An Epistemic Formulation of Information Flow Security
(Draft, Under Review)

Arbob Ahmad
Carnegie Mellon University
adahmad@cs.cmu.edu

Robert Harper
Carnegie Mellon University
rwh@cs.cmu.edu

Abstract
The non-interference (NI) property defines a program to be secure if changes to high-security inputs cannot alter the values of low-security outputs. NI indirectly states the epistemic property that no low-security principal acquires knowledge of high-security data. We consider a directly epistemic account of information flow (IF) security focusing on the knowledge flows engendered by the program’s execution. Storage effects are of primary interest, since principals acquire knowledge from the execution only through these effects. The IF properties of the individual effectful actions are characterized using a substructural epistemic logic that accounts for the knowledge transferred through their execution. We prove that a low-security principal never acquires knowledge of a high-security input by executing a well-typed program.

The epistemic approach has several advantages over NI. First, it directly accounts for the knowledge flow engendered by a program. Second, in contrast to the bimodal NI property, the epistemic approach accounts for authorized declassification. We prove that a low-security principal acquires knowledge of a high-security input only if it is authorized by a proof in authorization logic. Third, the explicit formulation of IF properties as an epistemic theory provides a crisp treatment of “side channels.” Rather than prove that a principal does not know a secret, we instead prove that it is not provable that the principal knows that secret. The latter statement characterizes the “minimal model,” for which a precise statement may be made, whereas the former applies to “any model,” including those with “side channels” that violate the model’s basic premises. Fourth, the NI property is re-positioned as providing an adequacy proof of the epistemic theory of effects, ensuring that the logical theory corresponds to the actual program behavior. In this way we obtain a generalization of the classical approach to IF security that extends to authorized declassification.

Keywords information flow security, non-interference, authorized declassification, epistemic logic

1. Introduction
Standard accounts of information flow security (IFS) in programming languages express confidentiality in terms of the non-interference (NI) definition given by Goguen and Meseguer [16] stating that changes to high-security inputs cannot influence low-security outputs. This criterion may be seen as an indirect expression of the desired property that information provided by a high-security source is not disclosed to a low-security destination. Put in other terms, IFS seeks to enforce the epistemic requirement that knowledge possessed by high-security principals should not flow to low-security principals. In this paper we develop another approach to IFS based on the following key ideas:

1. IFS is defined in terms of effects that a program has on its execution environment, following Crary et al. [11].
3. Authorized declassification of sensitive data is permitted, using authorization logic [1, 15] to validate its use in a program.
4. The computational adequacy of the epistemic theory of program actions is verified using a generalization of NI [16].

The distinctive feature of the present approach is that IFS is phrased directly in terms of the knowledge that a principal may gain by executing a well-typed program. More precisely, IFS is expressed by necessary conditions on the derivability of statements of the form $[k]S$ stating that a principal $k$ possesses (knows) fact $S$. When $k$ is a low-security principal, and $S$ is a high-security fact, this amounts to proving that $k$ can come to know $S$ only under specified conditions—in the simplest case, falsehood, which amounts to showing that $k$ cannot know $S$ as the result of a well-typed execution. More generally, we show that $[k]S$ may be derived only under such circumstances only if there is a proof in authorization logic underwriting the information flow. This generalizes the previous statement by admitting controlled declassification.

It is important to our account that security is phrased in terms of the non-derivability of a knowledge statement, rather than derivability of its negation. The distinction lies in the ever-present possibility of “side channels”, such as measurements of time- and power-consumption, that are not typically modeled in a type system for IFS [8, 17]. Because of these “out of the model” attacks, it is almost never possible to prove the negation of the statement that a low-security principal knows a high-security fact. On the other hand it is possible to show that such a statement is underivable within the epistemic theory characterizing the effects of the program execution. This amounts to a precise characterization of the attacks against which the type system mounts a successful defense, avoiding the need for vague provisos about the limitations of the model.

The role of the NI property is re-positioned in our work as the basis for the proof of the computational adequacy of the epistemic theory. After all, a theory that predicts no knowledge disclosures would ensure that no knowledge statement is ever derivable. We must show, contrarily, that the epistemic theory is adequate in the
sense that it properly detects interference, even in the presence of
declassification. This is achieved using a generalization of NI
that, when coupled with authorization logic, provides a logical
account of IFS in the presence of declassification, something that
is problematic in the pure NI framework.

The epistemic framework we propose offers several advantages
over purely NI-based accounts of IFS:

1. It focuses attention directly on the core problem of confiden-
tiality, which is to control the knowledge that a principal may
acquire as a result of executing a program.

2. It provides a linkup between authorization [1, 15] and security
in a single framework. Authorization logic ensures that security
protocols are obeyed; epistemic logic gives these protocols
meaning in terms of confidentiality and integrity.

3. It naturally encompasses declassification [37], a well-known
weakness of the pure NI framework.

4. It uses substructural reasoning to express ephemeral, as well as
persistent, knowledge [13]. For example, an internal data
structure may “know” a secret at one moment, but “forget”
that secret at the next moment (if, say, some datum is erased).

5. It provides the basis for developing a tool to explore the epis-
temic consequences of a programming language and its asso-
ciated authorization logic. Such consequences can be hard to
envison without mechanical assistance to trace out the possible
consequences of a policy.

One notable weakness of our framework is the simplicity of
its authorization logic. A more expressive authorization logic such as
PCMLo [4] can encode more interesting authorization policies and
would demonstrate the full advantage of the linkup between
authorization logic and epistemic logic.

Overview

This section outlines the methodology of the paper by describing
how it applies to some example programs. Although these descrip-
tions omit many details, the important ideas are introduced.

The security language SL we analyze distinguishes computa-
tions that may have storage effects from effect free expressions by
dividing them into two distinct syntactic classes in a monadic lan-
guage for effects [24, 25, 32]. We write σ for expressions and Σ
for commands. An expression may contain a suspended command, which
is denoted cmd(τ), but evaluation of the expression never
executes the command. Other than these suspended commands, ex-
pressions closely resemble the pure expressions of functional lan-
guages. The return command ret forms a command from an ex-
pression by returning the value of the expression without per-
forming any effects. A suspended command is eliminated by the bind
command x ← e1; m2. Bind evaluates the expression e1 to a sus-
pended command, which is a value. The suspended command is
then executed, and the value it returns is bound to the variable x in
the scope of the command m2. For brevity, when the variable is not
used we omit the binding, and when e1 is a suspended command
we write x ← m1; m2 for x ← cmd(m1); m2. The commands
get and set read from and write to assignable variables, which we
will call assignables.

Each command is run on behalf of a principal, which dic-
tates the storage operations it may perform. The sudo command
switches the principal on behalf of whom a command is run en-
abling it to read assignables that the less privileged principal can-
not access directly. Therefore, principals may also be thought of as
roles. The sudo switches are reminiscent of upcalls performed by
operating systems such as the UNIX sudo. Passing arbitrary val-
ues computed by a more privileged principal back to a less privi-
leged principal would subvert the access restriction. To avoid this
the sudo requires that the type of the value returned is informa-
tive only to principals that can perform all of the reads within the
sudo. Crary et al. [11] defined non-informativeness to permit more
privileged reads in a limited scope. Our approach is distinguished
by the choice to syntactically represent the non-informative com-
mands with a sudo command. We also differ in explicitly running
commands on behalf of principals to dictate the effects that may be
performed rather than implicitly representing this information in
the type system.

The example program in Figure 1 reads the contents of the
assignables a and b and writes their conjunction to the assignable
c under the store typing Σ. The assignables a, b, and c store val-
ues of type bool. Each assignable is associated with a permission
set of principals that may read its contents. The permission set of a
is \{ k1, k2 \} = Φa indicating that both principals may read it. The
permission set of both b and c is \{ k2 \} = Φb = Φc indicating
that only k2 may read them. As we focus on confidentiality rather
than integrity, there is not an analogous restriction for writing to
an assignable. The example program initially runs on behalf of k1,
and then performs a sudo to run on behalf of k2. In this simplest
case, the type returned by the sudo command is completely non-
informative because it is unit. The sudo is necessary because the
permission set Φa does not include the principal k1. The conjunc-
tion is computed with a nested if-then-else expression.

The type system constrains which assignables a principal may read,
and in what order reads and writes may be performed in order to restrict the possible information flows. Each command is
associated with an effect level based on the reads and writes it
performs. The effect level consists of a read set that is a set of prin-
cipals permitted to see the result returned by the command and a
write set that is a set of principals to whom the command may
disclose information through its writes. The read set is a set that
may see the result rather than the set that may see the result be-
cause the type system builds in weakening as an admissible property. It is
always safe from a confidentiality perspective to impose a more
severe restriction on the principals that may see the result. For
example, it is safe to assert that no principal is permitted to see the
result. Similarly, it is safe to assert that a command may write to
assignables readable by more principals than is actually true since
this imposes a greater restriction on the information that may be
passed into the command.

The intersection of the permission sets of the assignables read
by a command is an upper bound on its read set as the value
returned by the command may contain information read from any
or all of these assignables. Only principals permitted to read all
of the assignables may see the result. The union of the permission
sets of the assignables written by a command is a lower bound on
its write set as information passed into the command may affect

\[ \Sigma = a : \text{bool} @ \{ k_1, k_2 \}, b : \text{bool} @ \{ k_2 \}, c : \text{bool} @ \{ k_2 \} \]

\[ \text{set}(c)(\text{false}); \]

\[ x \leftarrow \text{get}[a]; \]

\[ \text{sudo}[k_1 \rightarrow k_2](y \leftarrow \text{get}[b]; \]

\[ \text{if } y \text{ then} \]

\[ \text{if } x \text{ then} \]

\[ \text{cmd(set}(c)(\text{true})) \]

\[ \text{else} \]

\[ \text{cmd(ret} \Rightarrow) \]

\[ \text{else} \]

\[ \text{cmd(ret} \Rightarrow); \]

\[ \text{ret} \Rightarrow \]
the value written to any one of the assignables modified by the command. Therefore, a principal that belongs to the permission set of any of the assignables may indirectly read this value from the assignables written. As a result, the bind command that sequences two commands requires that the read set of the bind is contained in the intersection of the read sets of the respective commands and that the write set of the bind contains the union of the write sets of the respective commands.

The read set of the first two commands of the example program must be contained in the permission set $\Phi_c$, and their write set must contain $\Phi_c$. The write to $c$ imposes no constraint on the read set of the first command, and the read from $a$ imposes no constraint on the write set of the second command.

The $\texttt{sudo}$ command has an unrestricted read set because the resulting value is non-informative thereby preventing the reads performed within the $\texttt{sudo}$ from disclosing information through its result. In the second part of the example run by $k_2$, the read set of the $\texttt{sudo}$ is unrestricted even though the read set of the command within the $\texttt{sudo}$ must be contained in $\Phi_c$. Therefore, the read set of the full example program need only be contained in the permission set $\Phi_c$. The $\texttt{sudo}$ preserves the write set of the command within it as writes performed within a $\texttt{sudo}$ can be affected by values passed into the command just like other writes. The write set of the $\texttt{sudo}$ in the example must contain the permission set $\Phi_c$. This is also the write set of the full program as only $c$ is written to by either principal. Note that the read set for the full program is $\Phi_c$, reflecting that principal $k_1$ only learns the contents of $a$, not $b$.

To prevent reading from one assignable and then writing the result to another with a less restrictive permission set, the bind command requires that the read set of the first command contains the write set of the second. For example, the bind executed by $k_2$ first reads from $b$ and then writes to $c$. Therefore, this restriction requires $\Phi_b \supseteq \Phi_c$. In the full program, the read from $a$ also precedes the write to $c$ within the $\texttt{sudo}$ so $\Phi_a$ must also contain $\Phi_c$.

These two requirements are reasonable as the final value written to $\Phi$ because the type summarizes what may happen in either branch.

We have an epistemic theory that governs the epistemic consequences of traces. The semantic actions express the epistemic consequences of each effect in the trace as linear implications that consequence the next trace action in the context and modify the knowledge of principals and assignables appropriately. Linearity enables principals and assignables to "forget" knowledge. An assignable may forget its previous contents when it is overwritten, and a principal may forget what it learned within a $\texttt{sudo}$ command when it leaves the scope of the variables it bound in the $\texttt{sudo}$. We present two of these semantic actions here to demonstrate what is expressed by the semantic actions for the read and write actions.

\[
\text{do}(\text{rd}_a[a]) \otimes [k]a(X) \odot [a]a(Y) \rightarrow [k]a(X \cdot Y) \odot [a]a(Y)
\]

\[
\text{do}(\text{wr}_a[a]) \otimes [k]a(X) \odot [a]a(Y) \rightarrow [k]a(X) \odot [a]a(X)
\]

The proposition $[p]a(X)$ represents the knowledge of an entity $p$, which may be either a principal or an assignable. The special atomic proposition $a(X)$ maintains all of the knowledge in a single proposition. We abstractly represent the knowledge of the principals because we are primarily interested in how information flows between principals, not precisely what information is transferred. The symbols $X$ and $Y$ represent two such sets of secrets implicitly universally quantified over each formula. The $\otimes$ operator combines these into a single set of secrets. Each entity's secrets are grouped in a single $a(X)$ as otherwise a semantic action that causes an entity to forget may only consume part of that entity's knowledge. For example, if there was another proposition $[a]a(Z)$, in the context then the semantic action for writing to $a$ would only erase part of the previous information stored in the assignable. The $\text{do}(\alpha)$ proposition indicates the next trace action to be performed. The action $\text{rd}_a[a]$ shares the assignable's knowledge, $a(Y)$, with the principal $k$ performing the action. The previous knowledge of the principal, $\text{do}(\alpha)$, is preserved so the resulting knowledge is $a(X \cdot Y)$. The knowledge of the assignable is also preserved. The action $\text{wr}_a[a]$ is similar except the knowledge is transferred from the principal $k$ to the assignable $a$ and the previous knowledge of $a$ is forgotten.

Returning to the example, if the initial contents of $a$ and $b$ are both true then the trace of the example program would be:

\[
\text{wr}_a[c], \text{rd}_a[a], \text{sudo}[k_1 \rightarrow k_2], \text{rd}_b[b], \text{wr}_b[c], \text{sudo}[k_1 \leftarrow k_2]
\]

This trace makes $c$ learn anything previously known by $a$ and $b$. The flow from $b$ to $c$ is immediate as $k_2$ writes to $c$ after reading $b$. The flow from $a$ to $c$ requires an intermediate flow of knowledge from $k_1$ to $k_2$, which results from the semantic action for $\text{sudo}[k_1 \rightarrow k_2]$ since any variable bound before the $\text{sudo}$ remains in scope within the $\text{sudo}$. The trace also results in a flow of knowledge from $a$ to $k_1$ but not from $b$ to $k_1$ as this was the purpose of reading $b$ within the $\text{sudo}$. If a contained false instead then the trace would be the same except the $\text{wr}_b[c]$ action would be replaced by a pseudo action reflecting that this write was possible even though it did not occur dynamically.

The disclosure of knowledge between principals and assignables defined by the semantic actions has several important properties that will be formally stated and proved later, but we briefly introduce a few of them here. The disclosure interpolation lemma states that if $T$ discloses $a$ to $c$ and $T = T_1 ; T_2$ then there is an entity $p$ such that $T_2$ discloses $a$ to $p$ and $T_2$ discloses $p$ to $c$. In the example trace the lemma holds of the disclosure from $a$ to $c$ with $p = k_2$ by taking $T_1 = \text{wr}_b[c], \text{rd}_a[a], \text{sudo}[k_1 \rightarrow k_2]$ and $T_2 = \text{rd}_b[b], \text{wr}_b[c], \text{sudo}[k_1 \leftarrow k_2]$. The knowledge transfers derived from the trace in the epistemic theory are related to the values computed through the execution of the program that produced the trace by the adequacy theorem for the epistemic theory. The adequacy theorem implies that if we...
change the initial contents of \(a\) from true to false while leaving the rest of the state unchanged and if in the final state, the value stored in \(c\) changes from true to false then the trace must disclose \(a\) to \(c\). The adequacy theorem demonstrates that the semantic actions correctly derive all information flows of a trace that may occur through the execution of the program that generated that trace. In fact, the semantic actions conservatively assume that more disclosures may occur than are actually possible.

The typing soundness lemma asserts that if the trace of a well-typed program discloses \(a\) to \(k_1\) then \(k_1\) must belong to \(\Phi_a\). In the example, this means \(k_1\) and \(k_2\) must belong to \(\Phi_a\) and \(k_2\) must belong to \(\Phi_b\). The conservativeness of the semantic actions makes the requirements of the typing soundness lemma more strict.

The familiar NI theorem implies that if two executions produce final states that differ in the value of \(c\) then there must be an assignable whose values differ in the initial states and whose permission set is no more restrictive than that of \(c\). In the example, this could be either \(a\) or \(b\) as both have permission sets that are no more restrictive than \(c\) and the final value stored in \(c\) is computed from their initial values. NI is proved as a corollary of adequacy and typing soundness.

The epistemic approach can go beyond NI results. We introduce a declassification command \(\text{decl}\) that permits a principal to read the contents of an assignable it cannot directly access according to the permission set. The \(\text{decl}\) command requires an authorization proof that the assignable may be declassified. For simplicity, these authorization proofs are abstract tokens of authentication obtained by executing the \(\text{auth}\) command. The authorization proofs are proofs of propositions in the same epistemic logic used to represent the knowledge.

Figure 2 defines a second example program run on behalf of \(k_1\). It illustrates the use of declassification and authentication. As in the first example, the program computes the conjunction of the values stored in the assignables \(a\) and \(b\) and stores the result in \(c\), but the store typing \(\Sigma'\) differs from \(\Sigma\) in the permission set \(\Phi_c\), which is now \(\{k_1, k_2\}\). The first example program is ill-typed in \(\Sigma'\) because \(\Phi_b \not\supset \Phi_c\), so the write to \(c\) following the read from \(b\) is disallowed. To make the program well-typed, we declassify \(b\) rather than performing a "udo" to access it. This declassification requires an authorization proof from an \(\text{auth}\) command that authenticates \(k_2\). If the authentication fails, the value stored in \(c\) will remain false; however, if it succeeds, \(b\) is declassified using the resulting proof, and the conjunction of \(a\) and \(b\) is written to \(c\) as before.

The example declassification complicates reasoning about information flow. In the example, the final contents of \(c\) in two runs of the program may differ based on the success or failure of the \(\text{auth}\) command even if the initial values stored in \(a\) and \(b\) are true in both runs. Many of the theorem statements are modified to account for the outcomes of authentication. Moreover, additional trace effects for declassification and authentication require semantic actions specifying their epistemic consequences. An authentication effect in the trace creates a persistent proof authorizing appropriate declassifications. This proof is discharged in the semantic action for declassification. Finally, the NI theorem is generalized to assert that a low-security principal acquires knowledge of a high-security input only if it is authorized by a proof in authorization logic.

2. Security language SL

Figures 3, 4, and 5 formally define SL. The terms are divided into two syntactic categories yielding a modalic structure as in Crary et al. [11], but the type system and dynamic semantics differ in a few ways including the explicit representation of non-informative upcalls as changing principals and the addition of effect traces.

2.1 Type system

The types \(A\), \(B\) defined in Figure 3 are mostly familiar. One notable exception is the type of suspended commands, \(\text{cmd}_d[\Phi_1. \Phi_2](A)\). It indicates the type \(A\) returned by the command as well as its effect level and the principal on behalf of whom it is run. The expressions \(e\) are pure as their evaluation cannot cause writes or reads from assignables. Therefore, the typing judgment for expressions, \(\Sigma; \Gamma \vdash e : A\), is mostly familiar as seen in rule 3.1. The most notable difference is the separation of the context into the variable context \(\Gamma\) and the store context \(\Sigma\). The store context is only used to type the suspended commands within expressions in rule 3.2. This rule embeds a command in an expression as a suspended computation. A suspended command is always a value so it does not perform any reads or writes when it is evaluated within an expression.

The commands \(m\) are computations that read from and write to the store. Most are standard for a monadic language such as Pfennig and Davies [33]. The judgment \(\Sigma; \Gamma \vdash m : \tau \rightarrow A[\Phi_1. \Phi_2]\) is more elaborate than traditional monadic type systems because it restricts the effect level \([\Phi_1. \Phi_2]\) to control information flow. The subscript \(\tau\) indicates the principal on behalf of whom the command is run. The read set \(\Phi_1\) is a set of principals permitted to see the value returned by the command. The write set \(\Phi_2\) is a set of principals to whom the command may disclose information through its writes. The type system builds in weakening of the effect level as an admissible property. Therefore, a command with effect level \([\Phi_2'. \Phi_1']\) may also be typed with effect level \([\Phi_2', \Phi_2]\) if \(\Phi_2' \subseteq \Phi_2\) and \(\Phi_1' \supseteq \Phi_2\). For example, rule 3.3 for typing the command \(\text{ret}\)\(e\) permits any effect level because the \(\text{ret}\) command evaluates the pure expression \(e\) without performing any effects.

Rule 3.4 for typing the bind command, \(x \leftarrow e; \ m\), is critical for restricting information flow. The expression \(e\) is a suspended command so its type \(\text{cmd}_d[\Phi_1. \Phi_2](A)\) includes its effect level. The typing judgment for the command \(m\) gives the effect level \([\Phi_2', \Phi_2]\) of the second part of the bind. Rule 3.4 restricts how the subcommands of a bind may be chained together. Consider the bind when \(e\) is a suspended command that reads the assignable \(a\), \(\text{cmd}_d[\Phi_1. \Phi_2](\text{get}(a))\), and \(m\) writes the value read from \(a\) to another assignable \(b\), \(\text{set}(b)(x)\). As \(\text{get}\) is used to read an assignable, rule 3.5 requires that the executing principal is in the permission set \(\Phi_a\) associated with \(a\) and that \(\Phi_a \supseteq \Phi_1\). Intuitively, the rule imposes no restrictions on the write set. Conversely, rule 3.6 requires that the permission set \(\Phi_b \subseteq \Phi_2\) and imposes no restriction on the read set. Therefore, the restriction of rule 3.4 that \(\Phi_2' \subseteq \Phi_2\) implies \(\Phi_2' \subseteq \Phi_a\) as \(\Phi_b \subseteq \Phi_2' \subseteq \Phi_2 \subseteq \Phi_a\). This means that the principals that may learn the contents of \(a\) indirectly by reading the contents of \(b\) can also just directly read the contents of \(a\).
If each of the subcommands of a bind command reads from some assignables then the premise of rule 3.4 that requires $\Phi^r \subseteq \Phi^s \cap \Phi^t$ forces the read level to be restrictive enough to protect all of the assignables read. For example, if the permission set of a is $\Phi_a = \{k_1, k_2\}$ and the permission set of b is $\Phi_b = \{k_2, k_3\}$ then the read level of a bind command that reads both of these assignables must be a subset of $\{k_2\}$ as only $k_2$ may read both assignables. This restriction is necessary in the case that the bind’s result contains information about both values read from the assignables. For example, the result returned by the command could be a pair containing both values. Similarly, the premise that requires $\Phi^r \supseteq \Phi^s \cup \Phi^t$ forces the write level to reflect all of the assignables that may be written in either part of the sequencing command. A value passed into the sequencing command may be written in either of the subcommands and therefore, any of the principals that can read any of the assignables written to by the command may be able to read that value.

Rules 3.5 and 3.6 for the `net` and `get` commands are asymmetric because there is no restriction on the principal on behalf of whom the `net` command executes whereas rule 3.5 requires that the executing principal is in the permission set of the assignable read. This asymmetry reflects the focus on the confidentiality instead of the integrity of the assignables. As usual, integrity in the sense of NI can be addressed with a dual technique [9]. This form of integrity prevents low-integrity inputs from influencing high-integrity outputs, but does not make any other guarantees about the values written to high-integrity outputs. The application to integrity is outlined in section B of the supplementary material. Essentially, the dual representation flips the lattice of principals upside down, but most of the other components of SL remain the same.

Rule 3.7 for the `sudo` command relies on the informativeness judgment $A \not\ni\Phi$ given in Figure 4. If $A \not\ni\Phi$ then the type A is informative only to the principals in $\Phi$. The set $U$ is the set of all principals. Asserting that a type is informative only to the principals in the set of all principals is trivially true so rule 4.1 says that any type A is informative only to the principals in $U$. Rule 4.1 gives the informativeness rule for any type not otherwise specified. For example, it applies to the sum type $A + B$ because even if A and B are both uninformative, the sum type is still informative to any principal since it can see the outer tag. The unit type is never informative. Rule 4.2 asserts it is informative only to the principals in the empty set $\emptyset$. Rule 4.3 depends on the informativeness of the return type as information is extracted from a function by applying it to an argument and observing the result. A pair is analyzed by projecting its components so it is informative to a principal if either component is informative to that principal. Rule 4.4 specifies this by taking union of the two sets of principals to whom the component types are informative. A suspended command is analyzed by running it and viewing the result, but information can also be extracted by reading values written during the execution of the command. Therefore, rule 4.5 states that it is as informative as the union of the informativeness set of its return type and the set of principals that can read assignables written by it. It is safe to assert that a type is informative to more principals than it actually is. Rule 4.6 asserts that a type that is informative only to principals in $\Phi_1$ is also informative only to principals in a larger set.

The `sudo` command is the only one to change the principal on behalf of whom a command is run. The command `sudo[k_1 \rightarrow k_2](m)` switches principals from $k_1$ to the more privileged $k_2$ provided the result returned by $m$ is uninformative to $k_2$. The privilege restriction is enforced by the ordering $k_1 \subset k_2$ in rule 3.4. Because the principal that makes the `sudo` upcall can transfer information to the more privileged principal, the partial order $\subset$ imposes the restriction that the permission sets must be upward closed under $\subset$. That is, if a principal $k \in \Phi$ and $k \subset k'$ then $k' \in \Phi$. Therefore, the more privileged principal could have directly read any secret passed to it through a `sudo`. While executing the privileged command as $k_2$, values may be read that $k_1$ cannot read. The premises $A \not\ni\Phi_2$ and $k_1 \notin \Phi_2$ assure that these values are not returned back to $k_1$ through the result of the `sudo` because the type of the

![Figure 4. Non-informativeness](image-url)
value returned is uninformative to \( k_1 \). In the first example program in Figure 1, principal \( k_1 \) uses a `sudo` to \( k_2 \) to read \( b \) and write its conjunction with a to \( c \). The permission set of \( b \) is \( \Phi_b = \{ k_2 \} \), so \( k_1 \) cannot directly read \( b \). The read set of the command in the `sudo` is contained in \( \Phi_b \), so rule 3.7 requires that the type returned by the command is only informative to the principal \( k_2 \). The type returned is unit so it is not informative to any principal, but we weaken this and say it is informative only to \( k_2 \). Encapsulating the read of \( b \) in a `sudo` command permits the surrounding computation to continue execution without any restriction based on the reads performed within the `sudo`. Note that the write set is not modified by the `sudo` command as any writes it performs can still leak information passed into it.

The command `new a@\Phi := e \in m` declares a new assignable \( a \) with permission set \( \Phi \) initialized to the value of \( e \) and then executes the command \( e \). As observed in Crary et al. [11], the write set of rule 3.8 is not restricted by the permission set \( \Phi \) of the new assignable because the initial value stored in the assignable cannot be leaked unless a reference to the assignable itself is leaked first. Therefore, even if a secret value is written to a freshly allocated assignable with no restrictions on who may read it, the fresh assignable cannot leak the secret unless the assignable itself is first leaked, which is prevented by the type system.

### 2.2 Dynamic semantics

Figure 5 defines memory stores, trace effects, and traces and presents the rules of the execution judgment for a command. A store \( \nu \) is a collection of assignables paired with values representing their contents. We view stores modulo the order of assignables for ease of use in the evaluation rules. The effects \( \alpha \) correspond to each of the effectful operations a command can perform. These effects include the principal that performed the operation and the assignable involved, not the values read or written. A basic trace is a list of effects so it is either empty, \( \varepsilon \), or has an effect added to the front of a trace, \( \alpha, T \). We also form a trace by appending two subtraces together, \( T_1 ; T_2 \). A `sudo` trace \( [T]_{k \rightarrow k'} \) reflects that the subtrace \( T \) is nested inside a `sudo` command. When we reason about these traces in epistemic logic we reduce the traces to simple lists by replacing the `sudo` trace with two `sudo` effects for starting and ending the `sudo` before and after the subtrace. The subtraces of \( T_1; T_2 \) are also appended together to form a single list.

The execution judgment \( \nu, (m | | \mu) \downarrow_k \nu \Sigma'.(m' | | \mu') (T) \) is divided into four parts. There are two execution states \( \nu \Sigma.(m | | \mu) \) and \( \nu \Sigma'.(m' | | \mu') \), each consisting of a store context of assignables in scope within the command, the command itself, and the memory store. The store context \( \Sigma \) is similar to the store context used in the static semantics but without the type information. The permission set of every assignable in the store is given by the store context. The command in an execution state only contains free assignables in its store. The other two parts of the execution judgment are the principal \( k \) on behalf of whom the execution is performed and the trace \( T \) produced by the execution.

The rules of the execution judgment are mostly familiar from similar monadic languages with the small addition of the traces for recording the effects. Rule 5.1 produces an empty trace since the `ret` command just evaluates a pure expression and has no storage effects. Rule 5.2 concatenates the traces of its subcommands together as expected, but it also adds a `leak` pseudo effect in the middle to account for writes that may not have occurred dynamically but were possible according to the write set of the suspended command. When the example program in Figure 1 is executed, the second write to \( c \) may not occur dynamically but will be reflected in the trace through the `leak` effect. This rule defines how a suspended command is executed. The expression is evaluated to a suspended command, which is a value. Then the suspended command is paired with the current store and executed to produce an intermediate execution state. Since this execution state is the result of an execution, its command is a `ret` with a value. This value is substituted into the second subcommand of the bind. The result of the substitution is combined with the store context and store from the intermediate execution state and then executed to produce the final execution state. Rules 5.3 and 5.4 read from and write to the memory store, respectively. Each produces a single element trace to represent that the corresponding operation has occurred. Rule 5.5 is primarily noteworthy for the change in principal from \( k \) in the conclusion to \( k' \) in the premise. The trace \( [T]_{k \rightarrow k'} \) nests the trace \( T \) of the subcommand of the `sudo` in square brackets indicating the principals involved and the extent of the non-informative block. Rule 5.6 conses an effect indicating the assignable declared to the front of the trace of its subcommand. The subcommand is executed in an extended memory store that includes the new assignable and its initial value.

### 3. Epistemic Logic

The logic we employ to model information flow is directly taken from DeYoung and Pfenning [13]. In addition to the cut elimination property of the substructural epistemic logic, which enables proving that undesired knowledge transfers are not derivable, the features of this logic that are of particular importance for our representation are the linear knowledge modality and the monad. The linear knowledge modality is also known as possession. It allows an entity to possess a secret temporarily. For example, an assignable may temporarily possess one secret until another value is written to the assignable causing it to possess a different secret. Similarly, a principal may temporarily acquire some secrets during a `sudo` and then lose them at the end of the `sudo` block. The principal must perform additional reads in subsequent `sudo` blocks if it needs to reacquire these secrets. The monad indicated by \{ \} marks the main branch of a derivation making it possible to restrict the semantic actions to a single branch of the derivation in which the actions of
the order in which actions are processed. There would be a more direct representation of this requirement for this type of representation. If the applied is a standard technique for this type of representation. If the

Semantic actions specify the epistemic consequences of each trace effect. Semantic actions for the effects defined in the dynamic semantics are given in Figure 6. The semantic action for each effect α has the form (6.1). The semantic action for each effect α has the form (6.2). The semantic action for each effect α has the form (6.3). The semantic action for each effect α has the form (6.4). The semantic action for each effect α has the form (6.5). The semantic action for each effect α has the form (6.6).

\[
\text{do}(\text{[k→k']} \odot [k]a(X) \odot [k']a(Y)) \\
\rightarrow \{[k]a(X) \odot [k']a(X + Y) \odot \text{next}\} \tag{6.1}
\]

\[
\text{do}(\text{[l→l']) \odot [k']a(X) \rightarrow \{[k]a(1) \odot \text{next}\} \tag{6.2}
\]

\[
\text{do}(\text{rd}[a]) \odot [k]a(X) \rightarrow \{a[Y]\} \tag{6.3}
\]

\[
\text{do}(\text{wr}[a]) \odot [k]a(X) \odot [a[Y]\} \tag{6.4}
\]

\[
\text{do}(\text{leak}_k(\Phi)) \rightarrow \{\text{do}(\text{wr}_k[a])\}, \tag{6.5}
\]

\[
\text{next} \odot \text{doTrace}(\alpha, T) \rightarrow \{\text{do}(\alpha) \odot \text{doTrace}(T)\} \tag{6.6}
\]

---

**Figure 6. Semantic Actions**

The traces are processed one after another. The remaining features of the logic are familiar from standard linear logic.

Semantic actions specify the epistemic consequences of each trace effect. Semantic actions for the effects defined in the dynamic semantics are given in Figure 6. The semantic action for each effect α has the form (6.1). The semantic action for each effect α has the form (6.2). The semantic action for each effect α has the form (6.3). The semantic action for each effect α has the form (6.4). The semantic action for each effect α has the form (6.5). The semantic action for each effect α has the form (6.6).

\[
\text{do}(\text{[k→k']} \odot [k]a(X) \odot [k']a(Y)) \\
\rightarrow \{[k]a(X) \odot [k']a(X + Y) \odot \text{next}\} \tag{6.1}
\]

\[
\text{do}(\text{[l→l']) \odot [k']a(X) \rightarrow \{[k]a(1) \odot \text{next}\} \tag{6.2}
\]

\[
\text{do}(\text{rd}[a]) \odot [k]a(X) \rightarrow \{a[Y]\} \tag{6.3}
\]

\[
\text{do}(\text{wr}[a]) \odot [k]a(X) \odot [a[Y]\} \tag{6.4}
\]

\[
\text{do}(\text{leak}_k(\Phi)) \rightarrow \{\text{do}(\text{wr}_k[a])\}, \tag{6.5}
\]

\[
\text{next} \odot \text{doTrace}(\alpha, T) \rightarrow \{\text{do}(\alpha) \odot \text{doTrace}(T)\} \tag{6.6}
\]

---

4. Adequacy and Non-Interference

In this section we describe the main technical results about the information flow properties of SL. Some properties that are not essential for understanding the main technical development are deferred to section A of the supplementary material. To state these results precisely we must define what is considered a flow of information in SL. If an information flow was defined to include too much the adequacy theorem would not hold. For example, if observing a difference in the number of steps of execution was considered a form of information flow then the theorem would be false. More importantly, if a principal k computes two different values but those values appear equivalent to k because their type is uninformative then we do not consider it a leak. We compare values up to equivalence relative to the view of a principal, which is defined to be the least congruence containing the rule in Figure 7. This ≈ rule equates two values if their type is not informative to the principal. A difference in the contents of the assignables in the initial store may affect whether certain new assignables are allocated. Therefore, the equivalence judgment is relative to two different storage contexts. The notation $\Sigma_1 \cap \Sigma_2$ indicates the storage
context containing assignables that appear in both, and the notation 
\( \Sigma_1| \) indicates the context containing only those assignables whose 
permission sets include \( k \).

We will employ several properties of this equivalence. For example, Lemma A.1 states that substitution respects the equivalence judgment. It is essential to the proof of Lemma A.2, which states that equivalence is preserved under evaluation. The formal 
statements and proofs of these lemmas are deferred to the supplementary 
material.

### 4.1 Preliminary Technical Results

We prove some results about the definitions from the previous 
section that will be used to prove the central results of this section.
The first theorem, which corresponds to the analogous result in 
DeYoung and Pfenning [13], states a property of our model for 
reasoning about what is and is not derivable.

**Theorem 4.1. (Rewrite Step Schemata).** Each rewrite step from a valid state has exactly one of the following forms:

1. \( \Gamma; \Delta, \text{do}(rd_1[a]), [k]iset(X), [a]is(Y) \rightarrow \Gamma; \Delta, [k]iset(X + Y), [a]iset(Y) \)
2. \( \Gamma; \Delta, \text{do}(wr_1[a]), [k]iset(X), [a]iset(Y) \rightarrow \Gamma; \Delta, [k]iset(X), [a]iset(Y) \)
3. \( \Gamma; \Delta, \text{do}(\langle \rightarrow \rangle, [k]iset(X), [k']iset(Y)) \rightarrow \Gamma; \Delta, [k]iset(X), [k']iset(Y) \)
4. \( \Gamma; \Delta, \text{do}(\langle \rightarrow \rangle, [k]iset(X), [a]iset(Y) \rightarrow \Gamma; \Delta, [k]iset(X), [a]iset(Y) \)
5. \( \Gamma; \Delta, \text{do}(\langle \rightarrow \rangle, [k]iset(X), [a]iset(Y) \rightarrow \Gamma; \Delta, [k]iset(X), [a]iset(Y) \)
6. \( \Gamma; \Delta; \text{doTrace(a, } T), \text{next} \rightarrow \Gamma; \Delta; \text{do(a), doTrace(T)} \)

Moreover, the states in the conclusions of these rewrite steps are valid.

**Proof.** The proof relies on the observation that only the semantic actions have the monadic heads required for a left focusing step to begin a rewrite derivation. There is then a case for each semantic action. This proof is possible because of the structure of the logic and its cut elimination property.

This theorem is essential for showing that only permissible disclosures are derivable as it specifies the possible rewrite steps. Due to the modal restrictions in the logic, there are only a few possible rewrite steps, each corresponding to one of the semantic actions. It simplifies reasoning about disclosure by characterizing each step in a disclosure. Theorem 4.1 facilitates the proofs of several lemmas about our disclosure judgment found in the supplementary material as well as the following lemma, which is used to prove properties of the traces of well-typed programs.

**Lemma 4.1. (Disclosure Interpolation).** If a trace \( T \) is the concatenation of two traces (i.e., \( T = T_1; T_2 \)) and \( T \) discloses \( p \) to \( p' \), then there is an entity \( q \) such that \( T_1 \) discloses \( p \) to \( q \) and \( T_2 \) discloses \( q \) to \( p' \).

**Proof.** The essential observation is that the rewrite steps in Theorem 4.1 only permit actions to be processed one at a time and in the specified order. Therefore, a derivation of \( \Gamma; \Delta \rightarrow_T \Gamma'; \Delta' \) in which \( [p]iset(X) \in \Delta \) and \( [p']iset(Y) \in \Delta' \) yields two derivations: \( \Gamma; \Delta \rightarrow_T \Gamma_1; \Delta'' \) and \( \Gamma; \Delta' \rightarrow_T \Gamma_2; \Delta'' \). As none of the rewrite steps create new knowledge, there must be at least one entity \( q \) such that \( [p]iset(Z) \in \Delta'' \) and \( Z \subseteq X \). The derivations of \( \Gamma; \Delta \rightarrow_T \Gamma_1; \Delta'' \) for varying \( \Gamma; \Delta \) then yield that \( T_1 \) discloses \( p \) to \( q \) for any entity \( q \) that is always in possession of the secret. Such an entity may be found by considering the case where only \( p \) has the secret \( X \) initially. We similarly find that at least one of the entities also has the property that \( T_2 \) discloses \( q \) to \( p' \) from the derivations of \( \Gamma''; \Delta'' \rightarrow_T \Gamma_2; \Delta'' \).

### 4.2 Adequacy

The adequacy theorem proves that any information disclosed according to the dynamic semantics of SL is also disclosed in the logic according to the formal definition given in the previous section, thereby establishing a correspondence between the semantic actions and the actual information flows in the program.

We define information flow in a program both between an assignable and a principal and between two assignables in terms of the definition of equivalence. A flow between an assignable and a principal occurs when executing the program with different initial values for the assignable affects the resulting value of a command executed by the principal. A flow between two assignables occurs when executing the program with different initial values for one assignable affects the final value of the other. This intuition for when there is a flow of information in SL yields the following adequacy theorem.

**Theorem 4.2. (Adequacy).** If \( \Sigma; \Sigma'; \vdash m \approx_k m' \triangleleft_k A \oplus \Phi' , \Psi' , \mu : \Sigma, \mu' : \Sigma' \), then \( \nu \Sigma.(m \parallel \mu) \backsim \nu \Sigma.(\text{ret } v \parallel \mu) (T') \), and \( \nu \Sigma.(m \parallel \mu') \backsim \nu \Sigma.(\text{ret } v' \parallel \mu') (T'' \parallel T') \). Then

1. Either \( v \approx_k v' \) or there exists \( b \in \Sigma \cap \Sigma' \) such that \( \mu(b) \not\approx_k \mu'(b) \) and \( T \) and \( T' \) disclose \( b \) to \( k \).
2. For all \( c \in \Sigma \cap \Sigma' \) such that \( \mu_1(c) \not\approx_k \mu_2(c) \), there exists \( b \in \Sigma \cap \Sigma' \) such that \( \mu(b) \not\approx_k \mu'(b) \) and \( T \) and \( T' \) disclose \( b \) to \( c \).

**Proof.** Structural induction on the derivation of \( \llcorner \). We will give a representative case of the proof for the bind command. The other cases for when the command is a bind are similar, and the remaining cases are straightforward.

In the bind case, \( m = x \leftarrow e_1 ; m_2 \) and \( m' = x \leftarrow e_1' ; m_2' \) such that:

- \( e_1 \llcorner \llcorner \text{cmd}(m_1) \) and \( e_1' \llcorner \llcorner \text{cmd}(m_1') \)
- \( \nu \Sigma.(m_1 \parallel \mu) \backsim \nu \Sigma.(\text{ret } v_1 \parallel \mu) (T_1) \)
- \( \nu \Sigma.(m_1' \parallel \mu') \backsim \nu \Sigma.(\text{ret } v_1' \parallel \mu') (T_1') \)
- \( \nu \Sigma.(v_1/x \llcorner m_2 \parallel \mu) \backsim \nu \Sigma.(\text{ret } v_1 \parallel \mu) (T_2) \)
- \( \nu \Sigma.(v_1'/x \llcorner m_2' \parallel \mu') \backsim \nu \Sigma.(\text{ret } v_1' \parallel \mu') (T_2') \)

By Lemma A.2 we have \( \text{cmd}(m_1) \approx_k \text{cmd}(m_1') : \text{cmd}_k(\Phi', \Psi') \parallel (B) \) as \( e_1 \approx_k e_1' \). By inversion, either \( m_1 \approx_k m_1' \) or \( \text{cmd}_k(\Phi', \Psi') \parallel (B) \parallel \Phi' \) and \( k \not\in \Phi \). In the latter case, we have \( B \not\in \Phi \) by inversion and therefore \( v_1 \approx_k v_1' : B \).

Otherwise, by the first case of the induction hypothesis on the evaluation derivation of \( m_1 \), we have either \( v_1 \approx_k v_1' \) or \( v_1 \approx_k v_1' \). In the latter case, Lemma A.3 for extending disclosures from a prefix of a trace to a whole trace yields \( T = T_1, \text{leak}_k(\Phi'), T_2 \) and \( T' = T_1, \text{leak}_k(\Phi'), T_2 \) also disclose \( b \) to \( k \) completing this case.

In the cases when \( v_1 \approx_k v_1' \), we apply the first case of the induction hypothesis to \( v_1/x \llcorner m_2 \) and \( v_1'/x \llcorner m_2' \) to conclude that
proof of a NI result for SL.

To demonstrate the utility of this methodology we now present the disclosure is derivable in the logic. Therefore, we may use the first case of the induction hypothesis to c to b. Then Lemma A.4 for composing disclosures yields $T = T_1, \text{leak}_k(\Phi_1^f), T_2$ and $T' = T_1', \text{leak}_k(\Phi_1'^f), T_2'$ disclose c to k completing this case.

The theorem states that if there is a flow of information in SL then there is a corresponding disclosure in the trace. This result is essential because of its contrapositive. When there is no disclosure in the trace according to the logic, there is no flow of information in SL. Therefore, to prove a NI result it is sufficient to prove no disclosure is derivable in the logic.

4.3 Non-Interference

To demonstrate the utility of this methodology we now present the proof of a NI result for SL. The adequacy theorem reduces proving a NI result about SL to proving that only permissible disclosures are derivable in the logic when reasoning about the traces of well-typed programs.

We can now prove the following lemma about the confidentiality properties of well-typed programs.

Lemma 4.2. (Typing Soundness). If

\[ \Sigma, \sum_k \vdash_m m \rightsquigarrow k \Phi_k(\Phi_k^f), \mu : \Sigma \text{ and } \nu_S(m || \mu) \downarrow_k \nu_S.T_r.(\text{ret } v || \mu_k) \{T\} \text{ then} \]

1. For all a : $A \times \Phi_a \subseteq \Sigma$ if T discloses a to k then $\Phi_k^f \subseteq \Phi_a$ and $k \in \Phi_a$

2. For all k : $B \times \Phi_b \subseteq \Sigma$ if T discloses a to b then $\Phi_k \subseteq \Phi_a$

3. For all a : $A \times \Phi_a \subseteq \Sigma$ and b : $B \times \Phi_b \subseteq \Sigma$ if T discloses a to b then $\Phi_a \subseteq \Phi_b$

Proof. The proof is by structural induction on the evaluation derivation. The base cases for net, get, and ret are straightforward consequences of the typing rules. We give some representative cases for bind. They critically depend on Lemma 4.1 to reason about the disclosures of the two subcommands independently.

In these cases we have m = x ← e_1; m_2 and:

- $e_1, \downarrow \text{cmd}(m_1)$
- $\nu_S(m_1 || \mu) \downarrow_k \nu_S.T_r.(\text{ret } v || \mu_k) \{T_1\}$
- $\nu_S.T_r.(\text{ret } v || \mu_k) \{T_2\}$

For the first case, we assume T discloses a to k. Therefore, we may apply Lemma 4.1 to conclude that there exists an assignable $p$ such that $T_1, \text{leak}_k(\Phi_1^f)$ discloses a to p and $T_2$ discloses p to k. We proceed by case analysis depending on whether p is and assignable or a principle.

In the former case where p is some assignable, b, we apply the first case of the induction hypothesis to $[v_1/x]m_2$ to conclude that $\Phi_k \subseteq \Phi_k' \subseteq \Phi_a$ and $k \in \Phi_a$. If the derivation of disclosure actually used the $\text{leak}_k(\Phi_1^f)$ then we would have $T_1$ discloses a to k and would be finished by the induction hypothesis. Therefore, we may also apply the third case of the induction hypothesis to conclude that $\Phi_k \subseteq \Phi_a$. Combining this containment with the result of the earlier appeal to the induction hypothesis yields $\Phi_k \subseteq \Phi_a$ and $k \in \Phi_a$ completing this case.

In the latter case where $p$ is a principal, $k'$, Lemma A.5 states that we must have $k' = k$ since any other principal could not carry its knowledge through the complete execution of $m_2$ as the end of a saldo block would clear its knowledge. Therefore, this case holds by an appeal to the first case of the induction hypothesis on $m_1$.

The other cases employ similar reasoning about how the disclosure is divided between the two commands.

Composing the adequacy and typing soundness results yields the expected NI result.

Theorem 4.3. (Non-interference). If

\[ \Sigma, \sum_k \vdash m \rightsquigarrow k A \times \Phi_a(\Phi_k^f), \mu : \Sigma, \mu' : \Sigma', \nu_S(m || \mu) \downarrow_k \nu_S.T_r.(\text{ret } v || \mu_k) \{T\}, \text{ and } \nu_S.T_r.(\text{ret } v || \mu_k' \nu_S.T_r.(\text{ret } v || \mu_k) \{T'\} \text{ then} \]

1. If $v \not\subseteq \Phi_k'$ then there exists $b : B \times \Phi_b \subseteq \Sigma$ such that $\mu(b) \not\subseteq \Phi_k(\Phi_k^f), k \in \Phi_k$

2. For all $b : B \times \Phi_b \subseteq \Sigma$ such that $\mu(b) \not\subseteq \Phi_k(\Phi_k^f), there exists $a : A \times \Phi_a \subseteq \Sigma$ such that $\mu(a) \not\subseteq \Phi_k(\Phi_k^f)$

Proof. NI is a corollary of Theorem 4.2 and Lemma 4.2 by just applying the latter to the disclosures in the conclusions of the former.

The NI result may be better understood by considering the contrapositives of the two parts. If all assignables with k in their permission set are equivalent from the view of k then the resulting values will also be equivalent from the view of k, and if the initial values of every assignable with a permission set at least as permissible as a given assignable are equivalent from the view of k then the final values of the assignable will also be equivalent. Therefore, if only an assignable that does not have k in its permission set is modified then it will not interfere with the final value observed by k, and similarly, if only an assignable with a more restrictive permission set is modified then it will not interfere with the final value of the given assignable.

5. Security language with declassification SLD

The expressiveness of the logic facilitates the addition of authorized declassification to SL. For simplicity, we focus on authorization proofs that take the form of a certificate verifying that the appropriate principal has authenticated. These proofs are atomic in the logic. In this section we describe how the system changes to accommodate authorized declassification and how the theorems change to correspond to the more permissive policy.

5.1 Static and dynamic semantics

The new commands of SLD for authentication and declassification are given in Figure 8. The auth command verifies that the indicated principal has authenticated. Therefore, the type is an option as the verification may fail. The type assign(k) is the type of a proof that k has authenticated. The read level of the command is arbitrary as we assume the database of authentication credentials is readable by all principals. Intuitively, the write level is also unrestricted. Rule 8.2 is similar to rule 3.5 except that instead of requiring that k is in the permission set $\Phi$, the doacl command requires an authorization proof in the form of an authentication certificate of one of the principals in $\Phi$. This certificate is obtained from a successful execution of the auth command. Also unlike a standard get, the read level of the command does not reflect the permission set of the declassified assignable as this access is permitted through the authentication proof rather than the permission set.

The evaluation judgment now contains an additional parameter, S, which corresponds to the authentication database. Explicitly parameterizing by $S$ rather than defining a non-deterministic evaluation judgment facilitates comparing two runs. This parameter is used to specify the two evaluation rules for authentication such that the resulting value depends on the value associated with the authenticating principal in $S$. Rule 8.5 is also very similar to rule 5.3.
The only differences are that the authorization proof must be first evaluated and the result is included in the new trace effect.

Semantic action (8.6) for authorization adds a persistent proposition to the context indicating that the authenticated principal has authorized declassification. Semantic action (8.7) for declassification is similar to semantic action (6.3) for a read as both have the same dynamic behavior in terms of the value produced. The only difference is that the declassification action requires a authorization proof. The value \( \varphi \) witnesses that the authorization proof exists in the trace of any well-typed program because \( \varphi \) is such a proof.

5.2 Authorized declassification

With the addition of authorized declassification it is no longer possible to prove a non-interference theorem as privileged inputs now affect public outputs through a declassification. Nevertheless, it is possible to prove that each disclosure of this type requires a proof of authorization. Many of the lemmas for SLD still hold for SLD though possibly in a slightly modified form.

Theorem 4.1 that states the possible rewrite steps still holds with additional case for the new actions. Theorem 4.2 that states the adequacy of the semantic actions for modeling the actual observed values produced by the dynamic semantics is modified to accommodate the disclosure of values through declassification. For the purposes of this theorem, the \( \text{decl} \) command behaves like a get command as the theorem does not mention permission sets. Therefore, the proof for this case base relies on the similarity between the semantic actions for \( \text{decl} \) and get. The only difference is the additional tracking of the authorization proofs, which does not affect the disclosures. However other cases must be more significantly modified to adjust to the more complicated form of disclosures in the presence of declassification.

The statement of the theorem distinguishes the assignable \( a \) that is declassified from the assignable \( b \) that differs in the initial store because any assignable that is disclosed to the declassified assignable may be leaked through the declassification. To prevent the value of an assignable \( c \) from being leaked by the declassification of \( a \), the permission set \( \Phi_a \) must not be contained in the permission set \( \Phi_c \). If \( \Phi_a \nsubseteq \Phi_c \) then \( c \) cannot be disclosed to \( a \) without an additional declassification. Alternatively, simultaneously enforcing integrity would allow us to avoid undesired leaks by making all declassified assignables have high integrity and all assignables that should not be declassified have low integrity.

Theorem 5.1. (Adequacy). If \( \Sigma; \Sigma'; \vdash m \approx_k m' \vdash_k A@[\Phi', \Phi]^* \), \( \mu : \Sigma', \mu' : \Sigma' \), \( \nu \Sigma. (m \mid \mu) \downarrow^\varphi_\nu \nu \Sigma. (\text{ret } v \mid \mu) \{ T \} \), and \( \nu \Sigma'. (m' \mid \mu') \downarrow^\varphi_\nu \nu \Sigma'. (\text{ret } v' \mid \mu') \{ T' \} \) then

1. Either \( v \approx_k v' \) or there exists \( b \) such that either
   - \( b \in \Sigma \cap \Sigma'_k \) or
   - \( \exists a \in \Sigma \cap \Sigma'_k \), \( \text{decl}_k[a][\varphi][a] \in T \) and \( \text{T}' \), \( S(\varphi) = \text{SOME } \varphi \), and \( T \) and \( T' \) disclose \( b \) to \( a \)

   such that \( \mu(b) \nsubseteq \mu'(b) \) and \( T \) and \( T' \) disclose \( b \) to \( k \).

2. For all \( c \in \Sigma \cap \Sigma'_k \) such that \( \mu(c) \nsubseteq \mu'_c(\varphi) \) there exists \( b \) such that either
   - \( b \in \Sigma \cap \Sigma'_k \) or
   - \( \exists a \in \Sigma \cap \Sigma'_k \), \( \text{decl}_k[a][\varphi][a] \in T \) and \( \text{T}' \), \( S(\varphi) = \text{SOME } \varphi \), and \( T \) and \( T' \) disclose \( b \) to \( a \)

   such that \( \mu(b) \nsubseteq \mu'(b) \) and \( T \) and \( T' \) disclose \( b \) to \( c \).

Proof. The proof is still by structural induction on the derivation of \( \vdash \).

By Lemma A.2 we have \( \text{cmd}(m_1) = \text{cmd}(m'_1) = \text{cmd}_S(\Phi'_1, \Phi'_1)(\text{B}) \) as \( \approx_k \approx_k e_1 \). By inversion either \( m_1 \approx_k m'_1 \) or \( \text{cmd}_S(\Phi'_1, \Phi'_1)(\text{B}) \nsubseteq \Phi \\text{and } k \notin \Phi \). In the latter case, we have \( B \nsubseteq \Phi \) by inversion and therefore \( \approx_k \approx_k e_1 \).

Otherwise, by the first case of the induction hypothesis on the evaluation derivation of \( m_1 \) we have either \( v_1 \approx_k v'_1 \) or there exists \( b \) such that \( b \in \Sigma \cap \Sigma'_k \) or \( \exists a \in \Sigma \cap \Sigma'_k \), \( \text{decl}_k[a][\varphi[a]][a] \in T \) and \( T' \), \( S(\varphi) = \text{SOME } \varphi \), and \( T \) and \( T' \) disclose \( b \) to \( a \) and \( \mu(b) \nsubseteq \mu'(b) \) and \( T \) and \( T' \) disclose \( b \) to \( k \).

In the latter case, Lemma A.3 yields \( T = T_1, \text{leak}_k(\Phi'_1), T_2 \) and \( T' = T'_1, \text{leak}_k(\Phi'_1), T'_2 \) also disclose \( b \) to \( k \), and the traces satisfy the other conditions on \( b \) to complete this case.

In the cases when \( v_1 \approx_k v'_1 \), we apply the first case of the induction hypothesis to \( v_1/x_2m_2 \) and \( v'_1/x'_2m'_2 \) to conclude that \( v \approx_k v' \) or there exists \( b \) such that \( b \in \Sigma \cap \Sigma'_k \) or \( \exists a \in \Sigma \cap \Sigma'_k \), \( \text{decl}_k[a][\varphi[a]][a] \in T \) and \( T' \), \( S(\varphi) = \text{SOME } \varphi \), and \( T \) and \( T' \) disclose \( b \) to \( a \) and \( \mu(b) \nsubseteq \mu'(b) \) and \( T \) and \( T' \) disclose \( b \) to \( k \).

In the former case, we have completed this case. Otherwise, we apply the second case of the induction hypothesis to \( m_1 \) and \( m'_1 \) to conclude that there exists a \( c \) such that \( c \in \Sigma \cap \Sigma'_k \) or \( \exists a \in \Sigma \cap \Sigma'_k \), \( \text{decl}_k[a][\varphi[a]][a] \in T \) and \( T' \), \( S(\varphi) = \text{SOME } \varphi \), and \( T \) and \( T' \) disclose \( c \) to \( a \) such that \( \mu(c) \nsubseteq \mu'(c) \) and \( T \) and \( T' \) disclose \( c \) to \( b \). Then Lemma A.4 yields \( T = T_1, \text{leak}_k(\Phi'_1), T_2 \) and \( T' = T'_1, \text{leak}_k(\Phi'_1), T'_2 \) disclose \( c \) to \( k \) completing this case. Note that in this case the assignable that differs in the initial store is \( c \) while it may be the assignable \( b \) that is declassified to \( k \), necessitates the more general statement of the theorem.

□
The typing soundness lemma changes more substantially as the theorem as originally stated no longer holds due to the addition of declassifications. The revised statement only guarantees non-interference for assignables that could not have been disclosed through declassification.

Lemma 5.1. (Typing Soundness). If
\[
\Sigma; \cdot \vdash \nu \langle \Phi^c \rangle \mu : \Sigma \quad \nu \Sigma' \vdash (\mu \mid m) \nu \Sigma' \vdash (\text{ret } v) \{|\mu|\} \{T\} \text{ then if each assignable } c \text{ associated with a declassification action in } T \text{ has permission set } \Phi_c \text{ such that } \Phi_c \not\subseteq \Phi \text{ then:}
\]
1. For all \(a : A@\Phi_a \in \Sigma \text{ if } \Phi_a \subseteq \Phi \text{ and } T \text{ discloses } a \to k \text{ then } \Phi' \subseteq \Phi_a \text{ and } k \in \Phi_a
2. For all \(a : A@\Phi_a \in \Sigma \text{ if } T \text{ discloses } p \to a \text{ and } p \neq a \text{ then } \Phi_a \not\subseteq \Phi^p
3. For all \(a : A@\Phi_a \in \Sigma \text{ and } b : B@\Phi_b \in \Sigma \text{ if } \Phi_a \subseteq \Phi \text{ and } T \text{ discloses } a \to b \text{ then } \Phi_c \not\subseteq \Phi_b
\]

Proof. The proof follows the same structure as before. Most of the cases are essentially the same. The case for a declassification command uses the fact that the assignable being declassified cannot be the a in cases 1 and 3 because its permission set is not contained in \(\Phi \) by assumption.

The non-interference theorem becomes the following theorem that includes the possibility of an authorized declassification that could subvert the permission sets. It is still a direct corollary of the type soundness and adequacy results.

Theorem 5.2. (Authorized Declassification).
If
\[
\Sigma; \Sigma' \vdash \cdot \vdash m \vdash \nu \langle \Phi^c \rangle \mu : \Sigma \mu' : \Sigma',
\]
\[
\nu \Sigma'.(m \mid |\mu|) \nu \Sigma'.(\text{ret } v) \{|\mu|\} \{T\}, \text{ and }
\nu \Sigma'.(m' \mid |\mu'|) \nu \Sigma'.(\text{ret } v') \{|\mu'|\} \{T'\}
\]
\text{ then}
1. If \(v \neq \Phi_a \) \(v' \) then there exists \(b : B@\Phi_b \in \Sigma \cap \Sigma' \) such that \(\mu(b) \neq \Phi_b \mu'(b) \) and either \(\Phi' \subseteq \Phi_a \) and \(k \in \Phi_b \) or there is a proof authorizing the declassification of an assignable \(c \) with permission set \(\Phi_c \subseteq \Phi_b
2. For all \(b : B@\Phi_b \in \Sigma \cap \Sigma' \) such that \(\mu(b) \neq \Phi_b \mu'(b) \), there exists \(a : A@\Phi_a \in \Sigma \cap \Sigma' \) such that \(\mu(a) \neq \Phi_a \mu'(a) \) and either \(\Phi_a \subseteq \Phi_b \) or there is a proof authorizing the declassification of an assignable \(c \) with permission set \(\Phi_c \subseteq \Phi_a
\]

Proof. The presence of declassification actions in the trace in Theorem 5.1 guarantees the existence of corresponding authorization proofs when composed with Lemma 5.1.

6. Related Work

Early work on language-based IFS is summarized in Sabelfeld and Myers [36]. The most closely related work is Crary et al. [11]. Our type system is based on theirs with the notable exception of our syntactic representation of non-informative upcalls as principal switches. This modification facilitates forming traces to connect the programs with our epistemic logic model of information flow.

In Balliu et al. [5], epistemic logic is also applied to reason about information flow. This work employs a temporal epistemic logic for reasoning about security properties. Using a substructural epistemic logic grants us some of the advantages of a temporal logic as the linear context changes after each trace action corresponding to different temporal states. In Balliu et al. [6], they extend this work by employing an SMT solver along with concrete and symbolic execution to verify the enforcement of the policies. This work also uses traces of actions from the execution of the program to mediate between the program and the logic. Despite these similarities, this work substantially differs from ours in its overall approach. By analyzing programs individually rather than employing a type system to avoid illicit flows to all programs, their work is able to validate the NI of many programs that appear to leak information under most type system based approaches including ours. However, our approach provides a proof that the type system ensures NI or only authorized declassifications so that any program that is well-typed will be safe to execute without further analysis.

Halpern and O’Neill [18] employs the interpreted systems formalism [14] for reasoning about secrecy in multiagent systems whereas we employ a static language-based approach. Secure multi-execution (SME) [12] dynamically enforces IFS. Rather than just monitoring the behavior to prevent insecurities, SME repairs them. In the Dependency Core Calculus (DCC) [2], the monadic type values seals with a security level. Following Crary et al. [11], the monad we employ encapsulates storage effects and specifies bounds on the security levels read and written. Crary et al. [11] encodes DCC dependency analysis into this style of type system.

Sabelfeld and Sands [37] surveys work on declassification and provides dimensions of declassification for analyzing these approaches. SLD does not directly address what information is released in a quantification sense, but it can be encoded in the system by choosing a sufficiently fine stratification of the security levels or by enforcing integrity constraints on declassified assignables. If only part of a value should be declassified, such as the last four digits of a credit card, then this part can be stored in a separate assignable with a less restrictive permission set. Zdancewic and Myers [40] define robust declassification to prevent an attacker from obtaining more information than intended through declassifications. Our approach for encoding what-dimension declassification can address this issue at the cost of dealing with more cumbersome fine-grained security levels or integrity. Control of who releases information is enforced through our protocol that requires authentication certificates to form authorization proofs. We restrict when information is released in the relative sense that it must follow authentication. Our policies do not dictate where information is declassified in either the level locality or code locality sense, but both could be addressed by increasing the expressiveness of the policies.

Montagu et al. [26] defines label algebras to compare the expressiveness of various IF languages with labels. Our approach roughly corresponds to their reader model where each label is a set of principals and each authority is the set of principals that have authenticated. The authorization proofs and declassification policies presented here are simple. More complicated policies are necessary for many applications of authorized declassification. One technique for expressing policies for declassification is presented in Banerjee et al. [7]. Modeling information flow in systems with declassification is addressed in Zdancewic and Myers [40].

Tse and Zdancewic [39] proposes a method for enforcing information flow policies with run-time principals. It provides a flexible method for enforcing policies that depend on data that is only available dynamically. It is unclear how our approach can be adapted to this setting as it relies on statically determining what traces are possible and reasoning about them in the epistemic logic. It would only validate a conservative subset of the safe programs whose policies depend on information only available at run time. Bohannon et al. [10] defines NI in reactive systems such as web browsers and develops a technique for proving NI properties in this setting.

Other approaches support information flow reasoning in existing functional languages. For example, Li and Zdancewic [21], Li and Zdancewic [22], and Russo et al. [35] demonstrate how to reason about information flow in Haskell, and Pottier and Simonet [34] addresses information flow in ML. Our work focuses on a simple monadically structured imperative language, and we designed the type system to explicitly restrict information flow. However, the general techniques are applicable to more robust languages.
Nanevski et al. [30] models information flow properties including NI with dependent types. The type system is expressive enough to state that low outputs must be equal if the low inputs are equal. Other approaches to enforcing security properties using dependent types are given in Morgenstern and Licata [27], which modifies the dependently-typed language Agda [31] for this purpose, and in Jia and Zdancewic [19], which employs the access control language AURA [20]. These approaches employing dependent types are inherently more powerful in their ability to express and enforce policies. If this expressiveness is required, applying our epistemic re-formulation of information flow properties to a dependently-typed language may be an interesting direction for future work.

7. Future Work

The security policies considered in this paper were essentially normal access control lists for the assignables. However, the use of the substructural logic should facilitate enforcing more complicated security policies. These policies would be represented in the logic, and assessing the security of a trace would involve verifying that the relevant policy is satisfied for each disclosure. This initial presentation of our approach avoids this additional complexity.

The authorization proofs we consider are atomic tokens generated dynamically by consulting an authentication database. One motivation for our approach is that it seems conducive to augmenting the authorization policy and representing it in the logic. The transfers of knowledge are represented in the logic so it is natural to also express whether a leak is authorized by the policy if the policy is expressed in the logic. Properly representing these disclosures requires more precise modeling of the specific pieces of knowledge in the logic. Currently all of the knowledge of a principal’s knowledge is modeled by a single abstract predicate as we are interested in proving a NI-like property. However, if the policy distinguishes the disclosure permissions for different pieces of a principal’s knowledge then this distinction must also be represented in the logic, which would require a more fine-grained approach to representing the knowledge exchanges in the trace. The type system would also have to be modified to account for these authorized declassifications.

The focus of this work is confidentiality although section B of the supplementary material briefly addresses integrity as well. Our approach to preserving the integrity of data is the straightforward dual of confidentiality [9], but there are other techniques that are appropriate for more permissive integrity policies. Redesigning the system with the initial goal of enforcing integrity policies could yield an additional modality in the logic besides knowledge that is more appropriate for reasoning about integrity. Some integrity policies permit implicit flows as these are less likely to enable certain classes of attacks such as SQL injection. The type system and traces would need to be modified to account for these differences.

Liu et al. [23] proposes the Fabric system for building secure distributed information systems. Fabric builds on the Jif programming language [29]. Distributed information systems would be an interesting extension of our work. Integrating this work with the ML5 system for distributed systems proposed in Murphy [28] is one possible approach for advancing in this direction.

A. Technical Lemmas

The following technical lemmas are not essential for understanding the development of this paper but may be interesting to the curious reader. The first lemma essentially states that substitution respects the equivalence judgment we defined.

Lemma A.1. (Functionality).

1. If \( \Sigma; \Sigma'; \Gamma \vdash e \equiv e' : A \) and \( \Sigma; \Sigma'; \Gamma, x : A \vdash m \approx_k m' \xrightarrow{x}{\Sigma'} B \otimes \Phi^f, \Phi^o \) then \( \Sigma; \Sigma'; \Gamma \vdash [e/x]m \approx_k [e'/x]m' \xrightarrow{x}{\Sigma'} B \otimes \Phi^f, \Phi^o \)

2. If \( \Sigma; \Sigma'; \Gamma \vdash e \equiv e' : A \) and \( \Sigma; \Sigma'; \Gamma, x : A \vdash e_1 \approx_k e_2 : B \) then \( \Sigma; \Sigma'; \Gamma \vdash [e/x]e_1 \approx_k [e'/x]e_2 : B \)

Proof. The proof is essentially the same as the proof of the corresponding result in Craey et al. [11].

Functionality is used to prove the following lemma, which states that equivalence is preserved under evaluation.

Lemma A.2. (Equivalence under Evaluation).

1. If \( \Sigma; \Sigma'; \vdash m \approx_k m' : A \otimes \Phi^f, \Phi^o \), \( \Sigma; \Sigma'; \vdash \nu \Sigma.(m \mid \mu) \xrightarrow{\nu \Sigma.(\text{ret } v \mid \mu)} \{T\} \), and \( \nu \Sigma.(m \mid \mu) \xrightarrow{\nu \Sigma.(\text{ret } v' \mid \mu)} \{T'\} \) then \( \Sigma; \Sigma'; \vdash v \approx_k v' : A \) and \( \Sigma; \Sigma'; \vdash \nu \Sigma.(m \mid \mu) \xrightarrow{\nu \Sigma.(\text{ret } v \mid \mu)} \{T\} \)

2. If \( \Sigma; \Sigma'; \vdash e \equiv e' : A, e \downarrow v, \) and \( e' \downarrow v' \) then \( \Sigma; \Sigma'; \vdash v \equiv_k v' : A \)

Proof. We give the following interesting case:

1. \( m = x \leftarrow e_1 : m_2 \) and \( m' = x \leftarrow e_1' : m_2' \)

2. \( \Sigma; \Sigma'; \vdash e_1 \equiv_k e_1' : \text{cmd}(m_1) \otimes \Phi^f \), \( \Sigma; \Sigma'; \vdash e_2 : B \otimes m_2 \approx_k m_2' : A \otimes \Phi^f, \Phi^o \), \( \Sigma; \Sigma'; \vdash \text{cmd}(m_1) \downarrow v_1 \)

3. \( e_1 \downarrow \text{cmd}(m_1) \) and \( e_1' \downarrow \text{cmd}(m_1') \)

The induction hypothesis yields \( \text{cmd}(m_1) \approx_k \text{cmd}(m_1') \). This case is interesting when the equivalence is by virtue of the \( \approx_k \) rule rather than the compatibility rule. By inversion, we have \( \text{cmd}(\Phi^f \Phi^o) \)) \text{ cmd}(m_1) \) and \( \text{cmd}(m_1') \). Again by inversion, we have \( \Phi^f \Phi^o \cup \Phi^f \subseteq \Phi^f \) and \( \Phi^f \Phi^o \cup \Phi^f \subseteq \Phi^f \). Therefore, \( \Phi^f \Phi^o \cup \Phi^f \subseteq \Phi^f \). Moreover, as \( \Phi^f \Phi^o \cup \Phi^f \subseteq \Phi^f \Phi^o \cup \Phi^f \subseteq \Phi^f \). The induction hypothesis can be applied to \( \{v_1 / x \} m_2 \) and \( \{v_1 / x \} m_2' \) to complete this case.

The next three lemmas assert properties of the disclosure judgment defined in Definition 3.3. They are all proved using Theorem 4.1.

Lemma A.3. (Disclosure Extension). If \( \Sigma; \vdash m \approx_k A \otimes \Phi^f, \Phi^o \), \( \nu \Sigma.(m \mid \mu) \xrightarrow{\nu \Sigma.(\text{ret } v \mid \mu)} \{T\} \), \( \Sigma; \vdash \text{cmd}(m) \downarrow v \) then \( \Sigma; \vdash \text{cmd}(m) \downarrow v \)

Lemma A.4. (Disclosure Composition). If \( \Sigma; \vdash m \approx_k A \otimes \Phi^f, \Phi^o \), \( \nu \Sigma.(m \mid \mu) \xrightarrow{\nu \Sigma.(\text{ret } v \mid \mu)} \{T\} \), \( \Sigma; \vdash [v \mid x] m \downarrow [v \mid x] m \) then \( \Sigma; \vdash [v \mid x] m \downarrow [v \mid x] m \)

Lemma A.5. (Principal Disclosure). If \( \Sigma; \vdash m \approx_k A \otimes \Phi^f, \Phi^o \), \( \nu \Sigma.(m \mid \mu) \xrightarrow{\nu \Sigma.(\text{ret } v \mid \mu)} \{T\} \), \( \Sigma; \vdash \text{cmd}(m) \downarrow v \) then \( \Sigma; \vdash \text{cmd}(m) \downarrow v \)

B. Integrity

We have focused on confidentiality, but this methodology may also be applied for preserving integrity by modifying the interpretation of a few components. For example, when enforcing confidentiality the set \( \Phi^f \) represented the set of principals permitted to know the
value of the computation. When enforcing integrity, this set represents the set of principals that trust the value of the computation. Similarly, when enforcing confidentiality the set $\Phi^c \supset \Phi$ represents the set of principals to whom the computation may disclose information, but when enforcing integrity this set represents the set of principals whose assignables may be influenced by the computation. Therefore, we still require $\Phi^c \supset \Phi$ as the principals that trust the integrity of an assignable that may be influenced by a computation but we must also trust the integrity of the computation.

Despite these slight differences in semantics, the type system remains unchanged. The only difference is that we use the dual lattice for our relation between principals. If before $k \in \kappa'$ we now have $k' \subseteq k$ instead because rather than protecting the secrets of principal $k'$ from being disclosed to principal $k$, we are now protecting the integrity of the assignables of principal $k'$ from principal $k$. Abstractly, we are still preventing a flow of information from one principal to the other. As a result of this change in the lattice, the upward closed condition on permission sets also changes correspondingly. Now rather than always giving a more privileged principal permission to access an assignable, we always force a lower integrity principal to trust an assignable.

The same non-interference theorem still applies but may now be interpreted through the lens of integrity. The condition that states the final values of the two computations will only differ if there is an assignable with initial values that differ in the two stores and with the executing principal in its permission set now indicates that these final values only differ if an assignable trusted by the executing principal differs in the two initial states. Therefore, if a computation is run in two different stores that only differ in the assignables not trusted by the principal then the result of the computation will be the same. The other condition now states that if the integrity of an assignable is compromised by a computation then there must be a more trusted assignable that had differing values in the initial state. The contrapositive of these two conditions implies that modifying the low integrity inputs will not affect the final values of the high integrity outputs. There are other integrity results that may be more appropriate for particular applications. We discuss one of these in the future work.

### C. Linear Epistemic Logic

The important rules of the linear epistemic logic from DeYoung and Pfenning [13] are presented in Figure 9. The monad, $\{\}_t$, is essential for isolating the application of the semantic effects to a single spine of the derivation. For simplicity, we have omitted polarity annotations in this work, but they are a familiar part of the focusing methodology of Andreoli [3]. The rules are divided into right and left focusing sequents to chain non-invertible rules together as is common in focusing calculi.

### References


