Secrecy by Typing in Security Protocols*

Martín Abadi
Systems Research Center
Compaq
ma@pa.dec.com

December 8, 1998

Abstract

We develop principles and rules for achieving secrecy properties in security protocols. Our approach is based on traditional classification techniques, and extends those techniques to handle concurrent processes that use shared-key cryptography. The rules have the form of typing rules for a basic concurrent language with cryptographic primitives, the spi calculus. They guarantee that, if a protocol typechecks, then it does not leak its secret inputs.

*A preliminary version of this paper was presented in conjunction with the Third International Symposium on Theoretical Aspects of Computer Software in September 1997, and appeared in its proceedings, volume 1281 of Springer Verlag *Lecture Notes in Computer Science*, pages 611–638.

Contents

1 Introduction

Security is an elusive cocktail with many rare ingredients. For any given security protocol, one may want properties of integrity, confidentiality, availability, various forms of anonymity and non-repudiation, and more. Seldom does a protocol achieve all the properties that its designers intended. Moreover, even when a protocol is sound, it is often delicate to define all its important properties, and difficult to prove them.

The tasks of protocol design and analysis can be simplified by having principles that make it easier to achieve particular security objectives, in isolation, and rules that help recognize when these objectives have been achieved (cf. [WL94, AN95, AN96, Syv96, Aur97]). For example, if we wish to obtain some availability properties and are concerned about denial of service attacks, we may design our protocols in such a way that there is an obvious, small bound on the amount of work that any principal will do in response to any message. One could relax this bound for messages from trusted, authenticated principals; but trust and authentication are not always correct, so letting availability depend on them should not be done lightly.

In this paper, we develop informal principles and formal rules for achieving secrecy properties in security protocols. These principles and rules are based on traditional concepts of classification and information flow [Den82, Gas88], extended to deal with concurrent processes that use shared-key cryptography. In particular, in analyzing a protocol, we label each piece of data and each communication channel as either secret or public. Secret data should not be sent on public channels, and secret channels should not be made available indiscriminately.

In our approach, encryption keys are pieces of data, and as such they are labelled. The result of encrypting secret data under a secret key can be made public, but only with some precautions. For example, given a secret bit b and a secret key K, we cannot simply publish b under K if we may also publish 0 or 1 under K: an attacker could deduce the value of b by comparing ciphertexts. The rules of this paper capture a sufficient set of simple precautions that permit the publication of ciphertexts that contain secrets.

The rules have the form of typing rules for a basic concurrent language, the spi calculus [AG97a, AG97b, AG97c, AG98]; this calculus is an extension of the pi calculus [MPW92] with shared-key cryptographic primitives. The purpose of these rules is rather different from those of standard typing rules for related languages (such as those of Pierce and Sangiorgi [PS96]). The rules guarantee that, if a protocol typechecks, then it does not leak its secret inputs. This secrecy is obtained independently of any other feature (or any flaw) of the protocol. For example, the rules may guarantee that a protocol does not leak the contents of certain messages, without concern for whether message replay is possible. The notion of leaking is formalized in terms of testing equivalence [DH84, BN95]: roughly, a process $P(x)$ does not leak the input x if a second process Q cannot distinguish running in parallel with $P(M)$ from running in parallel with $P(N)$, for every M and N.

These typing rules are helpful, in that following them may lead to designs that are clearer, more robust, and more likely to be sound. Furthermore, they enable us to give simple proofs of properties that would be hard to establish from first principles. However, the secrecy theorems that we obtain should be taken with a grain of salt: they are dependent on the choice of a particular model, that of the spi calculus. This model is fairly accurate and expressive, but does not take into account issues of key length, for example.

The next section explains, informally, our approach for achieving secrecy. Section 3 is a review of the spi calculus. (The spi calculus presented is a generalization of that defined originally [AG97b]; it includes polyadic constructs [Mil91].) Section 4 provides the typing rules for the spi calculus, and section 5 shows that these rules can be applied to prevent undesirable flows of information. Section 6 illustrates the use of the rules in examples. Finally, sections 7 and 8 suggest further work and conclude.

Throughout this paper, we often opt for simplicity over generality, considering this work only a first exploration of a promising approach. In particular, we take a binary, Manichaean view of secrecy. According to this view, the world is divided into system and attacker, and a secret is something that the attacker does not have. A more sophisticated view of secrecy would distinguish various principals within the system, and enable us to discuss which of these principals have a given piece of data. In our binary view, however, we can vary the boundary between system and attacker, with some of the same benefits.

2 Some Principles for Secrecy

In the security literature there are well-known methods for controlling flows of information. Typically, these methods rely on putting objects and subjects into security classes, and guaranteeing that no data flows from higher classes to lower classes. In some of these methods, security classes are formalized as types, and the control of flows of information relies on typing rules (e.g., [VIS96]).

We adapt some of that work to security protocols. This section describes our approach informally, along with the main difficulties that it addresses. It is probable that some of the basic observations of this section have already been made, but they do not seem to be documented in the open literature.

2.1 On Rules in Distributed Systems

In a centralized system, an administrator that controls all the hardware in the system may hope to control all information flows. If all communication is mediated by the system hardware, the control of all information flows is plausible at least in principle. In particular, the administrator may check user programs before running them, statically, or may apply some dynamic checks.

In a distributed system, on the other hand, no single administration may control all the hardware. No part of the system may be able to check that the software of any other part is constructed according to a given set of rules. At best, each principal can analyze the programs that it receives from other principals, as well as all other messages.

Therefore, whatever rules we propose, they should be such that an attacker satisfies them vacuously as a result of physical laws or other reasonable premises. In some situations, we may assume that the attacker cannot guess certain keys, but we cannot expect to restrict the code that the attacker runs. Our rules should constrain only the principals that want to protect their secrets from the attacker.

2.2 Preliminaries on Keys and Channels

As mentioned in the introduction, this paper concerns shared-key protocols. We write $\{M\}_K$ for the result of encrypting M with K, using a shared-key cryptosystem such as DES [DES77]. With shared-key cryptography, secrecy can be achieved by communication on public channels under secret keys.

In addition to public channels, on which anyone may communicate, we consider channels with some built-in protection. We restrict attention to channels on which the same principals can send and receive. On a single machine, channel protection can be provided by an operating system that mediates communication between user processes; in a distributed system, the protection can be implemented cryptographically.

The ability to communicate on a channel is often determined by possession of a capability, such as a password or a key. (In the pi calculus and the spi calculus, the name for a channel is the capability for the channel.) A public channel is one for which the capability is public; similarly, a secret channel is one for which the capability is secret.

2.3 Classifying Data

We consider only three classes of data:

- *Public* data, which can be communicated to anyone,
- *Secret* data, which should not be leaked,
- *Any* data, that is, arbitrary data.

It should be possible to generalize our rules to richer classification structures, with more than three classes, but such a generalization is not essential for our immediate purposes.

We use the symbols T and R to range over the classes *Secret*, *Public*, and *Any*. We refer to *Secret*, *Public*, and *Any* as classes, levels, or types; the difference is one of emphasis at most. In informal discussions, we continue to use the terms "secret" and "public", and often do not consider explicitly the class *Any*.

Encryption keys are data, so our classification scheme applies to them. Several different levels can be associated with a key:

- its level as a piece of data,
- the levels of the data that it is used to encrypt,
- the levels of the resulting ciphertexts.

However, not all combinations are possible, as for example a public key should not be used to turn secret data into public ciphertexts. It is simplest to retain only one level for each key. Similarly, we associate a single classification with each channel. We adopt the following principles:

> The result of encrypting data with a public key has the same classification as the data, while the result of encrypting data with a secret key may be made public.
>
> Only public data can be sent on public channels, while all kinds of data may be sent on secret channels.

The relation $T <: R$ holds if T equals R or if R is *Any*. If a piece of data has level T and $T <: R$, then the piece of data has level R as well. Because a piece of data of level *Any* could be of level *Secret*, it should not be leaked. On the other hand, a piece of data of level *Any* could be of level *Public*, so it cannot be used as a secret. For example, it cannot be used as a secret key for encrypting secret data. Thus, if all we know about a piece of data is that it has level *Any*, then we should protect it as if it had level *Secret*, but we can exploit it only as if it had level *Public*. This piece of data is therefore not very useful for constructing channel capabilities or encryption keys; we find it cleaner to forbid these uses altogether; they could be accommodated, but with substantial restrictions and limited benefit.

2.4 Classifying Inputs

Whereas each principal may know the classification of the data that it creates, the principal may not always know the classification of the data that it acquires through communication with other principals. Data that arrives in clear on public channels can be presumed to be public. On the other hand, data that arrives with some protection may be either secret or public.

The participants of protocols typically know how to handle each of the fields of the encrypted messages that they receive, as in the following example (inspired by the Needham-Schroeder protocol [NS78]):

$$\begin{array}{lll} \text{Message 1} & A \rightarrow S: & A, B \\ \text{Message 2} & S \rightarrow A: & \{A, B, I_A, \{I_B\}_{K_{SB}}\}_{K_{SA}} \\ \text{Message 3} & A \rightarrow B: & \{I_B\}_{K_{SB}} \end{array}$$

In this protocol, the principals A and B share keys K_{SA} and K_{SB} with the server S, respectively. The server provides some confidential information I_A to A and I_B to B, in response to a request from A. When A receives a message from the server, it decrypts it, retrieves I_A, and forwards $\{I_B\}_{K_{SB}}$ to B. It is crucial that A be able to recognize when this action is appropriate. For example, if a principal X plays the role of A and B in two concurrent runs of the protocol, it should be able to recognize whether a message is an instance of Message 2 or an instance of Message 3. If X mistakes an instance $\{I_X\}_{K_{SX}}$ of Message 3 for an instance of Message 2, then X would forward part of I_X in clear.

As in this example, it is common for principals to deduce the sensitivity of inputs from the expected kind of a message or other implicit information. Such implicit information is often incorrect and often hard to analyze [AN96].

It is clearer to label explicitly each component of a message with a classification, avoiding the dependence on implicit context. This labelling is important only for messages on secret channels or under secret keys. All other messages can contain only public information (helpful or misleading, but always public); labelling their components would be redundant.

Alternatively, we may adopt a standard format for all messages on secret channels or under secret keys. The format should guarantee that there is a standard way to attach classifications to the parts of each message, avoiding again the dependence on implicit context. In our rules, we adopt this scheme. Each message on a secret channel has three components, the first of which has level *Secret*, the second *Any*, and the third *Public*. Each message under a secret key has those three components plus a confounder component, as discussed next.

Both of these schemes are implementations of the following principle:

> Upon receipt of a message, it should be easy to decide which parts of the contents are sensitive information, if any. This decision is least error-prone when it does not depend on implicit context.

2.5 Confounders

As noted in the introduction, given a secret bit b and a secret key K, we cannot simply publish b under K if we may also publish 0 or 1 under K: an attacker could deduce the value of b by comparing ciphertexts. On the other hand, we can create a fresh value n, then publish the concatenation of b and n under K. A value such as n is sometimes called a *confounder*. The purpose of n is to guarantee that the resulting ciphertext differs from all previous ones. The resulting ciphertext will differ from all future ones too if each ciphertext includes a fresh confounder, always in the same position. In general (unless one is concerned about encrypting known plaintext), confounders need not be kept secret.

Confounders are not needed if encryption is history-dependent, so a different transformation is applied to each message. In particular, confounders are not needed when encryption is done with a stream cipher [MvOV96, chapter 6] or with a block cipher in an appropriate chaining mode [MvOV96, section 7.2.2]. The remarks of this section are not intended to apply to protocols built on such algorithms.

Independently of the choice of cipher, confounders are not needed in protocols where all ciphertexts generated are guaranteed to be different. Unfortunately, it is not always clear whether this guarantee is offered.

As an example, we consider a simple protocol where a principal A sends a message M to a principal B under a shared key K_{AB}. Before A sends the message, B provides a challenge N_B, fresh for each message; the challenge serves as a proof of freshness, and protects against replays.

$$\begin{array}{lll} \text{Message 1} & B \rightarrow A: & N_B \\ \text{Message 2} & A \rightarrow B: & \{M, N_B\}_{K_{AB}} \end{array}$$

We may reason that all the ciphertexts from A are different, since each of them includes a fresh challenge. However, this reasoning is incorrect. An attacker C could provide a challenge instead of B, and A would reply without noticing that the challenge did not come from B. The attacker may pick the same challenge N_C twice in a row. In that case, the ciphertexts with which A responds, $\{M, N_C\}_{K_{AB}}$ and $\{M', N_C\}_{K_{AB}}$, are identical if and only if the cleartexts M and M' are identical. Thus, C can find out whether A is sending two identical cleartexts, even without knowing the key K_{AB}. Thus, the protocol is leaking some information.

In order to prevent this small leak, A should create a confounder N_A for each encryption. The modified protocol is:

$$\begin{array}{lll} \text{Message 1} & B \rightarrow A: & N_B \\ \text{Message 2} & A \rightarrow B: & \{M, N_B, N_A\}_{K_{AB}} \end{array}$$

This protocol is analyzed in [AG97c], where it is proved that the protocol guarantees the secrecy of M.

It is prudent to adopt the following principle:

> If each encrypted message of a protocol includes a freshly generated confounder in a standard position, then the protocol will not generate the same ciphertext more than once. Confounders should be used unless it is obvious that they are not needed.

2.6 Implicit Flows

A system may reveal something about one of its parameters even if this parameter never appears explicitly in a message. For example, the system may send different cleartext messages depending on the value of the parameter. An attacker could deduce something about the parameter from patterns of communication. Such a leak of information is sometimes called an *implicit flow.*

It is of course important to restrict implicit flows. For this purpose, we may forbid any comparison that involves pieces of sensitive data and that could be followed by actions that would reveal the result of the comparison.

It is also important not to push this restriction to uncomfortable extremes. Many protocols exhibit implicit flows in some form, usually without severe undesirable effects. As an example, we consider again this protocol:

$$\begin{array}{lll} \text{Message 1} & A \rightarrow S: & A, B \\ \text{Message 2} & S \rightarrow A: & \{A, B, I_A, \{I_B\}_{K_{SB}}\}_{K_{SA}} \\ \text{Message 3} & A \rightarrow B: & \{I_B\}_{K_{SB}} \end{array}$$

An attacker can send an arbitrary message to A, instead of Message 2. On receipt of this message, A performs a test that involves the secret K_{SA}, and branches on the result of this test. The reaction of A depends visibly on whether the message is a valid ciphertext under K_{SA}. One could regard this as an implicit flow, but perhaps one of little importance because the chance that an independently created message will be a valid ciphertext under K_{SA} is negligible. We can allow this implicit flow; it is harmless in our model.

Our (tentative) policy on implicit flows is summarized in the following principle:

> Implicit flows of information should be prevented, except perhaps when the likelihood of the implicit flow is no greater than the likelihood that an attacker will guess the information.

2.7 Further Principles

The principles discussed above suffice as the basis for our rules and theorems, but they are not comprehensive. In practice, several additional warnings and techniques are important. Here are a few.

- It is often hard not to leak the size of a secret. The use of padding in encrypted messages can help in this respect.
- It is prudent to minimize the benefit that an attacker may derive from discovering any one secret. In particular, the same key should not be used to protect a great volume of sensitive traffic, because then even a brute-force attack on the key may be profitable.
- Weak secrets, such as passwords, should be protected from brute-force attacks (see for example [Sch96, MvOV96]).

Undoubtedly there are more.

3 The Untyped, Polyadic Spi Calculus

In the remainder of this paper, we develop rules for checking protocols, relying on the principles of section 2. Whereas those principles are informal, a rigorous definition of the rules requires a formal notation for describing protocols; a rigorous analysis of the rules requires a semantics for the notation. We describe protocols as spi-calculus processes and we reason about them using the operational semantics of the spi calculus and the induced relation of testing equivalence.

This section presents the version of the spi calculus that serves as the setting for our formal work, defining its syntax, operational semantics, and testing equivalence. The main novelty with respect to the earlier versions of the spi calculus is the introduction of polyadic forms: each input, output, encryption, and decryption operation applies to an arbitrary number of pieces of data, rather than to a single piece. This novelty is important for the typing rules of the next section. However, this novelty is not substantial, as in particular it does not affect the expressiveness of the spi calculus. Therefore, our presentation is mostly a review. Most of this material is derived from the earlier presentations of the spi calculus; it includes ideas common in the pi-calculus literature.

3.1 Syntax

We assume an infinite set of *names* and an infinite set of *variables*. We let m, n, p, q, and r range over names, and let w, x, y, and z range over variables. We identify expressions up to renaming of bound names and variables, and write $P[M_1/x_1, \dots, M_k/x_k]$ for the outcome of replacing each free occurrence of x_i in P with M_i (renaming in P any bound name or variable that occurs in M_i), for $i \in 1..k$.

The set of *terms* is defined by the grammar:

$L, M, N ::=$	terms
$\quad n$	name
$\quad (M, N)$	pair
$\quad 0$	zero
$\quad suc(M)$	successor
$\quad \{M_1, \dots, M_k\}_N$	shared-key encryption ($k \geq 0$)
$\quad x$	variable

The term $\{M_1, \dots, M_k\}_N$ represents the ciphertext obtained by encrypting M_1, $\dots$, M_k under the key N. The key is an arbitrary term; typically, we use names as keys because, in the spi calculus, names are unguessable capabilities.

The set of *processes* is defined by the grammar:

$P, Q ::=$	processes
$\quad \overline{M}\langle N_1, \ldots, N_k\rangle.P$	output ($k \geq 0$)
$\quad M(x_1, \ldots, x_k).P$	input ($k \geq 0$)
$\quad \mathbf{0}$	nil
$\quad P \mid Q$	parallel composition
$\quad !P$	replication
$\quad (\nu n)P$	restriction
$\quad [M \textit{ is } N]\ P$	match
$\quad \textit{let } (x, y) = M \textit{ in } P$	pair splitting
$\quad \textit{case } M \textit{ of } 0 : P\ \textit{suc}(x) : Q$	integer case
$\quad \textit{case } L \textit{ of } \{x_1, \ldots, x_k\}_N \textit{ in } P$	shared-key decryption ($k \geq 0$)

The name n and the variables x, y, x_1, …, x_k are bound in these processes. Most of these constructs should be familiar from earlier process algebras; see [AG97b] for a review, and see below for an operational semantics. Intuitively, the meaning of these constructs is as follows.

- The process $\overline{M}\langle N_1, \ldots, N_k\rangle.P$ outputs $N_1, \ldots, N_k$ on M and then behaves as P; the output happens only if M is a name and there is another process ready to receive k inputs on M. We use $\overline{M}\langle N_1, \ldots, N_k\rangle$ as an abbreviation for $\overline{M}\langle N_1, \ldots, N_k\rangle.\mathbf{0}$, so $\overline{M}\langle N_1, \ldots, N_k\rangle$ is a process that may output $N_1, \ldots, N_k$ on M and then stop.

  (In the terminology of the pi-calculus literature, the calculus defined in this section is synchronous because $\overline{M}\langle N_1, \ldots, N_k\rangle.P$ triggers P after communication. The asynchronous fragment is obtained by replacing $\overline{M}\langle N_1, \ldots, N_k\rangle.P$ with $\overline{M}\langle N_1, \ldots, N_k\rangle$ in the grammar; the results of this paper apply to the asynchronous fragment without change.)

- The process $M(x_1, \ldots, x_k).P$ is ready to receive k inputs $N_1, \ldots, N_k$ on M, and then to behave as $P[N_1/x_1, \ldots, N_k/x_k]$.

- The process $\mathbf{0}$ does nothing.

- The process $P \mid Q$ is the parallel composition of P and Q. Given a family of processes $P_1, \ldots, P_k$, we write $\prod_{i \in 1..k} P_i$ for their parallel composition $P_1 \mid \ldots \mid P_k$.

- The process $!P$ behaves as infinitely many copies of P running in parallel.

- The process $(\nu n)P$ makes a new name n and then behaves as P.
- The process $[M \textit{ is } N]\ P$ behaves as P if M and N are equal, and otherwise is stuck.
- The process $\textit{let } (x, y) = M \textit{ in } P$ behaves as $P[N/x, L/y]$ if M is a pair (N, L), and it is stuck if M is not a pair.
- The process $\textit{case } M \textit{ of } 0 : P\ \textit{suc}(x) : Q$ behaves as P if M is 0, as $Q[N/x]$ if M is $\textit{suc}(N)$ for some N, and otherwise is stuck.
- The process $\textit{case } L \textit{ of } \{x_1, \ldots, x_k\}_N \textit{ in } P$ attempts to decrypt L with the key N; if L has the form $\{M_1, \ldots, M_k\}_N$, then the process behaves as $P[M_1/x_1, \ldots, M_k/x_k]$, and otherwise the process is stuck.

Following these grammars, it is possible to write expressions that many standard typing systems would exclude, for example $\textit{suc}((0, 0))$ where an arithmetic operation is applied to a pair. The typing system of section 4 has different concerns, so it does not exclude this expression; a combination with a standard typing system may therefore be appealing, but it is not necessary for our purposes (see section 7).

The polyadic notations (input, output, encryption, decryption for $k \neq 1$) could be defined from the corresponding unary notations. For example, we could have set:

$$\begin{array}{rcl}\textit{case } L \textit{ of } \{x_1, x_2\}_N \textit{ in } P & \triangleq & \textit{case } L \textit{ of } \{y\}_N \textit{ in} \\ & & \quad \textit{let } (x_1, x_2) = y \textit{ in } P\end{array}$$

where variable y is fresh. However, as mentioned above, the polyadic notations are useful for typing. They also introduce a typing difficulty, when arities do not match, as in $\textit{case } \{M_1, M_2, M_3\}_N \textit{ of } \{x_1, x_2\}_N \textit{ in } P$. This typing difficulty could be overcome with an appropriate system of sorts.

In addition to the polyadic notations, we use the following standard abbreviations for any $k \geq 2$:

$$\begin{array}{rcl}(N_1, \ldots, N_k, N_{k+1}) & \triangleq & ((N_1, \ldots, N_k), N_{k+1}) \\ \textit{let } (x_1, \ldots, x_k, x_{k+1}) = N \textit{ in } P & \triangleq & \textit{let } (y, x_{k+1}) = N \textit{ in} \\ & & \quad \textit{let } (x_1, \ldots, x_k) = y \textit{ in } P\end{array}$$

where variable y is fresh.

We write $\textit{fn}(M)$ and $\textit{fn}(P)$ for the sets of names free in term M and process P respectively, and write $\textit{fv}(M)$ and $\textit{fv}(P)$ for the sets of variables free in M and P respectively. An expression is closed if it has no free variables. A closed expression may have free names.

3.2 Commitment

We give an operational semantics for the spi calculus by defining a commitment relation, in the style of Milner [Mil95]. The definition of commitment depends on some new syntactic forms, *abstractions* and *concretions*. An abstraction is an expression of the form $(x_1, \ldots, x_k)P$, where $k \geq 0$, $x_1, \ldots, x_k$ are bound variables, and P is a process. A concretion is an expression of the form $(\nu m_1, \ldots, m_l)\langle M_1, \ldots, M_k\rangle P$, where $l, k \geq 0$, $M_1, \ldots, M_k$ are terms, P is a process, and the names $m_1, \ldots, m_l$ are bound in $M_1, \ldots, M_k$ and P. An *agent* is an abstraction, a process, or a concretion. We use the metavariables A and B to stand for arbitrary agents, C for concretions, and F for abstractions.

We extend the operations of restriction and of parallel composition with a process, to abstractions:

$$\begin{array}{rcl} (\nu m)(x_1, \ldots, x_k)P & = & (x_1, \ldots, x_k)(\nu m)P \\ Q \mid (x_1, \ldots, x_k)P & = & (x_1, \ldots, x_k)(Q \mid P) \end{array}$$

assuming that $x_1, \ldots, x_k \notin fv(Q)$, and to concretions:

$$\begin{array}{rcl} (\nu m)(\nu n_1, \ldots, n_k)\langle M_1, \ldots, M_l\rangle P & = & (\nu m, n_1, \ldots, n_k)\langle M_1, \ldots, M_l\rangle P \\ Q \mid (\nu n_1, \ldots, n_k)\langle M_1, \ldots, M_l\rangle P & = & (\nu n_1, \ldots, n_k)\langle M_1, \ldots, M_l\rangle (Q \mid P) \end{array}$$

assuming that $m \notin \{n_1, \ldots, n_k\}$ and $\{n_1, \ldots, n_k\} \cap fn(Q) = \emptyset$. We define the dual composition $A \mid Q$ symmetrically. (The definition of $(\nu m)(\nu n_1, \ldots, n_k)\langle M_1, \ldots, M_l\rangle P$ preserves the distinctness of bound names in $(\nu m, n_1, \ldots, n_k)\langle M_1, \ldots, M_l\rangle P$ but, unlike the original definition [AG97b], it does not guarantee that these names occur in $\langle M_1, \ldots, M_l\rangle$. The change is crucial in the analysis of the rule (Comm Res) in Lemma 9 below.)

If F is the abstraction $(x_1, \ldots, x_k)P$ and C is the concretion $(\nu n_1, \ldots, n_l)\langle M_1, \ldots, M_k\rangle Q$, and if $\{n_1, \ldots, n_l\} \cap fn(P) = \emptyset$, we define the processes $F@C$ and $C@F$ as follows:

$$\begin{array}{rcl} F@C & \triangleq & (\nu n_1) \ldots (\nu n_l)(P[M_1/x_1, \ldots, M_k/x_k] \mid Q) \\ C@F & \triangleq & (\nu n_1) \ldots (\nu n_l)(Q \mid P[M_1/x_1, \ldots, M_k/x_k]) \end{array}$$

The *reduction relation* $>$ is the least relation on closed processes that satisfies the following axioms:

(Red Repl)
$$!P \;>\; P \mid !P$$
(Red Match)
$$[M \text{ } is \text{ } M]\, P \;>\; P$$
(Red Let)
$$let\ (x, y) = (M, N)\ in\ P \;>\; P[M/x, N/y]$$
(Red Zero)
$$case\ 0\ of\ 0 : P\ suc(x) : Q \;>\; P$$
(Red Suc)
$$case\ suc(M)\ of\ 0 : P\ suc(x) : Q \;>\; Q[M/x]$$
(Red Decrypt)
$$case\ \{M_1, \ldots, M_k\}_N\ of\ \{x_1, \ldots, x_k\}_N\ in\ P \;>\; P[M_1/x_1, \ldots, M_k/x_k]$$

A *barb* is a name m (representing input) or a co-name $\overline{m}$ (representing output). An *action* is a barb or the distinguished *silent action* τ. The *commitment relation* is written $P \xrightarrow{\alpha} A$, where P is a closed process, α is an action, and A is a closed agent. It is defined by the rules:

(Comm Out)
$$\frac{}{\overline{m}\langle M_1, \ldots, M_k\rangle.P \xrightarrow{\overline{m}} (\nu)\langle M_1, \ldots, M_k\rangle P}$$

(Comm In)
$$\frac{}{m(x_1, \ldots, x_k).P \xrightarrow{m} (x_1, \ldots, x_k)P}$$

(Comm Inter 1)
$$\frac{P \xrightarrow{m} F \quad Q \xrightarrow{\overline{m}} C}{P \mid Q \xrightarrow{\tau} F@C}$$

(Comm Inter 2)
$$\frac{P \xrightarrow{\overline{m}} C \quad Q \xrightarrow{m} F}{P \mid Q \xrightarrow{\tau} C@F}$$

(Comm Par 1)
$$\frac{P \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} A \mid Q}$$

(Comm Par 2)
$$\frac{Q \xrightarrow{\alpha} A}{P \mid Q \xrightarrow{\alpha} P \mid A}$$

(Comm Res)
$$\frac{P \xrightarrow{\alpha} A \quad \alpha \notin \{m, \overline{m}\}}{(\nu m)P \xrightarrow{\alpha} (\nu m)A}$$

(Comm Red)
$$\frac{P > Q \quad Q \xrightarrow{\alpha} A}{P \xrightarrow{\alpha} A}$$

3.3 Testing Equivalence

A *test* is a pair (Q, β) consisting of a closed process Q and a barb β. We say that P *passes* a test (Q, β) if and only if

$$(P \mid Q) \xrightarrow{\tau} Q_1 \ldots \xrightarrow{\tau} Q_n \xrightarrow{\beta} A$$

for some $n \geq 0$, some processes $Q_1, \ldots, Q_n$, and some agent A. We obtain a testing preorder $\sqsubseteq$ and a testing equivalence $\simeq$ on closed processes:

$$\begin{array}{lcl} P \sqsubseteq P' & \triangleq & \text{for any test } (Q,\beta), \text{ if } P \text{ passes } (Q,\beta) \text{ then } P' \text{ passes } (Q,\beta) \\ P \simeq P' & \triangleq & P \sqsubseteq P' \text{ and } P' \sqsubseteq P \end{array}$$

A *strict barbed simulation* is a binary relation $\mathcal{S}$ on closed processes such that $P \mathrel{\mathcal{S}} P'$ implies:

(1) for every barb β, if $P \xrightarrow{\beta} A$ for some A then $P' \xrightarrow{\beta} A'$ for some A',

(2) for every P_1, if $P \xrightarrow{\tau} P_1$ then there exists P_1' such that $P' \xrightarrow{\tau} P_1'$ and $P_1 \mathrel{\mathcal{S}} P_1'$.

A *strict barbed bisimulation* is a relation $\mathcal{S}$ such that both $\mathcal{S}$ and $\mathcal{S}^{-1}$ are strict barbed simulations. This definition is somewhat stronger than that of barbed bisimulations [AG97b]. However, barbed bisimulations and strict barbed bisimulations are alike in many respects: they are sensitive to τ steps and to the branching structure of processes, but, unlike standard bisimulations [AG97b], they are not sensitive to the contents of some messages, so for example $\overline{c}\langle 0 \rangle$ and $\overline{c}\langle suc(0) \rangle$ can be related although they output different terms.

The following lemma provides a method for proving testing equivalence:

Lemma 1 *If for every closed process Q there exists a strict barbed bisimulation $\mathcal{S}$ such that $(P \mid Q) \mathrel{\mathcal{S}} (P' \mid Q)$, then $P \simeq P'$.*

Proof The lemma is a consequence of earlier results [AG97b], but we give a simple direct proof, since there is one. We argue that if P passes a test (Q, β) then so does P', assuming that there exists a strict barbed bisimulation $\mathcal{S}$ such that $(P \mid Q) \mathrel{\mathcal{S}} (P' \mid Q)$. (Symmetrically, if P' passes a test (Q, β) then so does P.)

If P passes (Q, β), then

$$(P \mid Q) \xrightarrow{\tau} Q_1 \ldots \xrightarrow{\tau} Q_n \xrightarrow{\beta} A$$

for some agent A and processes $Q_1, \ldots, Q_n$, for some $n \geq 0$. By the definition of strict barbed simulation, there exist $Q'_1, \ldots, Q'_n$ and A' such that $Q_i \, \mathcal{S} \, Q'_i$ for all $i \leq n$, and

$$(P' \mid Q) \xrightarrow{\tau} Q'_1 \ldots \xrightarrow{\tau} Q'_n \xrightarrow{\beta} A'$$

Therefore, P' passes (Q, β). $\square$

Earlier presentations of the spi calculus define and study several equivalences in addition to testing equivalence. In the context of other process algebras, the work of Focardi and Gorrieri also investigates several equivalences and their relation to security properties [FG95, FG97].

4 The Typing System

This section describes our rules for controlling information flow in the spi calculus. They are based on the ideas of section 2. While there are several ways of formalizing those ideas, we embody them in a typing system for the spi calculus. This typing system is simple enough that it can be enforced statically; in fact, Simon Gay has recently implemented it [Gay97].

Our main results for this typing system are in section 5. They imply that if a process P typechecks then it does not leak the values of parameters of level *Any*. In examples, these parameters are typically the payload of messages of a protocol. Despite their secrecy, none of these parameters is declared with level *Secret*. However, the process P may produce terms of level *Secret* during its execution (for example, as encryption keys) using the restriction construct (ν). For instance, P may be $(\nu K)(\nu m)(\nu n)\overline{c}\langle\{m, x, 0, n\}_K\rangle$ where x is of level *Any* and c is of level *Public* and where we can assign the level *Secret* to the bound names K, m, and n. Our results imply that this process P does not leak the value of x, in the sense that $P[M/x]$ and $P[N/x]$ are testing equivalent for all closed terms M and N. Thus, the typing system is meant to protect parameters of level *Any* relying on dynamically generated names of level *Secret*.

The typing system gives rules for three kinds of assertions (or judgments):

- "$\vdash E$ well-formed" means that environment E is well-formed.
- "$E \vdash M : T$" means that term M is of class T in E.
- "$E \vdash P : Ok$" means that process P typechecks in E.

4.1 Environments

An environment is a list of distinct names and variables with associated levels. In addition, each name n has an associated term of the form $\{M_1, \ldots, M_k, n\}_N$ for some $k \geq 0$. Intuitively, this association means that the name n may be used as a confounder only in the term $\{M_1, \ldots, M_k, n\}_N$. This association is crucial for Proposition 8 below.

We write $x : T$ for variable x with level T, and $n : T :: \{M_1, \ldots, M_k, n\}_N$ for name n with level T and term $\{M_1, \ldots, M_k, n\}_N$. We write $n : T$ as a shorthand for $n : T :: \{n\}_0$, arbitrarily, when n is not needed as a confounder. The set of names and variables declared in an environment E are its *domain*; we write it $dom(E)$.

The rules for environments are:

(Environment Empty)

$$\frac{}{\vdash \emptyset \text{ well-formed}}$$

(Environment Variable)

$$\frac{\vdash E \text{ well-formed} \qquad x \notin dom(E)}{\vdash E, x : T \text{ well-formed}}$$

(Environment Name)

$$\frac{\begin{array}{c}\vdash E \text{ well-formed} \qquad n \notin dom(E) \\ E \vdash M_1 : T_1 \ \ldots \ E \vdash M_k : T_k \qquad E \vdash N : R\end{array}}{\vdash E, n : T :: \{M_1, \ldots, M_k, n\}_N \text{ well-formed}}$$

Collectively, these rules enable us to form environments as lists of variables and names with associated levels, and in addition with terms attached to the names. The empty list is written $\emptyset$ in the rule (Environment Empty).

In the rule (Environment Name), the hypotheses $E \vdash M_1 : T_1, \ldots, E \vdash M_k : T_k$ and $E \vdash N : R$ are included so that, if a variable x occurs in $\{M_1, \ldots, M_k, n\}_N$, then it is declared in E (to the left of n). Intuitively, this restriction is important because it implies that we cannot instantiate the variable x in several ways, obtaining several different terms with the same confounder, and thus defeating the purpose of confounders. For example, if K is a key of level *Secret*, the restriction will lead to excluding the process

$$(\nu n)!c(x_1, x_2, x_3).\overline{d}\langle\{x_1, x_2, x_3, n\}_K\rangle$$

which may generate many different ciphertexts with the same confounder n; note that x_1, x_2, and x_3 are bound to the right of n. On the other hand, the restriction will permit the process

$$c(x_1, x_2, x_3).(\nu n)!\overline{d}\langle\{x_1, x_2, x_3, n\}_K\rangle$$

which generates one confounder n for each ciphertext, although it sends each ciphertext many times; here x_1, x_2, and x_3 are bound to the left of n.

As Robin Milner and Benjamin Pierce have suggested [MP97], confounders are reminiscent of the idea of linearity (e.g., [KPT96]). The hypotheses of the rule (Environment Name) may be seen as a linearity requirement for the confounder n, namely that n should be used at most once as a confounder. However, this linearity requirement is rather peculiar; it does not yet seem to fit neatly into standard accounts of linearity.

4.2 Terms

The rules for terms are:

$$\text{(Level Subsumption)}\quad \frac{E \vdash M : T \qquad T <: R}{E \vdash M : R} \qquad\qquad \text{(Level Variable)}\quad \frac{\vdash E \text{ well-formed} \qquad x : T \text{ in } E}{E \vdash x : T}$$

$$\text{(Level Name)}\quad \frac{\vdash E \text{ well-formed} \qquad n : T :: \{M_1, \ldots, M_k, n\}_N \text{ in } E}{E \vdash n : T}$$

$$\text{(Level Zero)}\quad \frac{\vdash E \text{ well-formed}}{E \vdash 0 : \mathit{Public}} \qquad\qquad \text{(Level Successor)}\quad \frac{E \vdash M : T}{E \vdash \mathit{suc}(M) : T}$$

$$\text{(Level Pair)}\quad \frac{E \vdash M : T \qquad E \vdash N : T}{E \vdash (M, N) : T}$$

$$\text{(Level Encryption } \mathit{Public}\text{)} \qquad \text{with } T = \mathit{Public} \text{ if } k = 0$$
$$\frac{E \vdash M_1 : T \ \ldots \ E \vdash M_k : T \qquad E \vdash N : \mathit{Public}}{E \vdash \{M_1, \ldots, M_k\}_N : T}$$

$$\text{(Level Encryption } \mathit{Secret}\text{)}$$
$$\frac{\begin{array}{c} E \vdash M_1 : \mathit{Secret} \qquad E \vdash M_2 : \mathit{Any} \qquad E \vdash M_3 : \mathit{Public} \\ E \vdash N : \mathit{Secret} \qquad n : T :: \{M_1, M_2, M_3, n\}_N \text{ in } E \end{array}}{E \vdash \{M_1, M_2, M_3, n\}_N : \mathit{Public}}$$

The rule (Level Subsumption) says that a term of level *Public* or *Secret* has level *Any* as well.

The rules (Level Variable) and (Level Name) enable us to extract the levels of names and variables from an environment.

The rule (Level Zero) says that 0 is of level *Public*. The rule (Level Successor) says that adding one preserves the level of a piece of data. Therefore, the terms 0, $suc(0)$, $suc(suc(0))$, ... are all of level *Public*. However, a term of the form $suc(M)$ may be of other levels. For example, if M is a name or variable of level *Secret* or *Any*, then $suc(M)$ is of the same level. Intuitively, these classifications mean that the typing system works even against an attacker that may generate any number, starting from 0 and successively incrementing it. We can allow such an unrealistic attacker while preserving some guarantees for names and for numbers:

- Since names are not numbers in the spi calculus, the ability to produce any number is consistent with the inability to guess certain names—for example, names that represent secret keys. The protection of names does not require complexity-theoretic bounds that restrict the production of numbers.

- Although the terms 0, $suc(0)$, $suc(suc(0))$, ... are all of level *Public*, a process with a parameter of level *Any* need not reveal whether its value is 0, $suc(0)$, or anything else. For the attacker, the ability to generate a number does not entail the ability to deduce whether a variable has that number as its value.

The rule (Level Pair) says that the level of a pair is the level of its components. Both components must have the same level; when we pair a term of level *Public* and one of level *Secret*, we need to regard them both as having level *Any*. Thus, the rule (Level Pair) loses a little bit of typing information; it would be interesting to explore a richer, more "structural" typing system that would avoid this loss.

The rule (Level Encryption *Public*) says that k pieces of data of the same level T can be encrypted under a key of level *Public*, with a resulting ciphertext of level T. The rule (Level Encryption *Secret*) imposes more restrictions for encryption under keys of level *Secret*, because the resulting ciphertext is of level *Public*. These restrictions enforce a particular format for the contents and the use of a confounder, as explained in sections 2.4 and 2.5—the ciphertext must contain a first component of level *Secret*, a second one of level *Any*, a third one of level *Public*, and an appropriate confounder as final component. One could relax the rule (Level Encryption *Secret*) somewhat, considering also the case where the resulting ciphertext is given a level other than *Public*; the present rule strikes a reasonable balance between simplicity and flexibility. Finally, note that there is no rule for encryption for the case where N is a term of level *Any*. Thus, as explained in section 2.3, if N is a term of level *Any* and it is not known whether it is of level *Public* or *Secret*, then N cannot be used as a key.

4.3 Processes

The rules for processes are:

(Level Output *Public*)

$$\frac{\begin{array}{c} E \vdash M : \mathit{Public} \\ E \vdash M_1 : \mathit{Public} \ \ldots \ E \vdash M_k : \mathit{Public} \\ E \vdash P : \mathit{Ok} \end{array}}{E \vdash \overline{M}\langle M_1, \ldots, M_k \rangle.P : \mathit{Ok}}$$

(Level Output *Secret*)

$$\frac{\begin{array}{c} E \vdash M : \mathit{Secret} \\ E \vdash M_1 : \mathit{Secret} \qquad E \vdash M_2 : \mathit{Any} \qquad E \vdash M_3 : \mathit{Public} \\ E \vdash P : \mathit{Ok} \end{array}}{E \vdash \overline{M}\langle M_1, M_2, M_3 \rangle.P : \mathit{Ok}}$$

(Level Input *Public*)

$$\frac{E \vdash M : \mathit{Public} \qquad E, x_1 : \mathit{Public}, \ldots, x_k : \mathit{Public} \vdash P : \mathit{Ok}}{E \vdash M(x_1, \ldots, x_k).P : \mathit{Ok}}$$

(Level Input *Secret*)

$$\frac{E \vdash M : \mathit{Secret} \qquad E, x_1 : \mathit{Secret}, x_2 : \mathit{Any}, x_3 : \mathit{Public} \vdash P : \mathit{Ok}}{E \vdash M(x_1, x_2, x_3).P : \mathit{Ok}}$$

(Level Nil)

$$\frac{\vdash E \text{ well-formed}}{E \vdash \mathbf{0} : \mathit{Ok}}$$

(Level Parallel)

$$\frac{E \vdash P : \mathit{Ok} \qquad E \vdash Q : \mathit{Ok}}{E \vdash P \mid Q : \mathit{Ok}}$$

(Level Replication)

$$\frac{E \vdash P : \mathit{Ok}}{E \vdash !P : \mathit{Ok}}$$

(Level Restriction)

$$\frac{E, n : T :: L \vdash P : \mathit{Ok}}{E \vdash (\nu n)P : \mathit{Ok}}$$

(Level Match) for $T, R \in \{\mathit{Public}, \mathit{Secret}\}$

$$\frac{E \vdash M : T \qquad E \vdash N : R \qquad E \vdash P : \mathit{Ok}}{E \vdash [M \ \mathit{is} \ N] \ P : \mathit{Ok}}$$

(Level Pair Splitting) for $T \in \{Public, Secret\}$

$$\frac{E \vdash M : T \qquad E, x : T, y : T \vdash P : Ok}{E \vdash let\ (x, y) = M\ in\ P : Ok}$$

(Level Integer Case) for $T \in \{Public, Secret\}$

$$\frac{E \vdash M : T \qquad E \vdash P : Ok \qquad E, x : T \vdash Q : Ok}{E \vdash case\ M\ of\ 0 : P\ suc(x) : Q : Ok}$$

(Level Decryption *Public*) for $T \in \{Public, Secret\}$

$$\frac{E \vdash L : T \qquad E \vdash N : Public \qquad E, x_1 : T, \ldots, x_k : T \vdash P : Ok}{E \vdash case\ L\ of\ \{x_1, \ldots, x_k\}_N\ in\ P : Ok}$$

(Level Decryption *Secret*) for $T \in \{Public, Secret\}$

$$\frac{\begin{array}{c} E \vdash L : T \qquad E \vdash N : Secret \\ E, x_1 : Secret, x_2 : Any, x_3 : Public, x_4 : Any \vdash P : Ok \end{array}}{E \vdash case\ L\ of\ \{x_1, x_2, x_3, x_4\}_N\ in\ P : Ok}$$

There are two rules for output and two rules for input. The rule (Level Output *Public*) says that terms of level *Public* may be sent on a channel of level *Public*. The rule (Level Output *Secret*) says that terms of all levels may be sent on a channel of level *Secret*, provided this is done according to the format described in section 2.4—that is, in a triple with a first component of level *Secret*, a second one of level *Any*, and a third one of level *Public*. The two rules for input, (Level Input *Public*) and (Level Input *Secret*), match these rules for output. In (Level Input *Public*) all inputs are assumed to be of level *Public*, while in (Level Input *Secret*) the levels of the inputs are deduced from their position, as allowed by the format of messages on channels of level *Secret*. As explained in section 2.3, if M is a term of level *Any* and it is not known whether it is of level *Public* or *Secret*, then M cannot be used as a channel.

The rules for nil, for parallel composition, for replication, and for restriction are routine. In the rule (Level Restriction), the name n being bound is associated with an arbitrary term L for which n can be used as a confounder.

The rule (Level Match) enables us to compare any two terms of levels *Public* or *Secret*. Terms of level *Any* are excluded in order to prevent implicit flows, as discussed in section 2.6. It may be a little surprising that terms of level *Secret* are allowed in this rule, because this may seem to permit an implicit flow. However, no implicit flow is possible if the terms of level *Secret* are generated uniformly in all executions of the process being considered, independently of the values of sensitive parameters. Thus, comparisons of terms of level *Secret* do not present an obstacle to our results.

The rule (Level Pair Splitting) enables us to try to break a term of level *Public* or *Secret* into two components, each assumed to be of the same level as the original term. The case where the original term is known only to be of level *Any* is disallowed; if it were allowed, this rule would permit leaking whether the term is in fact a pair.

Similarly, the rule (Level Integer Case) enables us to examine whether a term is 0 or a successor term, and to branch on the result. In the successor case, the variable x represents the predecessor of the term being examined, which is assumed to be of the same level as the term. As in (Level Pair Splitting), the term should not be of level *Any*, but it may be of level *Secret*. If names were numbers, then repeated applications of the rule (Level Integer Case) would enable us to publish a secret name in unary. Formally, this leak cannot happen because names are not numbers, as discussed above. The practical meaning of this small formal miracle is debatable. It may suggest that a model more concrete than the spi calculus would be worth investigating (cf. [LMMS98]).

Finally, there are two rules for decryption, analogous to the rules for input. The rule (Level Decryption *Public*) handles the case where the decryption key is of level *Public* while the rule (Level Decryption *Secret*) handles the case where the decryption key is of level *Secret*. The rule (Level Decryption *Secret*) gives the level *Any* to the confounder in the message being decrypted, for lack of more accurate static information but with no significant, practical loss. There is no rule for decryption with a key of level *Any*.

5 What Typing Guarantees

The goal of this section is to prove that if a process typechecks then it does not leak the values of parameters of level *Any*. As mentioned in the introduction, we use testing equivalence for formalizing the notion of leaking. More precisely, our main theorem says that if only variables of level *Any* and only names of level *Public* are in the domain of the environment E, if σ and σ' are two substitutions of values for the variables in E, and if P typechecks (that is, $E \vdash P : Ok$ can be proved), then $P\sigma$ and $P\sigma'$ are testing equivalent. This conclusion means that an observer cannot distinguish $P\sigma$ and $P\sigma'$, so it cannot detect the difference in the values for the variables.

In order to prove our main theorem, we develop a number of propositions and lemmas that analyze the typing system and characterize the possible behaviors of processes that typecheck.

5.1 Typing for Concretions and Abstractions

The first step in our proofs is to extend the typing rules to concretions and abstractions:

(Level Concretion *Public*)

$$\frac{\begin{array}{c} E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l \vdash M_1 : \mathit{Public} \\ \vdots \\ E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l \vdash M_k : \mathit{Public} \\ E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l \vdash P : \mathit{Ok} \end{array}}{E \vdash (\nu m_1, \ldots, m_l)\langle M_1, \ldots, M_k\rangle P : \mathit{OkC}\,\mathit{Public}}$$

(Level Concretion *Secret*)

$$\frac{\begin{array}{c} E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l \vdash M_1 : \mathit{Secret} \\ E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l \vdash M_2 : \mathit{Any} \\ E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l \vdash M_3 : \mathit{Public} \\ E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l \vdash P : \mathit{Ok} \end{array}}{E \vdash (\nu m_1, \ldots, m_l)\langle M_1, M_2, M_3\rangle P : \mathit{OkC}\,\mathit{Secret}}$$

(Level Abstraction *Public*)

$$\frac{E, x_1 : \mathit{Public}, \ldots, x_k : \mathit{Public} \vdash P : \mathit{Ok}}{E \vdash (x_1, \ldots, x_k)P : \mathit{OkA}\,\mathit{Public}}$$

(Level Abstraction *Secret*)

$$\frac{E, x_1 : \mathit{Secret}, x_2 : \mathit{Any}, x_3 : \mathit{Public} \vdash P : \mathit{Ok}}{E \vdash (x_1, x_2, x_3)P : \mathit{OkA}\,\mathit{Secret}}$$

These rules should be reminiscent of corresponding rules for output and input.

5.2 Auxiliary Propositions

Next, we obtain several auxiliary results. The first of them, Proposition 2, is a formal counterpart of the discussion of section 2.1: this proposition shows that, given a suitable environment, a closed process P that we may construe as an attacker always typechecks. Thus, the typing rules do not narrow the set of attackers against which we defend; we do not assume, arbitrarily, that an attacker adheres to a particular typing discipline.

Proposition 2 *Assume that* $\vdash E$ well-formed*, that* $dom(E)$ *does not contain any variables, and that all the names in* $dom(E)$ *are of level Public.*

- *If* M *is a closed term and* $fn(M) \subseteq dom(E)$*, then* $E \vdash M : Public$*.*
- *If* P *is a closed process and* $fn(P) \subseteq dom(E)$*, then* $E \vdash P : Ok$*.*

Proof We prove a more general property, allowing variables to occur in E, M, and P. We consider an environment E such that $\vdash E$ well-formed, where the levels of names and variables are all *Public*. We prove that:

- If M is a term with $fn(M) \cup fv(M) \subseteq dom(E)$, then $E \vdash M : Public$.
- If P is a process with $fn(P) \cup fv(P) \subseteq dom(E)$, then $E \vdash P : Ok$.

The former of these facts is obtained by a direct induction on the structure of M, using (Level Encryption *Public*) for terms of the form $\{M_1, \dots, M_k\}_N$. The latter of these facts is then obtained by a direct induction on the structure of P, using (Level Output *Public*), (Level Input *Public*), and (Level Decryption *Public*). □

Proposition 3 is fairly standard; it says that anything that can be proved in a given environment can also be proved after adding assumptions to that environment.

Proposition 3 *Assume that* $\vdash E, E', E''$ well-formed*.*

- *If* $E, E'' \vdash M : T$ *then* $E, E', E'' \vdash M : T$*.*
- *If* $E, E'' \vdash P : Ok$ *then* $E, E', E'' \vdash P : Ok$*.*

Proof This property is proved by induction on the derivations of $E, E'' \vdash M : T$ and $E, E'' \vdash P : Ok$. □

Proposition 4 enables us to reorder an environment, moving the declaration of a name past the declarations of some variables.

Proposition 4 *Let* E_1 *be* $E, n : T_0 :: L, x_1 : T_1, \dots, x_k : T_k, E'$ *and let* E_2 *be* $E, x_1 : T_1, \dots, x_k : T_k, n : T_0 :: L, E'$*.*

- *If* $\vdash E_1$ well-formed *then* $\vdash E_2$ well-formed*.*
- *If* $E_1 \vdash M : T$ *then* $E_2 \vdash M : T$*.*
- *If* $E_1 \vdash P : Ok$ *then* $E_2 \vdash P : Ok$*.*

Proof The proof is by induction on the derivations of the judgments $\vdash E_1$ well-formed, $E_1 \vdash M : T$, and $E_1 \vdash P : Ok$. $\square$

(The converse of this proposition is false: if L contains free occurrences of any of $x_1, \ldots, x_k$ then we do not have $\vdash E_1$ well-formed, but we may still have $\vdash E_2$ well-formed.)

The next proposition says that the levels *Secret* and *Public* are mutually exclusive.

Proposition 5 *If $E \vdash M : Secret$ then it is not the case that $E \vdash M : Public$.*

Proof We assume that $E \vdash M : Secret$ and $E \vdash M : Public$ both hold, and derive a contradiction, by induction on the size of the two derivations of $E \vdash M : Secret$ and $E \vdash M : Public$. The only interesting case is that where M has the form $\{M_1, \ldots, M_k\}_N$. The term $\{M_1, \ldots, M_k\}_N$ could have levels *Secret* and *Public* at once only if N did as well, and by application of the two rules for encryption. The induction hypothesis yields the expected contradiction. $\square$

The remaining auxiliary results all concern substitutions. In general, a substitution is a partial function with finite domain from the set of variables to the set of terms. We write $dom(\sigma)$ for the domain of the substitution σ.

Proposition 6 is a standard substitution lemma.

Proposition 6 *Assume that $E \vdash N : T$.*

- *If $\vdash E, x : T, E'$ well-formed then $\vdash E, E'[N/x]$ well-formed.*
- *If $E, x : T, E' \vdash M : R$ then $E, E'[N/x] \vdash M[N/x] : R$.*
- *If $E, x : T, E' \vdash P : Ok$ then $E, E'[N/x] \vdash P[N/x] : Ok$.*

Proof The proof is by a joint induction on the derivations of the judgments $\vdash E, x : T, E'$ well-formed, $E, x : T, E' \vdash M : R$, and $E, x : T, E' \vdash P : Ok$. In the case of the rule (Level Encryption *Secret*), it is important to note that if the confounder n appears in E then x cannot occur in the term being formed. $\square$

Proposition 7 says that substitutions for variables of level *Any* preserve the forms of terms of other levels.

Proposition 7 *Given an environment E, suppose that only variables of level Any in E are in $dom(\sigma)$, and that either $E \vdash L : Public$ or $E \vdash L : Secret$.*

- *If $L\sigma$ is a variable then L is the same variable.*
- *If $L\sigma$ is a name then L is the same name.*
- *If $L\sigma$ is (M, N) then L is of the form (M', N').*
- *If $L\sigma$ is 0 then L is 0.*
- *If $L\sigma$ is $suc(M)$ then L is of the form $suc(M')$.*
- *If $L\sigma$ is $\{M_1, \ldots, M_k\}_N$ then L is of the form $\{M'_1, \ldots, M'_k\}_{N'}$.*

Proof This follows from the fact that L cannot be a variable in $dom(\sigma)$, since this domain consists of variables of level *Any*. □

Proposition 8 says that substitutions for variables of level *Any* act injectively on terms of other levels.

Proposition 8 *Given an environment E, suppose that only variables of level Any in E are in $dom(\sigma)$. Suppose further that $E \vdash M : T$ and $E \vdash N : R$, where $T, R \in \{Public, Secret\}$. If $M\sigma = N\sigma$ then $M = N$.*

Proof The proof is by induction on the derivation of $E \vdash M : T$. There is one case for each of the rules for typechecking terms; the most interesting one is that for (Level Encryption *Secret*).

- The rule (Level Subsumption) can be applied only trivially as the last rule of the derivation since $T \in \{Public, Secret\}$. That is, (Level Subsumption) can yield $E \vdash M : T$ only from $E \vdash M : T$, so this case requires only a trivial invocation of the induction hypothesis.
- If the last rule of the derivation of $E \vdash M : T$ is (Level Variable), then M is a variable, but not one in $dom(\sigma)$ since $dom(\sigma)$ consists of variables of level *Any*, so $M\sigma = M$. Therefore, $M\sigma = N\sigma$ implies that $M = N$ by Proposition 7.
- If the last rule of the derivation of $E \vdash M : T$ is (Level Name) or (Level Zero), then M is a name or 0, so $M\sigma = M$. Therefore, $M\sigma = N\sigma$ implies that $M = N$ by Proposition 7.

- The cases of (Level Successor) and (Level Pair) are by easy applications of Proposition 7 and the induction hypothesis.

- The two remaining cases are for M of the form $\{M_1, \ldots, M_k\}_L$. We have $E \vdash L : \mathit{Public}$ or $E \vdash L : \mathit{Secret}$, depending on whether the derivation of $E \vdash M : T$ finishes with an application of (Level Encryption *Public*) or an application of (Level Encryption *Secret*). In both cases, Proposition 7 implies that N has the form $\{N_1, \ldots, N_k\}_{L'}$, with $L\sigma = L'\sigma$ and either $E \vdash L' : \mathit{Public}$ or $E \vdash L' : \mathit{Secret}$ depending on whether the derivation of $E \vdash N : R$ finishes with an application of (Level Encryption *Public*) or an application of (Level Encryption *Secret*) (possibly followed by trivial applications of (Level Subsumption)). By induction hypothesis, we obtain $L = L'$. By Proposition 5, the derivations of $E \vdash M : T$ and $E \vdash N : R$ both finish with applications of the same rule.

  - If this rule is (Level Encryption *Public*), then we have $E \vdash M_1 : T$, $\ldots$, $E \vdash M_k : T$, $E \vdash N_1 : R$, $\ldots$, $E \vdash N_k : R$ as hypotheses to the applications of the rule. Since $M\sigma = N\sigma$, we have $M_1\sigma = N_1\sigma$, $\ldots$, $M_k\sigma = N_k\sigma$. By induction hypothesis, we obtain $M_1 = N_1$, $\ldots$, $M_k = N_k$, and therefore $M = N$.
  - If this rule is (Level Encryption *Secret*), then $k = 4$, and M_4 is a name m with $m : T' :: M$ in E for some level T', and N_4 is a name n with $n : T'' :: N$ in E for some level T''. Since $M\sigma = N\sigma$, we have $m = n$. Since a name may be declared in an environment at most once, we conclude that $M = N$.

    Note that this last argument does not rely on the induction hypothesis, and it could not: the subterms M_2 and N_2 are of level *Any*, so the induction hypothesis does not apply to them. The reasoning about confounders is necessary.

$\square$

5.3 Lemmas on Commitment and Simulation

The main lemma of this section relates the typing system with the commitment relation. We write $E \vdash \sigma$ when $\sigma(x)$ is a closed term such that $fn(\sigma(x)) \subseteq dom(E)$ for every $x \in dom(E)$.

Lemma 9 *Assume that:*

(1) $E \vdash P : \mathit{Ok}$,

(2) $E \vdash \sigma$,

(3) *all variables in* $dom(E)$ *are of level* Any.

Then:

(1) *If* $P\sigma > Q'$ *then there is a process* Q *such that*

- $Q' = Q\sigma$,
- $E \vdash Q : Ok$,
- $P\sigma' > Q\sigma'$ *whenever* $E \vdash \sigma'$.

(2) *If* $P\sigma \xrightarrow{\tau} Q'$ *then there is a process* Q *such that*

- $Q' = Q\sigma$,
- $E \vdash Q : Ok$,
- $P\sigma' \xrightarrow{\tau} Q\sigma'$ *whenever* $E \vdash \sigma'$.

(3) *If* $P\sigma \xrightarrow{\overline{m}} A'$ *then either* $E \vdash m : Public$ *or* $E \vdash m : Secret$, *and there is a concretion* A *such that*

- $A' = A\sigma$,
- *either* $E \vdash A : OkCPublic$ *or* $E \vdash A : OkCSecret$ *(depending on whether* $E \vdash m : Public$ *or* $E \vdash m : Secret$*),*
- $P\sigma' \xrightarrow{\overline{m}} A\sigma'$ *whenever* $E \vdash \sigma'$.

(4) *If* $P\sigma \xrightarrow{m} A'$ *then either* $E \vdash m : Public$ *or* $E \vdash m : Secret$, *and there is an abstraction* A *such that*

- $A' = A\sigma$,
- *either* $E \vdash A : OkAPublic$ *or* $E \vdash A : OkASecret$ *(depending on whether* $E \vdash m : Public$ *or* $E \vdash m : Secret$*),*
- $P\sigma' \xrightarrow{m} A\sigma'$ *whenever* $E \vdash \sigma'$.

Proof Throughout, we assume that, when the variables x and y are bound anywhere, they do not appear in the domain or range of the substitutions σ and σ'. Similarly, when they are bound, we assume that the names m, $m_1, \ldots, m_l$, and n do not appear in the range of the substitutions σ and σ'. Both of these conditions can be achieved by renaming, if necessary.

For the first part, we examine the axioms for $>$ one by one. In each case we assume that a reduction yields a process Q' by the given axiom, and construct a process Q with the required properties. In particular, the equality $Q' = Q\sigma$ holds easily in all cases.

- (Red Repl) In this case, $(!P)\sigma > P\sigma \mid (!P)\sigma$.

  We let Q be $P \mid !P$. The judgment $E \vdash !P : Ok$ must be established via the rule (Level Repl) from $E \vdash P : Ok$; therefore, $E \vdash P \mid !P : Ok$, that is, $E \vdash Q : Ok$.

  In addition, $(!P)\sigma' > Q\sigma'$ for all σ' such that $P\sigma'$ is closed, and a fortiori whenever $E \vdash \sigma'$.

- (Red Match) In this case, $([M_1 \textit{ is } M_2]\ P)\sigma > P\sigma$, where $M_1\sigma = M_2\sigma$.

  We let Q be P. The judgment $E \vdash [M_1 \textit{ is } M_2]\ P : Ok$ must be established via the rule (Level Match) from $E \vdash P : Ok$, $E \vdash M_1 : T_1$, and $E \vdash M_2 : T_2$, for $T_1, T_2 \in \{\textit{Public}, \textit{Secret}\}$. Since Q is P, we have $E \vdash Q : Ok$.

  In order to obtain that $([M_1 \textit{ is } M_2]\ P)\sigma' > P\sigma'$, it suffices that the process $([M_1 \textit{ is } M_2]\ P)\sigma'$ be closed and that $M_1\sigma' = M_2\sigma'$. The former condition follows from $E \vdash \sigma'$. The latter condition follows from $M_1\sigma = M_2\sigma$ by Proposition 8 (via $M_1 = M_2$).

- (Red Let) In this case, $(\textit{let } (x, y) = L \textit{ in } P)\sigma > P\sigma[M'/x, N'/y]$, where $L\sigma$ is (M', N').

  The judgment $E \vdash \textit{let } (x, y) = L \textit{ in } P : Ok$ must be established via the rule (Level Pair Splitting) from $E \vdash L : T$ and $E, x : T, y : T \vdash P : Ok$ for $T \in \{\textit{Public}, \textit{Secret}\}$. By Proposition 7, L must be a pair (M, N). In addition, $E \vdash L : T$ must be established via the rule (Level Pair) from $E \vdash M : T$ and $E \vdash N : T$.

  We let Q be $P[M/x, N/y]$. We obtain $E \vdash Q : Ok$ from $E, x : T, y : T \vdash P : Ok$, $E \vdash M : T$, and $E \vdash N : T$, by Proposition 6.

  Whenever $E \vdash \sigma'$, we have $(\textit{let } (x, y) = L \textit{ in } P)\sigma' = (\textit{let } (x, y) = L\sigma' \textit{ in } P\sigma') = (\textit{let } (x, y) = (M, N)\sigma' \textit{ in } P\sigma') > P\sigma'[M\sigma'/x, N\sigma'/y] = Q\sigma'$.

- (Red Zero) In this case, $(\textit{case } M \textit{ of } 0 : P_1\ \textit{suc}(x) : P_2)\sigma > P_1\sigma$, where $M\sigma$ is 0.

  We let Q be P_1. The judgment $E \vdash \textit{case } M \textit{ of } 0 : P_1\ \textit{suc}(x) : P_2 : Ok$ must be established via the rule (Level Integer Case) from, among other judgments, $E \vdash M : T$ for $T \in \{\textit{Public}, \textit{Secret}\}$ and $E \vdash P_1 : Ok$, that is, $E \vdash Q : Ok$.

  By Proposition 7, M is 0. Therefore, $(\textit{case } M \textit{ of } 0 : P_1\ \textit{suc}(x) : P_2)\sigma' > P_1\sigma'$ for all σ' such that $(\textit{case } M \textit{ of } 0 : P_1\ \textit{suc}(x) : P_2)\sigma'$ is closed, and a fortiori whenever $E \vdash \sigma'$.

- (Red Suc) In this case, $(\mathit{case}\ M\ \mathit{of}\ 0 : P_1\ \mathit{suc}(x) : P_2)\sigma > P_2\sigma[N'/x]$, where $M\sigma$ is $\mathit{suc}(N')$.

  Again, the judgment $E \vdash \mathit{case}\ M\ \mathit{of}\ 0 : P_1\ \mathit{suc}(x) : P_2 : \mathit{Ok}$ must be established via the rule (Level Integer Case) from, among other judgments, $E \vdash M : T$ and $E, x : T \vdash P_2 : \mathit{Ok}$ for $T \in \{\mathit{Public}, \mathit{Secret}\}$. By Proposition 7, M is $\mathit{suc}(N)$ for some N (so N' is $N\sigma$). In addition, $E \vdash M : T$ must be established via the rule (Level Successor) from $E \vdash N : T$.

  We let Q be $P_2[N/x]$. We obtain $E \vdash Q : \mathit{Ok}$ from $E, x : T \vdash P_2 : \mathit{Ok}$ and $E \vdash N : T$ by Proposition 6.

  Whenever $E \vdash \sigma'$, we have $(\mathit{case}\ M\ \mathit{of}\ 0 : P_1\ \mathit{suc}(x) : P_2)\sigma' = (\mathit{case}\ \mathit{suc}(N\sigma')\ \mathit{of}\ 0 : P_1\sigma'\ \mathit{suc}(x) : P_2\sigma') > P_2\sigma'[N\sigma'/x] = Q\sigma'$.

- (Red Decrypt) In this case

  $$(\mathit{case}\ M\ \mathit{of}\ \{x_1, \ldots, x_k\}_N\ \mathit{in}\ P)\sigma > P\sigma[L_1'/x_1, \ldots, L_k'/x_k]$$

  where $M\sigma$ is $\{L_1', \ldots, L_k'\}_{N\sigma}$.

  The judgment $E \vdash \mathit{case}\ M\ \mathit{of}\ \{x_1, \ldots, x_k\}_N\ \mathit{in}\ P : \mathit{Ok}$ must be established via the rule (Level Decryption *Public*) or (Level Decryption *Secret*), with $E \vdash M : T$ and $E \vdash N : R$ for $T, R \in \{\mathit{Public}, \mathit{Secret}\}$, and either $E, x_1 : T, \ldots, x_k : T \vdash P : \mathit{Ok}$ or $k = 4$ and $E, x_1 : \mathit{Secret}, x_2 : \mathit{Any}, x_3 : \mathit{Public}, x_4 : \mathit{Any} \vdash P : \mathit{Ok}$.

  By Proposition 7, M is $\{L_1, \ldots, L_k\}_L$ for some terms L, L_1, …, L_k (so $L_i\sigma$ equals L_i' for $i \in 1..k$ and $N\sigma$ equals $L\sigma$).

  The judgment $E \vdash M : T$ must be established via the rule (Level Encryption *Public*) or (Level Encryption *Secret*), with $E \vdash L : S$ for $S \in \{\mathit{Public}, \mathit{Secret}\}$, and either $E \vdash L_i : T$ for $i \in 1..k$ or $k = 4$, $E \vdash L_1 : \mathit{Secret}$, $E \vdash L_2 : \mathit{Any}$, $E \vdash L_3 : \mathit{Public}$, and L_4 is a name n with $n : T^* :: M$ in E for some T^*, so $E \vdash L_4 : \mathit{Any}$.

  By Proposition 8, since $L\sigma$ equals $N\sigma$, we obtain that L equals N. It follows that S equals R, by Proposition 5. We proceed by cases on whether S is *Public* or *Secret*.

  - If S is *Public*, we let Q be $P[L_1/x_1, \ldots, L_k/x_k]$. We obtain $E \vdash Q : \mathit{Ok}$ from $E, x_1 : T, \ldots, x_k : T \vdash P : \mathit{Ok}$ and $E \vdash L_1 : T$, …, $E \vdash L_k : T$ by Proposition 6.
  - If S is *Secret*, we let Q be $P[L_1/x_1, L_2/x_2, L_3/x_3, L_4/x_4]$. We obtain $E \vdash Q : \mathit{Ok}$ from $E, x_1 : \mathit{Secret}, x_2 : \mathit{Any}, x_3 : \mathit{Public}, x_4 :$

$Any \vdash P : Ok$ and $E \vdash L_1 : Secret$, $E \vdash L_2 : Any$, $E \vdash L_3 : Public$, and $E \vdash L_4 : Any$ by Proposition 6.

In both cases, whenever $E \vdash \sigma'$, we have:

$$\begin{array}{ll} \multicolumn{2}{l}{(case\ M\ of\ \{x_1, \ldots, x_k\}_N\ in\ P)\sigma'} \\ = & (case\ M\sigma'\ of\ \{x_1, \ldots, x_k\}_{N\sigma'}\ in\ P\sigma') \\ = & (case\ \{L_1\sigma', \ldots, L_k\sigma'\}_{N\sigma'}\ of\ \{x_1, \ldots, x_k\}_{N\sigma'}\ in\ P\sigma') \\ > & P\sigma'[L_1\sigma'/x_1, \ldots, L_k\sigma'/x_k] \\ = & Q\sigma' \end{array}$$

The remaining parts can be proved together by induction over derivations. We consider the rules for commitment one by one.

- (Comm Out) In this case, we have

  $$(\overline{M}\langle M_1, \ldots, M_k\rangle.P)\sigma \xrightarrow{\overline{m}} (\nu)\langle M_1\sigma, \ldots, M_k\sigma\rangle P\sigma$$

  where $M\sigma$ is m.

  We let A equal $(\nu)\langle M_1, \ldots, M_k\rangle P$, so we have $(\nu)\langle M_1\sigma, \ldots, M_k\sigma\rangle P\sigma = A\sigma$. The judgment $E \vdash \overline{M}\langle M_1, \ldots, M_k\rangle.P : Ok$ must be established through one of the rules (Level Output *Public*) or (Level Output *Secret*), with $E \vdash M : R$, $E \vdash M_1 : R_1$, ..., $E \vdash M_k : R_k$, and $E \vdash P : Ok$, for $R \in \{Public, Secret\}$. By Proposition 7, M must be the name m, so we have either $E \vdash m : Public$ or $E \vdash m : Secret$. When R is *Public*, all of R_1, ..., R_k are also *Public*, and we obtain $E \vdash A : OkC\,Public$ by (Level Concretion *Public*). When R is *Secret*, we have $k = 3$ and $E \vdash M_1 : Secret$, $E \vdash M_2 : Any$, and $E \vdash M_3 : Public$ (as hypothesis for the application of (Level Output *Secret*)), so we obtain $E \vdash A : OkC\,Secret$ by (Level Concretion *Secret*). In either case, if $E \vdash \sigma'$, then $(\overline{M}\langle M_1, \ldots, M_k\rangle.P)\sigma' \xrightarrow{\overline{m}} (\nu)\langle M_1\sigma', \ldots, M_k\sigma'\rangle P\sigma' = A\sigma'$, since M is m.

- (Comm In) In this case, we have

  $$(M(x_1, \ldots, x_k).P)\sigma \xrightarrow{m} (x_1, \ldots, x_k)P\sigma$$

  where $M\sigma$ is m.

  We let A equal $(x_1, \ldots, x_k)P$, so we have $(x_1, \ldots, x_k)P\sigma = A\sigma$. The judgment $E \vdash M(x_1, \ldots, x_k).P : Ok$ must be established through one of the rules (Level Input *Public*) or (Level Input *Secret*), with $E \vdash$

$M : R$ and $E, x_1 : T_1, \ldots, x_n : T_n \vdash P : Ok$, for $R \in \{Public, Secret\}$. By Proposition 7, M must be the name m, so we have either $E \vdash m : Public$ or $E \vdash m : Secret$. When R is $Public$, all of $T_1, \ldots, T_k$ are also $Public$, and we obtain $E \vdash A : OkAPublic$ by (Level Abstraction *Public*). When R is $Secret$, we have $k = 3$ and $E, x_1 : Secret, x_2 : Any, x_3 : Public \vdash P : Ok$ (as hypothesis for the application of (Level Input *Secret*)), so we obtain $E \vdash A : OkASecret$ by (Level Abstraction *Secret*). In either case, if $E \vdash \sigma'$, then $(M(x_1, \ldots, x_k).P)\sigma' \xrightarrow{m} (x_1, \ldots, x_k)P\sigma' = A\sigma'$, since M is m.

- (Comm Inter 1) In this case, we obtain $(P_1 \mid P_2)\sigma \xrightarrow{\tau} F@C$ from $P_1\sigma \xrightarrow{m} F$ and $P_2\sigma \xrightarrow{\overline{m}} C$. The judgment $E \vdash P_1 \mid P_2 : Ok$ must be derived from $E \vdash P_1 : Ok$ and $E \vdash P_2 : Ok$. By induction hypothesis, there is an abstraction A with the properties stated in part 4 (corresponding to F), and there is a concretion B with the properties stated in part 3 (corresponding to C). In particular, we have $F = A\sigma$ and $C = B\sigma$.

  We consider two cases, one for $E \vdash m : Public$ and one for $E \vdash m : Secret$.

  - In case $E \vdash m : Public$, we have $E \vdash A : OkAPublic$ and $E \vdash B : OkCPublic$. So A has the form $(x_1, \ldots, x_k)P_1^*$ with $E, x_1 : Public, \ldots, x_k : Public \vdash P_1^* : Ok$, and B has the form $(\nu m_1, \ldots, m_l)\langle M_1, \ldots, M_k\rangle P_2^*$ with $E' \vdash M_1 : Public$, $\ldots$, $E' \vdash M_k : Public$, and $E' \vdash P_2^* : Ok$ for some environment E' of the form $E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l$. (The index k is the same in A and B because $F@C$ is defined.)

    We let Q be $(\nu m_1) \ldots (\nu m_l)(P_1^*[M_1/x_1, \ldots, M_k/x_k] \mid P_2^*)$. We obtain $E \vdash Q : Ok$ by Proposition 3 and Proposition 6, using the rules (Level Parallel) and (Level Restriction).

  - In case $E \vdash m : Secret$, we have $E \vdash A : OkASecret$ and $E \vdash B : OkCSecret$. So A has the form $(x_1, x_2, x_3)P_1^*$ with $E, x_1 : Secret, x_2 : Any, x_3 : Public \vdash P_1^* : Ok$, and B has the form $(\nu m_1, \ldots, m_l)\langle M_1, M_2, M_3\rangle P_2^*$ with $E' \vdash M_1 : Secret$, $E' \vdash M_2 : Any$, $E' \vdash M_3 : Public$, and $E' \vdash P_2^* : Ok$, for some environment E' of the form $E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l$.

    We let Q be $(\nu m_1) \ldots (\nu m_l)(P_1^*[M_1/x_1, M_2/x_2, M_3/x_3] \mid P_2^*)$. We obtain $E \vdash Q : Ok$ by Proposition 3 and Proposition 6, using the rules (Level Parallel) and (Level Restriction).

In both cases, we have $F@C = Q\sigma$. Moreover, suppose that $E \vdash \sigma'$. We have $P_1\sigma' \xrightarrow{m} A\sigma'$ and $P_2\sigma' \xrightarrow{\overline{m}} B\sigma'$, so

$$\begin{array}{ll} (P_1 \mid P_2)\sigma' & \\ \xrightarrow{\tau} & (\nu m_1)\ldots(\nu m_l)(P_1^*\sigma'[M_1\sigma'/x_1,\ldots,M_k\sigma'/x_k] \mid P_2^*\sigma') \\ = & Q\sigma' \end{array}$$

by (Comm Inter 1).

- (Comm Inter 2) is analogous to (Comm Inter 1).
- (Comm Par 1) In this case, we obtain $(P_1 \mid P_2)\sigma \xrightarrow{\alpha} A_1' \mid P_2\sigma$ from $P_1\sigma \xrightarrow{\alpha} A_1'$. Here α is τ, a name m, or a co-name $\overline{m}$, and A_1' is correspondingly a process, an abstraction, or a concretion. The judgment $E \vdash P_1 \mid P_2 : Ok$ must be derived from $E \vdash P_1 : Ok$ and $E \vdash P_2 : Ok$. By induction hypothesis, there exists A_1 such that $A_1' = A_1\sigma$ and $E \vdash A_1 : someOk$ and $P_1\sigma' \xrightarrow{\alpha} A_1\sigma'$ whenever $E \vdash \sigma'$, where $someOk$ is one of Ok, $OkAPublic$, $OkASecret$, $OkCPublic$, and $OkCSecret$, depending on whether α is τ, m, or $\overline{m}$, and on whether m is of level $Public$ or $Secret$.

  We let A be $A_1 \mid P_2$. We obtain $E \vdash A : someOk$ from $E \vdash A_1 : someOk$ and $E \vdash P_2 : Ok$, as follows:

  - Suppose that α is τ, and A_1 is a process. Then $E \vdash A : Ok$ can be derived directly by (Level Parallel).
  - Suppose that α is m, that $E \vdash m : Public$, and that A_1 is an abstraction $(x_1,\ldots,x_k)P_1^*$ such that $E \vdash A_1 : OkAPublic$. In this case, $A_1 \mid P_2$ is an abbreviation for $(x_1,\ldots,x_k)(P_1^* \mid P_2)$. The judgment $E \vdash A_1 : OkAPublic$ must be established from $E, x_1 : Public, \ldots, x_k : Public \vdash P_1^* : Ok$. By Proposition 3, we have also $E, x_1 : Public, \ldots, x_k : Public \vdash P_2 : Ok$. By (Level Parallel) and (Level Abstraction $Public$), we conclude $E \vdash A : OkAPublic$.
  - Suppose that α is m, that $E \vdash m : Secret$, and that A_1 is an abstraction such that $E \vdash A_1 : OkASecret$. By reasoning analogous to that of the previous case, we obtain $E \vdash A : OkASecret$.
  - Suppose that α is $\overline{m}$, that $E \vdash m : Public$, and that A_1 is a concretion $(\nu m_1,\ldots,m_l)\langle M_1,\ldots,M_k\rangle P_1^*$ such that $E \vdash A_1 : OkCPublic$. In this case, $A_1 \mid P_2$ is an abbreviation for $(\nu m_1,\ldots, m_l)\langle M_1,\ldots,M_k\rangle(P_1^* \mid P_2)$. The judgment $E \vdash A_1 : OkCPublic$

must be established from $E' \vdash M_1 : \mathit{Public}, \ldots, E' \vdash M_k : \mathit{Public}$, and $E' \vdash P_1^* : \mathit{Ok}$ for some environment E' of the form $E, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l$. By Proposition 3, we have also $E' \vdash P_2 : \mathit{Ok}$. By (Level Parallel) and (Level Concretion *Public*), we conclude $E \vdash A : \mathit{OkCPublic}$.

  - Suppose that α is $\overline{m}$, that $E \vdash m : \mathit{Secret}$, and that A_1 is an abstraction such that $E \vdash A_1 : \mathit{OkCSecret}$. By reasoning analogous to that of the previous case, we obtain $E \vdash A : \mathit{OkCSecret}$.

For all cases, we obtain $(A_1' \mid P_2\sigma) = A\sigma$. Moreover, if $E \vdash \sigma'$ then $(P_1 \mid P_2)\sigma' = (P_1\sigma' \mid P_2\sigma') \xrightarrow{\alpha} (A_1\sigma' \mid P_2\sigma') = A\sigma'$ by (Comm Par 1).

- (Comm Par 2) is analogous to (Comm Par 1).

- (Comm Res) In this case, we obtain $((\nu n)P)\sigma \xrightarrow{\alpha} (\nu n)B'$ from $P\sigma \xrightarrow{\alpha} B'$. Here α is τ, a name m, or a co-name $\overline{m}$, with $m \neq n$, and $(\nu n)B'$ is correspondingly a process, an abstraction, or a concretion. The judgment $E \vdash (\nu n)P : \mathit{Ok}$ must be derived from $E, n : T :: L \vdash P : \mathit{Ok}$, for some T and L. By induction hypothesis, there exists B such that $(\nu n)B' = B\sigma$ and $E, n : T :: L \vdash B : \mathit{someOk}$ and $P\sigma' \xrightarrow{\alpha} B\sigma'$ whenever $E, n : T :: L \vdash \sigma'$. As in the case of (Comm Par 1), *someOk* is one of *Ok*, *OkAPublic*, *OkASecret*, *OkCPublic*, and *OkCSecret*, depending on whether α is τ, m, or $\overline{m}$, and on whether m is of level *Public* or *Secret*.

  We let A be $(\nu n)B$. We obtain $E \vdash A : \mathit{someOk}$ from $E, n : T :: L \vdash B : \mathit{someOk}$, as follows:

  - Suppose that α is τ, and B is a process. Then $E \vdash A : \mathit{Ok}$ can be derived directly by (Level Restriction).
  - Suppose that α is m, that $E \vdash m : \mathit{Public}$, and that B is an abstraction $(x_1, \ldots, x_k)P^*$ such that $E, n : T :: L \vdash B : \mathit{OkAPublic}$. In this case, $(\nu n)B$ is an abbreviation for $(x_1, \ldots, x_k)(\nu n)P^*$. The judgment $E, n : T :: L \vdash B : \mathit{OkAPublic}$ must be established from $E, n : T :: L, x_1 : \mathit{Public}, \ldots, x_k : \mathit{Public} \vdash P^* : \mathit{Ok}$. By Proposition 4, we have also $E, x_1 : \mathit{Public}, \ldots, x_k : \mathit{Public}, n : T :: L \vdash P^* : \mathit{Ok}$. By (Level Restriction) and (Level Abstraction *Public*), we conclude $E \vdash A : \mathit{OkAPublic}$.
  - Suppose that α is m, that $E \vdash m : \mathit{Secret}$, and that B is an abstraction such that $E, n : T :: L \vdash B : \mathit{OkASecret}$. By reasoning analogous to that of the previous case, we obtain $E \vdash A : \mathit{OkASecret}$.

– Suppose that α is $\overline{m}$, that $E \vdash m : \mathit{Public}$, and that B is a concretion $(\nu m_1, \ldots, m_l)\langle M_1, \ldots, M_k\rangle P^*$ such that $E, n : T :: L \vdash B : \mathit{OkCPublic}$. In this case, $(\nu n)B$ is an abbreviation for $(\nu n, m_1, \ldots, m_l)\langle M_1, \ldots, M_k\rangle P^*$. The judgment $E, n : T :: L \vdash B : \mathit{OkCPublic}$ must be established from $E' \vdash M_1 : \mathit{Public}$, ..., $E' \vdash M_k : \mathit{Public}$, and $E' \vdash P^* : \mathit{Ok}$ for some environment E' of the form $E, n : T :: L, m_1 : T_1 :: L_1, \ldots, m_l : T_l :: L_l$. By (Level Concretion *Public*), we conclude $E \vdash A : \mathit{OkCPublic}$.

– Suppose that α is $\overline{m}$, that $E \vdash m : \mathit{Secret}$, and that B is an abstraction such that $E \vdash B : \mathit{OkCSecret}$. By reasoning analogous to that of the previous case, we obtain $E \vdash A : \mathit{OkCSecret}$.

For all cases, we obtain $(\nu n)B' = A\sigma$. Moreover, since n does not appear in the range of σ' and $\alpha \notin \{n, \overline{n}\}$, if $E \vdash \sigma'$, then $((\nu n)P)\sigma' \xrightarrow{\alpha} ((\nu n)B)\sigma' = A\sigma'$, by (Comm Res).

- (Comm Red) In this case, we obtain $P\sigma \xrightarrow{\alpha} A'$ from $P\sigma > Q_0'$ and $Q_0' \xrightarrow{\alpha} A'$. Since $P\sigma > Q_0'$, there exists Q_0 such that $Q_0' = Q_0\sigma$ and $E \vdash Q_0 : \mathit{Ok}$ and $P\sigma' > Q_0\sigma'$ whenever $E \vdash \sigma'$.

  By induction hypothesis, $E \vdash Q_0 : \mathit{Ok}$ and $Q_0\sigma \xrightarrow{\alpha} A'$ yield that there exists A such that $A' = A\sigma$ and $E \vdash A : \mathit{someOk}$ and $Q_0\sigma' > A\sigma'$ whenever $E \vdash \sigma'$ (and with *someOk* defined as in the case for (Comm Par 1)). Therefore, whenever $E \vdash \sigma'$, we have $P\sigma' > Q_0\sigma' \xrightarrow{\alpha} A\sigma'$, so $P\sigma' \xrightarrow{\alpha} A\sigma'$ by (Comm Red).

□

Lemma 10 *Given an environment E, suppose that all the variables in $dom(E)$ are of level Any. Suppose further that $E \vdash \sigma$ and $E \vdash \sigma'$. Then the relation*

$$\{(P\sigma, P\sigma') \mid E \vdash P : \mathit{Ok}\}$$

is a strict barbed bisimulation.

Proof First we consider any commitment $P\sigma \xrightarrow{\alpha} A'$, where α is a barb. By Lemma 9, there is an agent A such that $P\sigma' \xrightarrow{\alpha} A\sigma'$.

Next, we consider any commitment $P\sigma \xrightarrow{\tau} Q'$. By Lemma 9, there is a process Q such that $E \vdash Q : \mathit{Ok}$, $Q' = Q\sigma$, and $P\sigma' \xrightarrow{\tau} Q\sigma'$. Thus, any τ step of $P\sigma$ may be matched by $P\sigma'$.

Therefore, the relation $\{(P\sigma, P\sigma') \mid E \vdash P : \mathit{Ok}\}$ is a strict barbed simulation. By symmetry, it is a strict barbed bisimulation. □

5.4 Main Theorem

Finally, we obtain the theorem described at the start of section 5:

Theorem 11 *Given an environment E, suppose that only variables of level Any and only names of level Public are in $dom(E)$. Suppose further that $E \vdash \sigma$ and $E \vdash \sigma'$. If $E \vdash P : Ok$ then $P\sigma \simeq P\sigma'$.*

Proof According to Lemma 1, it suffices to show that for every closed process Q there exists a strict barbed bisimulation that relates $P\sigma \mid Q$ and $P\sigma' \mid Q$. Since Q is closed, $P\sigma \mid Q$ equals $(P \mid Q)\sigma$, and $P\sigma' \mid Q$ equals $(P \mid Q)\sigma'$.

We construct an extension of E with the names that appear free in Q but are not in $dom(E)$. For each such name n, we add $n : Public$ to E. Let us call E^* the resulting environment. By Propositions 2 and 3, we obtain $E^* \vdash Q : Ok$. Also by Proposition 3, we obtain $E^* \vdash P : Ok$. Combining these two results, rule (Level Parallel) yields $E^* \vdash (P \mid Q) : Ok$.

Finally, Lemma 10 yields the desired result. □

Note that this theorem would not hold if P could have free occurrences of names of level *Secret*. Such occurrences are ruled out by the hypotheses that only names of level *Public* are in E and that $E \vdash P : Ok$.

6 Examples

In order to illustrate the use of our typing rules, we consider as examples two protocols for key exchange and secure communication.

In both cases, we can typecheck the protocols. (We do the typechecking manually, but Simon Gay has reproduced it in his implementation of our typing system [Gay97].) As corollaries, we obtain that the secrecy of certain messages is protected. The corollaries imply that the protocols do not publish those message directly or leak them through implicit flows. These corollaries should not be surprising. However, they would be much harder to prove from first principles, without the rules developed in this paper.

Analogues of our corollaries might be provable in other formal systems. Surprisingly, there do not seem to be any formal proofs of this sort in the literature on protocols. In some methods, such as Paulson's effective inductive method [Pau98], one may be able to show that the messages in question are not among the terms that the attacker obtains when the protocol runs. However, this result is only an approximation to the corollaries, as it does not rule out that the attacker could at least deduce whether the messages are even numbers or odd numbers, for example. The corollaries exclude this possibility.

Analogues of our corollaries can perhaps be established in informal but rigorous models (see for example [BR95]). These models are rather accurate, as in particular they can take into account issues of probability and complexity. Unfortunately, proofs in these models remain much more difficult than typechecking.

6.1 A First Example

The first protocol is similar in structure to the Wide Mouthed Frog protocol [BAN89]. It enables a principal A to transmit some sensitive data M to a principal B with the help of a server S. First, A generates a key K_{AB}, sends it to S encrypted under a pre-existent key, then S forwards K_{AB} to B under another pre-existent key, and finally A sends M to B under K_{AB}. In addition to the keys and to the payload M, the protocol messages include the names of the principals, nonces, and confounders.

Informally, the protocol is:

Message 1	$A \rightarrow S:$	A	on c_S
Message 2	$S \rightarrow A:$	N_S	on c_A
Message 3	$A \rightarrow S:$	$\{K_{AB}, *, (A, A, B, N_S), C_A\}_{K_{AS}}$	on c_S
Message 4	$S \rightarrow B:$	$*$	on c_B
Message 5	$B \rightarrow S:$	N_B	on c_S
Message 6	$S \rightarrow B:$	$\{K_{AB}, *, (S, A, B, N_B), C_S\}_{K_{SB}}$	on c_B
Message 7	$A \rightarrow B:$	$\{*, M, *, C'_A\}_{K_{AB}}$	on c_B
Message 8	$B \rightarrow ?:$	A, B	on d_B

The channels c_S, c_A, c_B, and d_B are public. The keys K_{AS} and K_{SB} are secret keys for communication with the server, while K_{AB} is the new secret key for communication from A to B. Both N_S and N_B are nonces (used to prove timeliness); $*$ is an arbitrary message of appropriate level (not necessarily the same for all occurrences of $*$); and C_A, C'_A, and C_S are confounders. In Messages 1 and 2, A requests and receives a nonce challenge from S; the request is simply A's name. In Messages 4 and 5, S requests and receives a nonce challenge from B; here an arbitrary message suffices as request since there is only one server. In Message 3, A provides the key K_{AB} to S, which passes it on to B in Message 6. In Message 3, the tuple (A, A, B, N_S) conveys the name of the sender, the names of the users of the key, and a nonce. Similarly, in Message 6, the tuple (S, A, B, N_B) conveys the name of the sender, the names of the users of the key, and a nonce. In Message 7, A uses K_{AB} for sending M. On receipt of this message from A, the recipient B outputs the names of A and B on a public channel d_B, in Message 8. It is not important to specify who receives this last message, which we include only in order to illustrate that B is allowed to react.

We can express this protocol in the spi calculus, much as in the earlier work on the spi calculus [AG97b] but with attention to the requirements of typing. The spi-calculus definition of the protocol is basically code that produces the message sequence shown above. (It does not always produce exactly that message sequence, as it allows more interleavings and may sometimes get stuck, but doing better is a simple matter of programming.) The code is long but not particularly deep or intricate—a careful reading should reveal its step-by-step behavior if not its invariants. Some familiarity with earlier work on the spi calculus may help understand its style. In any case, fortunately, the application of our rules and theorems does not require a detailed comprehension of the code.

The spi-calculus definition is for a given set of messages $M_1, \ldots, M_m$ with source addresses $i_1, \ldots, i_m$ and destination addresses $j_1, \ldots, j_m$, respectively. These addresses are natural numbers in the range $1..n$; they indicate who plays the role of A and who plays the role of B in each run of the protocol. In addition, we use S as an address. For each address i, there are channels c_i and d_i. We write $\underline{i}$ for the term representing i (so for example $\underline{2}$ is $suc(suc(0)))$, and simply write S for the term representing S. We construct a process Sys with code for the complete protocol by combining three processes, $Send_{i,j}$, Srv, and $Recv_j$. These three processes give the code for sending from address i to address j, for the server, and for receiving at address j, respectively. In the definition of $Send_{i,j}$, the variable z corresponds to the message M; we write $Send_{i,j}(M)$ for $Send_{i,j}[M/z]$.

$$
\begin{array}{rcl}
Send_{i,j} & \triangleq & \overline{c_S}\langle \underline{i} \rangle \mid \\
& & c_i(x_{nonce}). \\
& & (\nu K)((\nu C_A)\overline{c_S}\langle \{K, *, (\underline{i}, \underline{i}, \underline{j}, x_{nonce}), C_A\}_{K_{iS}} \rangle \mid \\
& & \qquad (\nu C'_A)\overline{c_j}\langle \{*, z, *, C'_A\}_K \rangle)
\end{array}
$$

$$
\begin{array}{rcl}
\mathit{Srv} & \triangleq & c_S(x_A).\prod_{i\in 1..n}[x_A\ \mathit{is}\ \underline{i}]\ (\nu N_S)(\overline{c_i}\langle N_S\rangle \mid \\
& & c_S(x_{cipher}). \\
& & \mathit{case}\ x_{cipher}\ \mathit{of}\ \{x_{key}, x_a, x_p, x_{cnf}\}_{K_{iS}}\ \mathit{in} \\
& & \mathit{let}\ (y_A, z_A, x_B, x_{nonce}) = x_p\ \mathit{in} \\
& & \prod_{j\in 1..n}[y_A\ \mathit{is}\ \underline{i}]\ [z_A\ \mathit{is}\ \underline{i}]\ [x_B\ \mathit{is}\ \underline{j}]\ [x_{nonce}\ \mathit{is}\ N_S] \\
& & (\overline{c_j}\langle *\rangle \mid \\
& & \ c_S(y_{nonce}). \\
& & \ (\nu C_S)\overline{c_j}\langle\{x_{key}, *, (S, \underline{i}, \underline{j}, y_{nonce}), C_S\}_{K_{Sj}}\rangle)) \\
\mathit{Recv}_j & \triangleq & c_j(w).(\nu N_B)(\overline{c_S}\langle N_B\rangle \mid \\
& & c_j(y_{cipher}). \\
& & \mathit{case}\ y_{cipher}\ \mathit{of}\ \{x_{key}, y_a, y_p, y_{cnf}\}_{K_{Sj}}\ \mathit{in} \\
& & \mathit{let}\ (x_S, x_A, x_B, y_{nonce}) = y_p\ \mathit{in} \\
& & \prod_{i\in 1..n}[x_S\ \mathit{is}\ S]\ [x_A\ \mathit{is}\ \underline{i}]\ [x_B\ \mathit{is}\ \underline{j}]\ [y_{nonce}\ \mathit{is}\ N_B] \\
& & c_j(z_{cipher}). \\
& & \mathit{case}\ z_{cipher}\ \mathit{of}\ \{z_s, z_a, z_p, z_{cnf}\}_{x_{key}}\ \mathit{in} \\
& & \overline{d_j}\langle\underline{i}, \underline{j}\rangle) \\
\mathit{Sys} & \triangleq & (\nu K_{1S})\ldots(\nu K_{nS})(\nu K_{S1})\ldots(\nu K_{Sn}) \\
& & (\mathit{Send}_{i_1,j_1}(M_1) \mid \ldots \mid \mathit{Send}_{i_m,j_m}(M_m) \mid \\
& & \ !\mathit{Srv} \mid \\
& & \ !\mathit{Recv}_1 \mid \ldots \mid !\mathit{Recv}_n)
\end{array}
$$

To be even more precise, we should replace each occurrence of $*$ with an appropriate term. For example, in the expression $\overline{c_j}\langle\{*, z, *, C'_A\}_K\rangle$, we may replace the first occurrence with K and the second with 0; alternatively, we may rewrite $\overline{c_j}\langle\{*, z, *, C'_A\}_K\rangle$ to $(\nu n_1)(\nu n_2)\overline{c_j}\langle\{n_1, z, n_2, C'_A\}_K\rangle$. We do not perform these easy replacements only because they are somewhat cumbersome and distracting.

The next proposition says that this protocol typechecks.

Proposition 12 *Let E be the environment*

$$
\begin{array}{l}
c_S : \mathit{Public}, c_1 : \mathit{Public}, \ldots, c_n : \mathit{Public}, d_1 : \mathit{Public}, \ldots, d_n : \mathit{Public}, \\
z_1 : \mathit{Any}, \ldots, z_m : \mathit{Any}
\end{array}
$$

Let i_k and j_k be any fixed numbers in $1..n$, for $k \in 1..m$. Let M_k be z_k, for $k \in 1..m$. Then $E \vdash \mathit{Sys} : \mathit{Ok}$.

Proof In order to indicate how the process *Sys* typechecks, we annotate its bound names and variables with their levels, as they are introduced; we also annotate confounders with the terms in which they are used. For

$K_{iS} : \mathit{Secret}$, $K_{Sj} : \mathit{Secret}$, and $z : \mathit{Any}$, we define:

$$\begin{array}{rcl}
\mathit{Send}_{i,j} & \triangleq & \overline{c_S}\langle \underline{i} \rangle \mid \\
& & c_i(x_{nonce} : \mathit{Public}). \\
& & (\nu K : \mathit{Secret}) \\
& & ((\nu C_A : \mathit{Secret} :: \{K, *, (\underline{i}, \underline{i}, \underline{j}, x_{nonce}), C_A\}_{K_{iS}}) \\
& & \quad \overline{c_S}\langle \{K, *, (\underline{i}, \underline{i}, \underline{j}, x_{nonce}), C_A\}_{K_{iS}} \rangle \mid \\
& & \; (\nu C'_A : \mathit{Secret} :: \{*, z, *, C'_A\}_K) \\
& & \quad \overline{c_j}\langle \{*, z, *, C'_A\}_K \rangle)
\end{array}$$

$$\begin{array}{l}
\mathit{Srv} \triangleq \\
\quad c_S(x_A : \mathit{Public}). \prod_{i \in 1..n} [x_A \mathrel{\mathit{is}} \underline{i}]\ (\nu N_S : \mathit{Public})(\overline{c_i}\langle N_S \rangle \mid \\
\quad c_S(x_{cipher} : \mathit{Public}). \\
\quad \mathit{case}\ x_{cipher}\ \mathit{of}\ \{x_{key} : \mathit{Secret}, x_a : \mathit{Any}, x_p : \mathit{Public}, x_{cnf} : \mathit{Any}\}_{K_{iS}}\ \mathit{in} \\
\quad \mathit{let}\ (y_A : \mathit{Public}, z_A : \mathit{Public}, x_B : \mathit{Public}, x_{nonce} : \mathit{Public}) = x_p\ \mathit{in} \\
\quad \prod_{j \in 1..n} [y_A \mathrel{\mathit{is}} \underline{i}]\ [z_A \mathrel{\mathit{is}} \underline{i}]\ [x_B \mathrel{\mathit{is}} \underline{j}]\ [x_{nonce} \mathrel{\mathit{is}} N_S] \\
\quad (\overline{c_j}\langle * \rangle \mid \\
\quad\; c_S(y_{nonce} : \mathit{Public}). \\
\quad\; (\nu C_S : \mathit{Secret} :: \{x_{key}, *, (S, \underline{i}, \underline{j}, y_{nonce}), C_S\}_{K_{Sj}}) \\
\quad\quad \overline{c_j}\langle \{x_{key}, *, (S, \underline{i}, \underline{j}, y_{nonce}), C_S\}_{K_{Sj}} \rangle))
\end{array}$$

$$\begin{array}{l}
\mathit{Recv}_j \triangleq \\
\quad c_j(w : \mathit{Public}).(\nu N_B : \mathit{Public})(\overline{c_S}\langle N_B \rangle \mid \\
\quad c_j(y_{cipher} : \mathit{Public}). \\
\quad \mathit{case}\ y_{cipher}\ \mathit{of}\ \{x_{key} : \mathit{Secret}, y_a : \mathit{Any}, y_p : \mathit{Public}, y_{cnf} : \mathit{Any}\}_{K_{Sj}}\ \mathit{in} \\
\quad \mathit{let}\ (x_S : \mathit{Public}, x_A : \mathit{Public}, x_B : \mathit{Public}, y_{nonce} : \mathit{Public}) = y_p\ \mathit{in} \\
\quad \prod_{i \in 1..n} [x_S \mathrel{\mathit{is}} S]\ [x_A \mathrel{\mathit{is}} \underline{i}]\ [x_B \mathrel{\mathit{is}} \underline{j}]\ [y_{nonce} \mathrel{\mathit{is}} N_B] \\
\quad c_j(z_{cipher} : \mathit{Public}). \\
\quad \mathit{case}\ z_{cipher}\ \mathit{of}\ \{z_s : \mathit{Secret}, z_a : \mathit{Any}, z_p : \mathit{Public}, z_{cnf} : \mathit{Any}\}_{x_{key}}\ \mathit{in} \\
\quad \overline{d_j}\langle \underline{i}, \underline{j} \rangle)
\end{array}$$

Finally, in the given environment E, we set:

$$\begin{array}{rcl}
\mathit{Sys} & \triangleq & (\nu K_{1S} : \mathit{Secret}) \ldots (\nu K_{nS} : \mathit{Secret}) \\
& & (\nu K_{S1} : \mathit{Secret}) \ldots (\nu K_{Sn} : \mathit{Secret}) \\
& & (\mathit{Send}_{i_1,j_1}(z_1) \mid \ldots \mid \mathit{Send}_{i_m,j_m}(z_m) \mid \\
& & \; !\mathit{Srv} \mid \\
& & \; !\mathit{Recv}_1 \mid \ldots \mid !\mathit{Recv}_n)
\end{array}$$

writing $\mathit{Send}_{i_k,j_k}(z_k)$ for $\mathit{Send}_{i_k,j_k}[z_k/z]$. □

As a consequence of the typechecking, we obtain that the protocol does not reveal the message M from A. This conclusion is stated in the following corollary, where for simplicity we restrict attention to the case where M is a numeral. (A numeral is one of the terms 0, $suc(0)$, $suc(suc(0))$, ...)

Corollary 13 *Let i_k and j_k be any fixed numbers in $1..n$, for $k \in 1..m$. Let Sys1 and Sys2 be two versions of Sys where the terms M_k are arbitrary numerals, for $k \in 1..m$. Then Sys1 $\simeq$ Sys2.*

Proof This is an immediate consequence of Proposition 12 and Theorem 11. $\square$

It is also possible to treat variants of the protocol where some of the keys K_{iS} and K_{Sj} are not secret. For example, the keys K_{1S} and K_{S1} might be declared with level *Public*. This variant would correspond to a situation where K_{1S} and K_{S1} may fall into enemy hands (perhaps because the principal at address 1 is part of the enemy). Clearly messages to and from address 1 may no longer be secret, but other messages would not be affected.

6.2 A Second Example

The second protocol has the same purpose as the first, namely the transmission of some sensitive data M from a principal A to a principal B. Here, however, A sends M under a key generated by the server S. This example is interesting because it brings up an issue of trust: A trusts S to provide a key appropriate for the transmission of M.

First, A requests the key by sending its name and a nonce to B. Then B adds its name and a nonce and sends the resulting information to S. In response, S provides a key K_{AB} to both A and B, encrypting it under pre-existent keys, adding the names of A and B, the nonces that A and B generated, and confounders. At this point, A sends M under K_{AB} with a confounder.

Message 1	$A \rightarrow B:$	A, N_A	on c_B
Message 2	$B \rightarrow S:$	A, N_A, B, N_B	on c_S
Message 3	$S \rightarrow A:$	$\{K_{AB}, *, (A, B, N_A), C_S\}_{K_{SA}}$	on c_A
Message 4	$S \rightarrow B:$	$\{K_{AB}, *, (A, B, N_B), C'_S\}_{K_{SB}}$	on c_B
Message 5	$A \rightarrow B:$	$\{*, M, *, C_A\}_{K_{AB}}$	on c_B
Message 6	$B \rightarrow ?:$	A, B	on d_B

Again, c_S, c_A, c_B, and d_B are public channels. The keys K_{SA} and K_{SB} are secret keys for communication from the server to A and B. Both N_A

and N_B are nonces, and C_S, C'_S, and C_A are confounders. As in the first example, we include the last message only in order to illustrate that B is allowed to react, so we do not specify the destination of this message.

We write this example in the spi calculus in much the same style as the first example. The definition is for a given set of messages $M_1, \ldots, M_m$ with source addresses $i_1, \ldots, i_m$ and destination addresses $j_1, \ldots, j_m$, respectively.

$$
\begin{array}{rcl}
Send_{i,j} & \triangleq & (\nu N_A) \\
& & (\overline{c_j}\langle \underline{i}, N_A\rangle \mid \\
& & \;c_i(x_{cipher}). \\
& & \;case\ x_{cipher}\ of\ \{x_{key}, x_a, x_p, x_{cnf}\}_{K_{Si}}\ in \\
& & \;let\ (x_A, y_B, x_{nonce}) = x_p\ in \\
& & \;[x_A\ is\ \underline{i}]\ [y_B\ is\ \underline{j}]\ [x_{nonce}\ is\ N_A] \\
& & \;(\nu C_A)\overline{c_j}\langle\{*, z, *, C_A\}_{x_{key}}\rangle) \\
Srv & \triangleq & c_S(x_A, x_{nonce}, y_B, y_{nonce}). \\
& & \prod_{i\in 1..n}[x_A\ is\ \underline{i}]\ \prod_{j\in 1..n}[y_B\ is\ \underline{j}] \\
& & (\nu K) \\
& & ((\nu C_S)\overline{c_i}\langle\{K, *, (\underline{i}, \underline{j}, x_{nonce}), C_S\}_{K_{Si}}\rangle \mid \\
& & \;(\nu C'_S)\overline{c_j}\langle\{K, *, (\underline{i}, \underline{j}, y_{nonce}), C'_S\}_{K_{Sj}}\rangle) \\
Recv_j & \triangleq & c_j(x_A, x_{nonce}). \\
& & \prod_{i\in 1..n}[x_A\ is\ \underline{i}] \\
& & (\nu N_B) \\
& & (\overline{c_S}\langle \underline{i}, x_{nonce}, \underline{j}, N_B\rangle \mid \\
& & \;c_j(y_{cipher}). \\
& & \;case\ y_{cipher}\ of\ \{x_{key}, y_a, y_p, y_{cnf}\}_{K_{Sj}}\ in \\
& & \;let\ (x_A, y_B, y_{nonce}) = y_p\ in \\
& & \;[x_A\ is\ \underline{i}]\ [y_B\ is\ \underline{j}]\ [y_{nonce}\ is\ N_B] \\
& & \;c_j(z_{cipher}). \\
& & \;case\ z_{cipher}\ of\ \{z_s, z_a, z_p, z_{cnf}\}_{x_{key}}\ in \\
& & \;\overline{d_j}\langle \underline{i}, \underline{j}\rangle) \\
Sys & \triangleq & (\nu K_{S1})\ldots(\nu K_{Sn}) \\
& & (Send_{i_1,j_1}(M_1) \mid \ldots \mid Send_{i_m,j_m}(M_m) \mid \\
& & \;!Srv \mid \\
& & \;!Recv_1 \mid \ldots \mid !Recv_n)
\end{array}
$$

The next proposition and corollary are the analogues of Proposition 12 and Corollary 13, respectively.

Proposition 14 *Let E be the environment*

$$c_S : \mathit{Public}, c_1 : \mathit{Public}, \ldots, c_n : \mathit{Public}, d_1 : \mathit{Public}, \ldots, d_n : \mathit{Public},$$
$$z_1 : \mathit{Any}, \ldots, z_m : \mathit{Any}$$

Let i_k and j_k be any fixed numbers in $1..n$, for $k \in 1..m$. Let M_k be z_k, for $k \in 1..m$. Then $E \vdash \mathit{Sys} : \mathit{Ok}$.

Proof As in Proposition 12, in order to indicate how the process Sys typechecks, we annotate its bound names and variables with their levels, and we annotate its confounders with terms. For $K_{Si} : \mathit{Secret}$, $K_{Sj} : \mathit{Secret}$, and $z : \mathit{Any}$, we define:

$$\begin{array}{l}
\mathit{Send}_{i,j} \triangleq \\
\quad (\nu N_A : \mathit{Public}) \\
\quad (\overline{c_j}\langle \underline{i}, N_A \rangle \mid \\
\quad\; c_i(x_{\mathit{cipher}} : \mathit{Public}). \\
\quad\; \mathit{case}\ x_{\mathit{cipher}}\ \mathit{of}\ \{x_{\mathit{key}} : \mathit{Secret}, x_a : \mathit{Any}, x_p : \mathit{Public}, x_{\mathit{cnf}} : \mathit{Any}\}_{K_{Si}}\ \mathit{in} \\
\quad\; \mathit{let}\ (x_A : \mathit{Public}, y_B : \mathit{Public}, x_{\mathit{nonce}} : \mathit{Public}) = x_p\ \mathit{in} \\
\quad\; [x_A\ \mathit{is}\ \underline{i}]\ [y_B\ \mathit{is}\ \underline{j}]\ [x_{\mathit{nonce}}\ \mathit{is}\ N_A] \\
\quad\; (\nu C_A : \mathit{Secret} :: \{*, z, *, C_A\}_{x_{\mathit{key}}})\overline{c_j}\langle \{*, z, *, C_A\}_{x_{\mathit{key}}} \rangle)
\end{array}$$

$$\begin{array}{rcl}
\mathit{Srv} & \triangleq & c_S(x_A : \mathit{Public}, x_{\mathit{nonce}} : \mathit{Public}, y_B : \mathit{Public}, y_{\mathit{nonce}} : \mathit{Public}). \\
 & & \prod_{i \in 1..n}[x_A\ \mathit{is}\ \underline{i}]\ \prod_{j \in 1..n}[y_B\ \mathit{is}\ \underline{j}] \\
 & & (\nu K : \mathit{Secret}) \\
 & & ((\nu C_S : \mathit{Secret} :: \{K, *, (\underline{i}, \underline{j}, x_{\mathit{nonce}}), C_S\}_{K_{Si}}) \\
 & & \quad \overline{c_i}\langle \{K, *, (\underline{i}, \underline{j}, x_{\mathit{nonce}}), C_S\}_{K_{Si}} \rangle \mid \\
 & & \;(\nu C'_S : \mathit{Secret} :: \{K, *, (\underline{i}, \underline{j}, y_{\mathit{nonce}}), C'_S\}_{K_{Sj}}) \\
 & & \quad \overline{c_j}\langle \{K, *, (\underline{i}, \underline{j}, y_{\mathit{nonce}}), C'_S\}_{K_{Sj}} \rangle)
\end{array}$$

$$\begin{array}{l}
\mathit{Recv}_j \triangleq \\
\quad c_j(x_A : \mathit{Public}, x_{\mathit{nonce}} : \mathit{Public}). \\
\quad \prod_{i \in 1..n}[x_A\ \mathit{is}\ \underline{i}] \\
\quad (\nu N_B : \mathit{Public}) \\
\quad (\overline{c_S}\langle \underline{i}, x_{\mathit{nonce}}, \underline{j}, N_B \rangle \mid \\
\quad\; c_j(y_{\mathit{cipher}} : \mathit{Public}). \\
\quad\; \mathit{case}\ y_{\mathit{cipher}}\ \mathit{of}\ \{x_{\mathit{key}} : \mathit{Secret}, y_a : \mathit{Any}, y_p : \mathit{Public}, y_{\mathit{cnf}} : \mathit{Any}\}_{K_{Sj}}\ \mathit{in} \\
\quad\; \mathit{let}\ (x_A : \mathit{Public}, y_B : \mathit{Public}, y_{\mathit{nonce}} : \mathit{Public}) = y_p\ \mathit{in} \\
\quad\; [x_A\ \mathit{is}\ \underline{i}]\ [y_B\ \mathit{is}\ \underline{j}]\ [y_{\mathit{nonce}}\ \mathit{is}\ N_B] \\
\quad\; c_j(z_{\mathit{cipher}} : \mathit{Public}). \\
\quad\; \mathit{case}\ z_{\mathit{cipher}}\ \mathit{of}\ \{z_s : \mathit{Secret}, z_a : \mathit{Any}, z_p : \mathit{Public}, z_{\mathit{cnf}} : \mathit{Any}\}_{x_{\mathit{key}}}\ \mathit{in} \\
\quad\; \overline{d_j}\langle \underline{i}, \underline{j} \rangle)
\end{array}$$

Finally, in the given environment E, we set:

$$\begin{array}{rcl} Sys & \triangleq & (\nu K_{S1} : \mathit{Secret}) \ldots (\nu K_{Sn} : \mathit{Secret}) \\ & & (\mathit{Send}_{i_1,j_1}(M_1) \mid \ldots \mid \mathit{Send}_{i_m,j_m}(M_m) \mid \\ & & \ !\mathit{Srv} \mid \\ & & \ !\mathit{Recv}_1 \mid \ldots \mid !\mathit{Recv}_n) \end{array}$$

writing $\mathit{Send}_{i_k,j_k}(z_k)$ for $\mathit{Send}_{i_k,j_k}[z_k/z]$. □

Corollary 15 *Let i_k and j_k be any fixed numbers in $1..n$, for $k \in 1..m$. Let Sys1 and Sys2 be two versions of Sys where the terms M_k are arbitrary numerals, for $k \in 1..m$. Then $\mathit{Sys1} \simeq \mathit{Sys2}$.*

Proof This is an immediate consequence of Proposition 14 and Theorem 11. □

7 Further Work

As indicated in the introduction, we regard this work only as a first exploration of a promising approach. This section briefly suggests some possible directions for further work. Several of the suggestions are fairly obvious and safe. Techniques from other information-flow analyses [Den82, Gas88, ØP97, VIS96, ML97, HR98, SV98] may help in pursuing them.

- As mentioned above, this paper relies on a binary view of secrecy according to which the world is divided into system and attacker. A finer model could distinguish individual principals and groups within the system. It could also permit a declassification operation whereby a principal can reduce the secrecy level of the data that it owns.

- The typing system of this paper does not allow comparisons between terms of level *Any* and other operations on those terms. The typing system may be relaxed to allow such operations in cases where their outcomes are not revealed on public channels.

- There is a trivial way to combine the typing system of this paper with any other typing system: we may simply require processes to be typechecked using both systems, separately. Through standard methods, the other typing system may exclude expressions such as $\mathit{suc}((0,0))$ and $\mathit{case}\ \{M_1, M_2, M_3\}_N\ \mathit{of}\ \{x_1, x_2\}_N\ \mathit{in}\ P$, as discussed in section 3. Therefore, even the trivial combination of the two typing systems may be appealing. However, a tighter integration may be more elegant and more powerful.

- This paper concerns only shared-key cryptography. It should be worthwhile to treat public-key cryptography as well.

Other suggestions are more speculative. For the sake of brevity, this list omits applications in other process calculi and avoids any discussion of alternative access-control models.

- The security literature contains quite a few principles for designing protocols (e.g., [WL94, AN95, AN96, Syv96, Aur97]). Perhaps more of those principles could be turned into rules and validated by formal theorems. Woo and Lam's useful principle of full information seems particularly tractable.

- Authenticity is dual to secrecy in the sense that authenticity properties concern the sources of data while secrecy properties concern their destinations. So we may expect that principles and rules similar to those of this paper would yield authenticity guarantees. On the other hand, authenticity and secrecy have significant differences. For example, evidences of timeliness (freshness) appear frequently in authenticity proofs but not in secrecy proofs.

- Inspired by some recent, type-directed compilers (e.g., [TMC+96]), we may imagine a compiler that preserves secrecy levels, mapping secret data of a source program to secret data in a lower-level representation. For instance, such a compiler may translate from the pi calculus to the spi calculus or to another low-level language, offering some secrecy guarantees for the low-level code that it produces [Aba98].

8 Conclusions

Perhaps in part because of advances in programming languages, the idea of static checking of security properties seems to be reviving. The Java bytecode verifier is a recent static checker with security objectives [LY96]. More sophisticated security checks have been based on self-certification and on information-flow techniques [Nec97, MWCG98, ØP97, VIS96, ML97, HR98, SV98]. In the last year (1998), several papers consider other applications of programming-language concepts and techniques to security in the context of process calculi [AFG98, Aba98, BDNN98, CG98, Dam98, LMMS98, RH98].

This work can be seen as part of that revival. It develops a method for static checking of secrecy properties of programs written in a minimal but expressive programming language, the spi calculus. These programs can be concurrent and can use cryptography. The method is embodied in a set of typing rules.

The principles and rules developed in this paper are neither necessary nor sufficient for security. They are not necessary because, like most practical static typechecking disciplines, ours is incomplete. They are not sufficient because they ignore all security issues other than secrecy, and because they do not account for how to implement the spi calculus while preserving secrecy properties. However, these principles and rules provide some useful guidelines. Furthermore, the rules are tractable and precise; so we have been able to study them in detail and to prove secrecy properties, establishing the correctness of the informal principles within a formal model.

Acknowledgments

Butler Lampson suggested studying authentication protocols through classification techniques, several years ago. That suggestion was the starting point for this work.

This work took place in the context of collaboration with Andrew Gordon on the spi calculus, so the themes and techniques of this paper owe much to him. Andrew Gordon, Rustan Leino, and anonymous referees suggested improvements to drafts of this paper. Conversations with Mike Burrows, Steve Kent, and Ted Wobber were helpful too.

References

[Aba98] M. Abadi. Protection in programming-language translations. In *Proceedings of the 25th International Colloquium on Automata, Languages and Programming*, pages 868–883, 1998.

[AFG98] M. Abadi, C. Fournet, and G. Gonthier. Secure implementation of channel abstractions. In *Proceedings of the Thirteenth Annual IEEE Symposium on Logic in Computer Science*, pages 105–116, 1998.

[AG97a] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. In *Proceedings of the Fourth ACM Conference on Computer and Communications Security*, pages 36–47, 1997.

[AG97b] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. Technical Report 414, University of Cambridge Computer Laboratory, January 1997. A revised version appeared as Digital Equipment Corporation Systems Research Center report No. 149, January 1998, and an abridged version will appear in Information and Computation. Extended version of both [AG97a] and [AG97c].

[AG97c] M. Abadi and A. D. Gordon. Reasoning about cryptographic protocols in the spi calculus. In *CONCUR'97: Concurrency Theory*, volume 1243 of *Lecture Notes in Computer Science*, pages 59–73. Springer Verlag, 1997.

[AG98] M. Abadi and A. D. Gordon. A bisimulation method for cryptographic protocols. In *Programming Languages and Systems: 7th European Symposium on Programming, ESOP '98*, volume 1381 of *Lecture Notes in Computer Science*, pages 12–26. Springer Verlag, 1998.

[AN95] R. Anderson and R. Needham. Robustness principles for public key protocols. In *Proceedings of Crypto '95*, pages 236–247, 1995.

[AN96] M. Abadi and R. Needham. Prudent engineering practice for cryptographic protocols. *IEEE Transactions on Software Engineering*, 22(1):6–15, January 1996.

[Aur97] T. Aura. Strategies against replay attacks. In *Proceedings of the 10th IEEE Computer Security Foundations Workshop*, pages 59–68, 1997.

[BAN89] M. Burrows, M. Abadi, and R. M. Needham. A logic of authentication. *Proceedings of the Royal Society of London A*, 426:233–271, 1989. A preliminary version appeared as Digital Equipment Corporation Systems Research Center report No. 39, February 1989.

[BDNN98] C. Bodei, P. Degano, F. Nielson, and H. R. Nielson. Control flow analysis for the π-calculus. In *CONCUR'98: Concurrency Theory*, volume 1466 of *Lecture Notes in Computer Science*, pages 84–98. Springer Verlag, September 1998.

[BN95] M. Boreale and R. De Nicola. Testing equivalence for mobile processes. *Information and Computation*, 120(2):279–303, August 1995.

[BR95] M. Bellare and P. Rogaway. Provably secure session key distribution: The three party case. In *Proceedings of the 27th Annual ACM Symposium on Theory of Computing*, pages 57–66, 1995.

[CG98] L. Cardelli and A. D. Gordon. Mobile ambients. In *Foundations of Software Science and Computation Structures, First International Conference (FoSSaCS '98)*, volume 1378 of *Lecture Notes in Computer Science*, pages 140–155. Springer Verlag, 1998.

[Dam98] M. Dam. Proving trust in systems of second-order processes. In *Proceedings of HICSS 31*, volume VII, pages 255–264, 1998.

[Den82] D. E. Denning. *Cryptography and Data Security.* Addison-Wesley, Reading, Mass., 1982.

[DES77] Data encryption standard. Fed. Inform. Processing Standards Pub. 46, National Bureau of Standards, Washington DC, January 1977.

[DH84] R. De Nicola and M. C. B. Hennessy. Testing equivalences for processes. *Theoretical Computer Science*, 34:83–133, 1984.

[FG95] R. Focardi and R. Gorrieri. A classification of security properties. *Journal of Computer Security*, 3:5–33, 1994/1995.

[FG97] R. Focardi and R. Gorrieri. The compositional security checker: A tool for the verification of information flow security properties. *IEEE Transactions on Software Engineering*, 23(9), September 1997.

[Gas88] M. Gasser. *Building a Secure Computer System*. Van Nostrand Reinhold Company Inc., New York, 1988.

[Gay97] S. Gay. Private communication. September 1997.

[HR98] N. Heintze and J. G. Riecke. The SLam calculus: Programming with secrecy and integrity. In *Proceedings of the 25th ACM Symposium on Principles of Programming Languages*, pages 365–377, 1998.

[KPT96] N. Kobayashi, B. C. Pierce, and D. N. Turner. Linearity and the pi-calculus. In *Proceedings of the 23th ACM Symposium on Principles of Programming Languages*, pages 358–371, 1996.

[LMMS98] P. Lincoln, J. Mitchell, M. Mitchell, and A. Scedrov. A probabilistic poly-time framework for protocol analysis. In *Proceedings of the Fifth ACM Conference on Computer and Communications Security*, pages 112–121, 1998.

[LY96] T. Lindholm and F. Yellin. *The Java Virtual Machine Specification*. Addison-Wesley, 1996.

[Mil91] R. Milner. The polyadic π-calculus: a tutorial. Technical Report ECS–LFCS–91–180, Laboratory for Foundations of Computer Science, Department of Computer Science, University of Edinburgh, UK, October 1991. Appeared in *Logic and Algebra of Specification*, F. L. Bauer, W. Brauer, and H. Schwichtenberg, eds., Springer Verlag, 1993.

[Mil95] R. Milner. The π-calculus. Undergraduate lecture notes, Cambridge University, 1995.

[ML97] A. C. Myers and B. Liskov. A decentralized model for information flow control. In *Proceedings of the 16th ACM Symposium on Operating Systems Principles*, pages 129–142, 1997.

[MP97] R. Milner and B. Pierce. Private communication. September 1997.

[MPW92] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, parts I and II. *Information and Computation*, pages 1–40 and 41–77, September 1992.

[MvOV96] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography.* CRC Press, 1996.

[MWCG98] G. Morrisett, D. Walker, K. Crary, and N. Glew. From System F to typed assembly language. In *Proceedings of the 25th ACM Symposium on Principles of Programming Languages*, pages 85–97, 1998.

[Nec97] G. Necula. Proof-carrying code. In *Proceedings of the 24th ACM Symposium on Principles of Programming Languages*, pages 106–119, 1997.

[NS78] R. M. Needham and M. D. Schroeder. Using encryption for authentication in large networks of computers. *Communications of the ACM*, 21(12):993–999, December 1978.

[ØP97] P. Ørbæk and J. Palsberg. Trust in the λ-calculus. *Journal of Functional Programming*, 7(6):557–591, November 1997.

[Pau98] L. C. Paulson. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 6(1–2):85–128, 1998.

[PS96] B. Pierce and D. Sangiorgi. Typing and subtyping for mobile processes. *Mathematical Structures in Computer Science*, 6(5):409–453, October 1996.

[RH98] J. Riely and M. Hennessy. A typed language for distributed mobile processes. In *Proceedings of the 25th ACM Symposium on Principles of Programming Languages*, pages 378–390, 1998.

[Sch96] B. Schneier. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, Inc., second edition, 1996.

[SV98] G. Smith and D. Volpano. Secure information flow in a multi-threaded imperative language. In *Proceedings of the 25th ACM Symposium on Principles of Programming Languages*, pages 355–364, 1998.

[Syv96] P. Syverson. Limitations on design principles for public key protocols. In *IEEE Symposium on Security and Privacy*, pages 62–72, 1996.

[TMC+96] D. Tarditi, G. Morrisett, P. Cheng, C. Stone, R. Harper, and P. Lee. TIL: A type-directed optimizing compiler for ML. In *Proceedings of the ACM SIGPLAN '96 Conference on Programming Language Design and Implementation*, pages 181–192, 1996.

[VIS96] D. Volpano, C. Irvine, and G. Smith. A sound type system for secure flow analysis. *Journal of Computer Security*, 4:167–187, 1996.

[WL94] T. Y. C. Woo and S. S. Lam. A lesson in authentication protocol design. *ACM Operating Systems Review*, 28(3):24–37, 1994.