \sigma) \models_{mc} S \quad \text{or} \quad (\rho, \kappa, \sigma) \models_l^l P.
\]
with the details. We therefore dispense

The role of $\rho, \kappa, me$ is exactly as in the previous sections. The purpose of the new entries $l$ and $\sigma = \langle \sigma_{in}, \sigma_{out} \rangle$, the abstract communication structure, is the following:

- $l \in \mathcal{L}$ keeps track of the current security level of the process under validation and is not needed for systems.
- $\sigma_{in}, \sigma_{out} : \mathcal{L} \rightarrow (\mathcal{C} \rightarrow \wp(\mathcal{C}))$ give the set of the channels that can be bound to the possible objects of an input and an output action respectively, performed by the subprocesses labelled by $l \in \mathcal{L}$, on a given channel $\chi \in \mathcal{C}$.

The analysis in Table 5 extends the analysis in Table 2, to deal with the levels of security clearance by imposing two further conditions while checking an input and an output prefix. The channels that can be bound to the object of an input (respectively, an output) action along channel $\chi$ must be included in $\sigma_{in}(l)(\chi)$ (respectively, $\sigma_{out}(l)(\chi)$), where $l$ is the current security level. This is determined by, and is the only task of, the clause for the analysis of the system $(P)^l$. The rules for the other systems are just as the rules for the corresponding processes. The technical results of Section 3 concerning the set of solutions forming a Moore family, as well as the computation of solutions in $O(N^5)$ time and $O(N^3)$ space via the generation of constraints, are easily adapted to the setting at hand. We therefore dispense with the details.

### TABLE 4

<table>
<thead>
<tr>
<th>Early Transition System for the $\pi$-Calculus with Security Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lev: $\frac{\rho \triangleright \sigma \</td>
</tr>
<tr>
<td>$\rho \downarrow l \</td>
</tr>
<tr>
<td>ParS: $\frac{\rho \downarrow l \</td>
</tr>
<tr>
<td>$\rho \downarrow l \</td>
</tr>
<tr>
<td>ResS: $\frac{\rho \downarrow l \</td>
</tr>
<tr>
<td>$\rho \downarrow l \</td>
</tr>
<tr>
<td>OpenS: $\frac{\rho \downarrow l \</td>
</tr>
<tr>
<td>$\rho \downarrow l \</td>
</tr>
<tr>
<td>ComS: $\frac{\rho \downarrow l \</td>
</tr>
<tr>
<td>$\rho \downarrow l \</td>
</tr>
<tr>
<td>(\rho \downarrow l \</td>
</tr>
</tbody>
</table>

The role of $\rho, \kappa, me$ is exactly as in the previous sections. The purpose of the new entries $l$ and $\sigma = \langle \sigma_{in}, \sigma_{out} \rangle$, the abstract communication structure, is the following:

- $l \in \mathcal{L}$ keeps track of the current security level of the process under validation and is not needed for systems.
- $\sigma_{in}, \sigma_{out} : \mathcal{L} \rightarrow (\mathcal{C} \rightarrow \wp(\mathcal{C}))$ give the set of the channels that can be bound to the possible objects of an input and an output action respectively, performed by the subprocesses labelled by $l \in \mathcal{L}$, on a given channel $\chi \in \mathcal{C}$.

The analysis in Table 5 extends the analysis in Table 2, to deal with the levels of security clearance by imposing two further conditions while checking an input and an output prefix. The channels that can be bound to the object of an input (respectively, an output) action along channel $\chi$ must be included in $\sigma_{in}(l)(\chi)$ (respectively, $\sigma_{out}(l)(\chi)$), where $l$ is the current security level. This is determined by, and is the only task of, the clause for the analysis of the system $(P)^l$. The rules for the other systems are just as the rules for the corresponding processes. The technical results of Section 3 concerning the set of solutions forming a Moore family, as well as the computation of solutions in $O(N^5)$ time and $O(N^3)$ space via the generation of constraints, are easily adapted to the setting at hand. We therefore dispense with the details.

### TABLE 5

<table>
<thead>
<tr>
<th>Control Flow Analysis for the $\pi$-Calculus with Security Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>$(\rho, \kappa, me) \models l \</td>
</tr>
<tr>
<td>$(\rho, \kappa, me) \models l \</td>
</tr>
</tbody>
</table>
| $(\rho, \kappa, me) \models l \ | me \ \exists \ y . \ P$ if and only if $(\rho, \kappa, me) \models l \ | me \ P \ \land \ \forall \chi \in \rho(me(x)):
  \begin{align*}
  \rho(me(y)) & \leq \kappa(\chi) \\
  \rho(me(y)) & \leq \sigma_{out}(l)(\chi)
  \end{align*}$ |
| $(\rho, \kappa, me) \models l \ | me \ \forall \ y . \ P$ if and only if $(\rho, \kappa, me) \models l \ | me \ P \ \land \ \forall \chi \in \rho(me(x)):
  \begin{align*}
  \kappa(\chi) & \leq \rho(\beta) \\
  \kappa(\chi) & \leq \sigma_{in}(l)(\chi)
  \end{align*}$ |
| $(\rho, \kappa, me) \models l \ | me \ P_1 \ \lor \ P_2$ if and only if $(\rho, \kappa, me) \models l \ | me \ P_1 \ \lor \ (\rho, \kappa, me) \models l \ | me \ P_2$ |
| $(\rho, \kappa, me) \models l \ | me \ P_1 \ \land \ (\rho, \kappa, me) \models l \ | me \ P_2$ |
| $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ if and only if $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ |
| $(\rho, \kappa, me) \models l \ | me \ ! \ x \ . \ y) \ P$ if and only if $(\rho, \kappa, me) \models l \ | me \ ! \ x \ . \ y) \ P$ |
| $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ if and only if $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ |
| $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ if and only if $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ |
| $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ if and only if $(\rho, \kappa, me) \models l \ | me \ (\forall \ y \ . \ P)$ |
Example 6.2. Consider the following system $S$. It consists of the processes $R$ and $Q$ of low level and of $P$ of high level.

- $R = \overline{a}b. \overline{a}b. \overline{b}c$
- $Q = a(x^b). \tilde{x}x$
- $P = a(y^b). y(z^b) \cdot ((y = z) \overline{y}a + y(w^b))$
- $S = l(R)^L | (Q)^L | (P)^H,$

where the marker environment $me$ is such that $me (f_v) = x_{fb}$ for all the free names $f_v \in \{a, b, c\}$. The triple $(\rho, \kappa, \sigma)$ is defined as follows, where the bound names are $bv \in \{x, y, z, w\}$:

$$\rho(\beta_{bv}) = \begin{cases} \{x_b\} & \text{if } bv = x, y \\ \{x_a, x_b, x_c\} & \text{if } bv = z, w \end{cases} \quad \kappa(x_{fb}) = \begin{cases} \{x_b\} & \text{if } fv = a \\ \{x_a, x_b, x_c\} & \text{if } fv = b \\ \emptyset & \text{if } fv = c \end{cases}$$

$$\sigma_{in}(L)(x_a) = \{x_b\} \quad \sigma_{in}(H)(x_a) = \{x_b\}$$
$$\sigma_{in}(L)(x_b) = \emptyset \quad \sigma_{in}(H)(x_b) = \{x_a, x_b, x_c\}$$
$$\sigma_{in}(L)(x_c) = \emptyset \quad \sigma_{in}(H)(x_c) = \emptyset$$
$$\sigma_{out}(L)(x_a) = \{x_b\} \quad \sigma_{out}(H)(x_a) = \emptyset$$
$$\sigma_{out}(L)(x_b) = \{x_b, x_c\} \quad \sigma_{out}(H)(x_b) = \{x_a\}$$
$$\sigma_{out}(L)(x_c) = \emptyset \quad \sigma_{out}(H)(x_c) = \emptyset.$$

Recall that $\rho(\chi) = \{\chi\}$. A simple check shows that $(\rho, \kappa, \sigma) \models_{me} S$.

The semantic soundness of our new analysis is stated by the new subject reduction theorem, which is almost identical to Theorem 3.10. The only differences are the new judgements $(\rho, \kappa, \sigma) \models_{me} S$ and the obvious conditions about the new components $\sigma$ and $l$. Its proof is a straightforward adaptation of the proof of Theorem 3.10, so we omit it. We also omit the easy extensions of the relevant lemmata in Section 3. As before, $(\rho, \kappa, \sigma) \models_{me} C$ stands for $(\rho, \kappa, \sigma) \models_{me} C \land me[fn(S)] \subseteq C$.

Theorem 6.3. If $(\rho, \kappa, \sigma) \models_{me} C$ and $S \vdash_{l} S'$ we have:

1. if $\mu = \tau$ then $(\rho, \kappa, \sigma) \models_{me} C$,
2. if $\mu = \tilde{x}y$ then $(\rho, \kappa, \sigma) \models_{me} C'$, $me(y) \in \kappa(me(x))$, and $me(y) \in \sigma_{out}l(me(x));$
3. if $\mu = \tilde{x}(y^z)$ then $(\rho, \kappa, \sigma) \models_{me} C'$, $x \in \kappa(me(x))$ and $\chi \in \sigma_{out}l(me(x));$
4. if $\mu = x(y^z)$ and $\chi \in \kappa(me(x))$ then $(\rho, \kappa, \sigma) \models_{me} C'$, and $me(y) \in \sigma_{in}l(me(x));$
5. if $\mu = x(y^z)$ and $\chi \in \kappa(me(x))$ then $(\rho, \kappa, \sigma) \models_{me} C'$, and $\chi \in \sigma_{in}l(me(x))$, with $l \in \{L, H\}$ in all cases, except for the case (1) where $l \in \{L, H\} \cup \{\epsilon\}.$

Dynamic Notion

We now introduce the dynamic version of the no read-up/no write-down property. As we did with censored steps, we impose a restriction on the channels that can be read by a process $P$ with a given clearance $l$. We assume that the environment is always willing to listen to $P$, but it can select which information is to be transmitted to $P$. To formalize the intentions of the environment, we use a function

$$\xi : L \rightarrow (C \rightarrow \Phi(C))$$
that maps a label \( l \in \mathcal{L} \) and a channel \( \chi \in \mathcal{C} \) to the set of channels that the environment considers secure to communicate to \( (P)^l \).

**Definition 6.4.** Given \( S, me, \varsigma \), a granted step is \( (S, me) \overset{\mu}{\rightarrow}_l (S', me') \), and is defined whenever

1. \( S \overset{\mu}{\rightarrow}_l S' \), and
2. (a) if \( \mu = xy \), then \( me(y) \in \varsigma(l)(me(x)) \)
   (b) if \( \mu = x(y^x) \), then \( \chi \in \varsigma(l)(me(x)) \),

where \( me' = \begin{cases} me & \text{if } \mu = \tau, \bar{x}y, xy \\ me[y \mapsto \chi] & \text{if } \mu = x(y^x), x(y^x) \end{cases} \)

A granted computation \((S, me) \overset{\cdot}{\rightarrow} (S', me') \overset{\mu}{\rightarrow}_l (S'', me'')\) is made of granted steps.

The definition of our version of the no read-up/no write-down property follows.

**Definition 6.5.** A system \( S \) is no read-up/no write-down (nru/nwd for short) with respect to \( \varsigma, me \) if and only if: whenever \((S, me) \overset{\cdot}{\rightarrow} (S', me') \overset{\cdot}{\rightarrow} (S'', me'')\), where the last granted step is a communication (between \( S_i \) and \( S_j \)) that has been deduced with either

(a) the rule \( \text{ComS} \), using the premises \( S_o \xrightarrow{\bar{x}y \ l_o} S'_o \) and \( S_i \xrightarrow{x(y^x) \ l_i} S'_i \), or

(b) the rule \( \text{CloseS} \), using the premises \( S_o \xrightarrow{x^y \ l_o} S'_o \) and \( S_i \xrightarrow{x(y^x) \ l_i} S'_i \),

then \( l_o = H \) implies \( l_i = H \).

**A Static Notion**

We define now a static property that guarantees that a process is nru/nwd. Besides finding a solution \((\rho, \kappa, \sigma)\) for a process \( P \), we require that the channels that can pass along a given channel \( \chi \) include those that can be read and sent along \( \chi \), recorded by the abstract communication structure \( \sigma \) (condition 2a below). More interesting is item (b) of the same condition, where the channels read along \( \chi \) should include those that the environment is willing to supply, expressed by \( \varsigma \). The last condition is the key condition. It requires that a channel \( \chi \) cannot be used for sending an object from a process with high level \( H \) to a process with low level \( L \).

**Definition 6.6.** Let \( S, me \) be such that \( me \ [fn(S)] \subseteq \mathcal{C} \). Then \( S \) is discreet (w.r.t. \( \varsigma, me \)) if and only if there exists \((\rho, \kappa, \sigma)\) such that

1. \( (\rho, \kappa, \sigma) \models_{me} S \)
2. \( \forall l \in \{L, H\}, \chi \in \mathcal{C} : \begin{cases} (a) \kappa(\chi) \supseteq \sigma_{in}(l)(\chi) \cup \sigma_{out}(l)(\chi) \\ (b) \sigma_{in}(l)(\chi) \supseteq \varsigma(l)(\chi) \end{cases} \)
3. \( \forall \chi \in \mathcal{C} : \sigma_{out}(H)(\chi) \cap \sigma_{in}(L)(\chi) = \emptyset \).

Below, we show that the property of being discreet is preserved under granted steps.

**Lemma 6.7 (Subject Reduction for Discreetness).** If \( S \) is discreet with respect to \( \varsigma, me \), and \((S, me) \overset{\mu}{\rightarrow}_l (S', me')\), then \( S' \) is discreet with respect to \( \varsigma, me' \).

**Proof.** Theorem 6.3 suffices to prove both \( me \ [fn(S')] \subseteq \mathcal{C} \) and \((\rho, \kappa, \sigma) \models_{me} S' \). The proof of the second and third items of discreetness is immediate, because the solution does not change. The only delicate point for the application of Theorem 6.3 is when the granted step is an input, while in the other cases the proof is trivial. For input, consider first the case \( \mu = xy \). It suffices to show that \( me(y) \in \kappa(me(x)) \). Conditions (2a) and (2b) of Definition 6.6 guarantee that \( \kappa(me(x)) \supseteq \sigma_{in}(l)(me(x)) \supseteq \varsigma(l)(me(x)) \). Furthermore, \( me(y) \in \varsigma(l)(me(x)) \) because the step is granted. The case when \( \mu = x(y^x) \) is similar.

**Theorem 6.8.** If \( S \) is discreet (w.r.t. \( \varsigma, me \)), then \( S \) is nru/nwd (w.r.t. \( \varsigma, me \)).
Proof. Since our computations are granted, by Lemma 6.7 it is enough to check that, if
\((S, me) \to (S', me')\) then \(S'\) is nru/nwd, with \(r\) being a communication between \(S_0\) and \(S_1\), defined as in Definition 6.5. Without loss of generality we may assume that all restrictions in \(S\) occur outermost or inside some \(\cdot\). Assume, per absurdum, that \(l_0 = H\) and \(l_1 = L\). Then there exists \(\langle P_o \rangle^H\) and \(\langle P_i \rangle^L\) such that either
\[
(a) \quad \langle P_o \rangle^H \xrightarrow{y} \langle P_o \rangle^H \text{ and } \langle P_i \rangle^L \xrightarrow{y} \langle P_i \rangle^L, \text{ or}
\]
\[
(b) \quad \langle P_o \rangle^H \xrightarrow{\pi^y} \langle P_o \rangle^H \text{ and } \langle P_i \rangle^L \xrightarrow{x^y} \langle P_i \rangle^L,
\]
given the assumptions about \(S_o\) and \(S_i\). Given that \((\rho, \kappa, \sigma) \models me\) \(S\) we obtain that \((\rho, \kappa, \sigma) \models me\langle P_o \rangle^H\) and \((\rho, \kappa, \sigma) \models me\langle P_i \rangle^L\), for some suitable \(me\) taking care of the restrictions mentioned above. The analysis and Theorem 6.3 tell us that
\[
(a) \quad me(y) \in \sigma_{out}(H)(me(x)) \text{ and } me(y) \in \sigma_{in}(L)(me(x)), \text{ or}
\]
\[
(b) \quad \chi \in \sigma_{out}(H)(me(x)) \text{ and } \chi \in \sigma_{in}(L)(me(x)).
\]
This contradicts item 3 of Definition 6.6, that demands the intersection of the two sets to be empty. □

Example 6.9. It is easy to prove that the process \(S\) validated in Example 6.2 is discreet. In particular, the following two conditions hold.
\[
\bullet \quad \sigma_{out}(H)(\chi_a) \cap \sigma_{in}(L)(\chi_a) = \emptyset \cap \{\chi_b\} = \emptyset.
\]
\[
\bullet \quad \sigma_{out}(H)(\chi_b) \cap \sigma_{in}(L)(\chi_b) = \{\chi_a\} \cap \emptyset = \emptyset.
\]
As was the case for confinement, the polynomial time algorithm of Section 4 can be used to perform a polynomial time check of whether or not a process \(P\) is discreet with respect to given \(\zeta, me\).

7. RELATED WORK

There are two strains of related work: the first concerns static analysis techniques, the second (mainly) their applications to security.

Static analysis of programs aims at developing efficient techniques that may be used to obtain approximate answers about how a program executes without actually executing it. Traditionally, this has been a main component in the construction of efficient implementations of programming languages. There is a vast literature on static program analysis and we here survey some of the more important approaches; we refer to [31] for further details.

Control Flow Analysis (e.g., [40]) deals with the problem of dynamic dispatch where it is not apparent which function (or method) is actually being invoked and where an analysis is needed in order to determine this information. This is a problem that appears all the time in higher order functional languages and many developments of control flow analysis have indeed been performed for functional languages, but also object-oriented languages [35] and languages with concurrency [18] can be addressed.

Recently, Venet [41, 42] has used Abstract Interpretation [11] to analyse processes in a fragment of the \(\pi\)-calculus, with particular attention to the usage of channels. Type Systems are intimately connected to ensuring the well-formedness of programs. In recent years they have been extended with annotations and effects and are becoming a very popular tool for the analysis of calculi of computations (e.g., [1, 9, 34, 43, 44]); in our view, type systems are particularly useful when they admit principal types, and this is not the case for all of the developments cited.

These approaches are not so dissimilar as might appear at first sight. In fact, Control Flow Analyses can be expressed in the Constraint Based Formulation used here, in the terminology of Type Systems and using abstract interpretation. We refer to [10, 31] and their references for further information about the relationships among these approaches.

We now turn to the second strain of related work. The first studies in system security reach back to the 1970s and were mainly carried out in the area of operating systems; see the detailed survey by
Landwehr [24]. Denning’s book [14] reports her pioneering work, inspired also by the work by Bell and LaPadula [5], Fenton [15], and Lampson [23]. They developed methods for detecting violations of secure flow while statically analysing the code.

Recently, security classes have been formalized as types and the control of flow is based on type checking. Heintze and Riecke [22] refine Denning’s analysis and study a noninterference property on the SLam Calculus (Secure $\lambda$-calculus). Well-typed processes are such that values of low-level expressions are independent of the values of high-level parameters. Volpano et al. develop a type system to ensure secure information flow in a sequential imperative language [44]; this work was later extended by the first two authors in a concurrent, shared-memory based setting [43].

The work closest to our proposal in Section 5 is that by Abadi [1], who studies the secrecy of channels and of encrypted messages using the $spi$-calculus, an extension of the $\pi$-calculus devised for writing secure protocols. His is a more ambitious goal than ours, because the $spi$-calculus also has cryptographic primitives. Semantic correctness of the type system, formalised using testing equivalence, guarantees that there is no leaking of secret information. As for the disciplined use of channels, Abadi’s and our aims are very close, as well as for the assumptions made (except that Abadi has a further notion of Any, besides those of Public and Secret). We conjecture that the two approaches are comparable in precision. Indeed our solution $(\rho, \kappa)$ can be seen as an explicit type annotation of processes (in the manner of Exercise 5.4 of [31]) and our notion of validation corresponds to validate the type annotation. However, whereas we established that a best solution always exists (via Moore families) and gave a procedure for constructing solutions, Abadi [1] does not establish the existence of the analogous notion of principal types, and hence it is unclear whether or not a sound and complete typing algorithm exists. The semantic correctness is checked against two different dynamic notions (testing equivalence versus no leaks).

Other interesting papers in this area are [4, 12, 13, 17, 36–39]. Particularly relevant are Hennessy and Riely’s papers [37, 38] that give a type system for $D_{\pi}$, a variant of the $\pi$-calculus with explicit sites that harbour mobile processes. A well-typed process correctly uses its capabilities and never compromises the integrity of well-behaved sites. Recently also Cardelli and Gordon [9] proposed a type system for the ambient calculus ensuring that a well-typed mobile computation cannot cause certain kinds of run-time faults, even when capabilities can be exchanged between processes.

The idea of static analysis for security has been followed also in the Java world, for example in the Java Bytecode Verifier [25]. Also, Abadi faces in [2] the problem of implementing secure systems and proposes to use full abstraction to check that the compiled code enjoys the same security properties of the source program.

The dynamic point of view has been adopted by a certain number of information flow models [16, 19, 26, 27] (to cite only a few). Here, only the external observable behaviour is the object of the analysis. A classical example is the noninterference model of [19, 20], where the actions of the group of high level users have no effect on what the group of low level users can observe. McCullough [26, 27] extends this definition to cope with non determinism. Focardi and Gorrieri [16] use a process algebras setting, by using SPA (Security Process Algebra), an extension of CCS [28]. Our property of no read-up/no write-down could be considered a variant of the noninterference property, studied by most of the authors mentioned above.

8. CONCLUSIONS

We presented a control flow analysis for the $\pi$-calculus that statically predicts how names will be bound to actual channels at run-time. The only extensions made to the syntax of processes are that a channel $x$ is explicitly assigned to a restricted name, and that an input action has the form $x(y^0)$, making explicit the role of the placeholder $y$; this change was motivated by the inclusion of $\alpha$-conversion in the semantics. Annotations can be done mechanically and do not affect the behaviour of processes; typically, all markers will be different. The results of our analysis approximate the actual solutions, because they may give a super-set of the corresponding actual values.

We defined judgements on solutions and processes and a set of clauses that operate on judgements so as to validate the correctness of the solution. We proved that a best solution always exists and we also presented a constructive procedure for generating solutions, which is in $O(N^5)$.

A recent result [33] shows that time complexity can be reduced to $O(n^3)$.\footnote{A recent result [33] shows that time complexity can be reduced to $O(n^3)$.}
point where we addressed reachability is in the two clauses for matching in Tables 2 and 5. There, we avoid analysing the “continuation” if the match cannot possibly be passed. Similar considerations could be applied to input and output actions, so as to avoid analysing the continuation, e.g., in case the empty set is associated with the subject of the action (see [8]).

We described how our analysis can be used to establish two simple properties of security. The first property we called confinement, the second property we called discreetness. The two properties are orthogonal, as the first puts constraints on the communications to the environment, and the second property enforces a discipline on the communications internal to the process under analysis. So, one can separately check them on a process.

An immediate extension to our (two-level) notion of confinement consists of defining a hierarchy of classification levels associated with channels. Equally immediate is extending our analysis in Section 5 to statically check that a high level of information is never transmitted on a channel with a lower level of security classification.

We did not consider, but we plan to, the more general notion of the no read-up/no write-down property that assigns levels of confidentiality also to the exchanged data (i.e., the objects of input and output actions). Processes with low level clearance are then not allowed to access (i.e., they can neither send nor receive) highly classified data. Note in passing that (an extension of) our first security property is not enough for getting the full version of the nru/nwd property; indeed, processes with different clearances are allowed to send objects with different classification along the same channel, while this is forbidden in the case considered in Section 5. A further extension to the nru/nwd property might consider to have a partial order of clearance levels (see Chapter 5 of [14]).

Future work will consider calculi more oriented to security. The last two authors have already considered in [21, 32] the ambient calculus [9] that extends the \( \pi \)-calculus with an explicit notion of mobility of computation. The main application concerns validating the protectiveness of a firewall, meaning that it does not allow agents to enter unless they know the required passwords. We are also interested in the spi-calculus [3] that enriches the \( \pi \)-calculus with primitives for encryption and decryption and distinguishes between data and channels. The core analysis for the spi-calculus should remain the same as presented here, while some sort of data flow analysis seems necessary to track data manipulations. It would also be interesting to study authentication properties. Preliminary work on a control flow analysis for the spi-calculus can be found in Bodei’s thesis [6], where a notion of secrecy and a restricted form of authentication are considered.

ACKNOWLEDGMENTS

We thank Martin Abadi, Andrew Gordon, Roberto Gorrieri, and Dennis Volpano for interesting discussions. Special thanks are due to the referees for their precise and invaluable suggestions.

A preliminary version of Sections 1, 2, 3.1, and 4 appeared in [7]; some ideas of Section 5 are presented in [8]. We thank René Rydhof Hansen for constructing two web-based systems for checking confinement and discreetness based on the algorithms reported here. They are available from at http://www.daimi.au.dk/~fn/FlowLogic.html under the entries for [7] and [8].

The first two authors have been partially supported by the CNR Progetto Strategico Modelli e Metodi per la Matematica e l’Ingegneria and by the MURST Progetto Tecniche Formali per la Specifica, l’Analisi, la Verifica, la Sintesi e la Trasformazione di Sistemi Software. The last two authors have been partially supported by the DART project.

REFERENCES