Abstract—Real-world applications routinely make authorization decisions based on dynamic computation. Reasoning about dynamically computed authority is challenging. Integrity of the system might be compromised if attackers can improperly influence the authorizing computation. Confidentiality can also be compromised by authorization, since authorization decisions are often based on sensitive data such as membership lists and passwords. Previous formal models for authorization do not fully address the security implications of permitting trust relationships to change, which limits their ability to reason about authority that derives from dynamic computation. Our goal is a way to construct dynamic authorization mechanisms that do not violate confidentiality or integrity.

We introduce the Flow-Limited Authorization Calculus (FLAC), which is both a simple, expressive model for reasoning about dynamic authorization and also an information flow control language for securely implementing various authorization mechanisms. FLAC combines the insights of two previous models: it extends the Dependency Core Calculus with features made possible by the Flow-Limited Authorization Model. FLAC provides strong end-to-end information security guarantees even for programs that incorporate and implement rich dynamic authorization mechanisms. These guarantees include noninterference and robust declassification, which prevent attackers from influencing information disclosures in unauthorized ways. We prove these security properties formally for all FLAC programs and explore the expressiveness of FLAC with several examples.

I. INTRODUCTION

Authorization mechanisms are critical components in all distributed systems. The policies enforced by these mechanisms constrain what computation may be safely executed, and therefore an expressive policy language is important. Expressive mechanisms for authorization have been an active research area. A variety of approaches have been developed, including authorization logics [1], [2], [3], often implemented with cryptographic mechanisms [4], [5]; role-based access control (RBAC) [6]; and trust management [7], [8], [9].

However, the security guarantees of authorization mechanisms are usually analyzed using formal models that abstract away the computation and communication performed by the system. Developers must take great care to faithfully preserve the (often implicit) assumptions of the model, not only when implementing authorization mechanisms, but also when employing them. Simplifying abstractions can help extract formal security guarantees, but abstractions can also obscure the challenges of implementing and using an abstraction securely. This disconnect between abstraction and implementation can lead to vulnerabilities and covert channels that allow attackers to leak or corrupt information.

A common blind spot in many authorization models is confidentiality. Most models cannot express authorization policies that are confidential or are based on confidential data. Real systems, however, use confidential data for authorization all the time: users on social networks receive access to photos based on friend lists, frequent fliers receive tickets based on credit card purchase histories, and doctors exchange patient data while keeping doctor–patient relationships confidential. While many models can ensure, for instance, that only friends are permitted to access a photo, few can say anything about the secondary goal of preserving the confidentiality of the friend list. Such authorization schemes may fundamentally require some information to be disclosed, but failing to detect these disclosures can lead to unintentional leaks.

Authorization without integrity is meaningless, so formal models are typically better at enforcing integrity. However, many formal models make unreasonable or unintuitive assumptions about integrity. For instance, in many models (e.g., [1], [2], [7]) authorization policies either do not change or change only when modified by a trusted administrator. This is a reasonable assumption in centralized systems where such an administrator will always exist, but in decentralized systems, there may be no single entity that is trusted by all other entities.

Even in centralized systems, administrators must be careful when performing updates based on partially trusted information, since malicious users may try to use the administrator to carry out an attack on their behalf. Unfortunately, existing models offer little help to administrators that need to reason about how attackers may have influenced security-critical update operations.

Developers need a better programming model for implementing expressive dynamic authorization mechanisms. Errors that undermine the security of these mechanisms are common [10], so we want to be able to verify their security. We argue that information flow control is a lightweight, useful tool for building secure authorization mechanisms. Using information flow control is attractive since it offers compositional, end-to-end security guarantees. However, applying information flow control to these mechanisms in a meaningful way requires building on a theory that integrates authority and information security. In this work, we show how to embed such a theory into a programming model, so that dynamic authorization mechanisms—as well as the programs that employ them—can be statically verified.

Approaching the verification of dynamic authorization mechanisms from this perspective is attractive for two reasons.
First, it gives a model for building secure authorization mechanisms by construction rather than verifying them after the fact. This model offers programmers insight into the sometimes subtle interaction between information flow and authorization, and helps programmers address problems early, during the design process. Second, it addresses a core weakness lurking at the heart of existing language-based security schemes: that the underlying policies may change in a way that breaks security. By statically verifying the information security of dynamic authorization mechanisms, we expand the real-world scenarios in which language-based information flow control is useful and strengthen its security guarantees.

We demonstrate that such an embedding is possible by presenting a core language for authorization and information flow control, called the Flow-Limited Authorization Calculus (FLAC). FLAC is inspired by the Polymorphic Dependency Core Calculus [2] (DCC).\(^1\) Abadi develops DCC as an authorization logic, but DCC is limited to static trust relationships defined externally to DCC programs by a lattice of principals. FLAC supports dynamic authorization by building on the Flow-Limited Authorization Model (FLAM) [12], which unifies reasoning about authority, confidentiality, and integrity. Furthermore, FLAC is a language for information flow control. It uses FLAM’s principal model and FLAM’s logical reasoning rules to define an operational model and type system for authorization computations that preserve information security.

The types in a FLAC program can be considered propositions [13] in an authorization logic, and the programs can be considered proofs that the proposition holds. Well-typed FLAC programs are not only proofs of authorization, but also proofs of secure information flow, ensuring the confidentiality and integrity of authorization policies and of the data those policies depend upon.

FLAC is useful from a logical perspective, but also serves as a core programming model for real language implementations. Since FLAC programs can dynamically authorize computation and flows of information, FLAC applies to more realistic settings than previous authorization logics. Thus FLAC offers more than a type system for proving propositions—FLAC programs do useful computation.

This paper makes the following contributions.

- We present two authorization mechanisms implemented in FLAC, commitment schemes and bearer credentials, and demonstrate that FLAC ensures the programs that use these mechanisms preserve the desired confidentiality and integrity properties.

We have organized our discussion of FLAC as follows. Section II introduces commitment schemes and bearer credentials, two examples of dynamic authorization mechanisms we use to explore the features of FLAC. Section III reviews the FLAM principal lattice [12], and Section IV defines the FLAC language and type system. FLAC implementations of the dynamic authorization examples are presented in Section V, and their properties are examined. Section VI explores aspects of FLAC’s proof theory, and Section VII discusses semantic security guarantees of FLAC programs, including noninterference and robust declassification. We explore related work in Section VIII and conclude in Section IX.

II. DYNAMIC AUTHORIZATION MECHANISMS

Dynamic authorization is challenging to implement correctly since authority, confidentiality, and integrity interact in subtle ways. FLAC helps programmers securely implement both authorization mechanisms and code that uses them. FLAC types support the definition of compositional security abstractions, and vulnerabilities in the implementations of these abstractions are caught statically. Further, the guarantees offered by FLAC simplify reasoning about the security properties of these abstractions.

We illustrate the usefulness and expressive power of FLAC using two important security mechanisms: commitment schemes and bearer credentials. We show in Section V that these mechanisms can be implemented using FLAC, and that their security goals are easily verified in the context of FLAC.

A. Commitment schemes

A commitment scheme [14] allows one party to give another a “commitment” to a secret value without revealing the value. The committing party may later reveal the secret in a way that convinces the receiver that the revealed value is the value originally committed.

Commitment schemes provide three essential operations: commit, receive, and open. Suppose \( p \) wants to commit to a value to principal \( q \). First, \( p \) applies \text{commit} to the value and provides the result to \( q \). Next, \( q \) applies \text{receive} to the committed value. Finally, when \( p \) wishes to reveal the value, \( p \) applies the \text{open} operation to the received value, permitting \( q \) to learn it.

A commitment scheme must have several properties in order to be secure. First, \( q \) should not be able to receive a value that hasn’t been committed by \( p \), since this could allow \( q \) to manipulate \( p \) to open a value it had not committed to. Second, \( q \) should not learn any secret of \( p \) that has not been opened by \( p \). Third, \( p \) should not be able to open a different value than the one received by \( q \).

One might wonder why a programmer would bother to create high-level implementations of operations like commit.
receive, and open. Why not simply treat these as primitive operations and give them type signatures so that programs using them can be type-checked with respect to those signatures? The answer is that an error in a type signature could lead to a serious vulnerability. Therefore, we want more assurance that the type signatures are correct. Implementing such operations in FLAC is often easy and ensures that the type signature is consistent with a set of assumptions about existing trust relationships and the information flow context the operations are used within. These FLAC-based implementations serve as language-based models of the security properties achieved by implementations that use cryptography or trusted third parties.

B. Bearer credentials with caveats

A bearer credential is a capability that grants authority to any entity that possesses it. Many authorization mechanisms used in distributed systems employ bearer credentials in some form. Browser cookies that store session tokens are one example: after a website authenticates a user’s identity, it gives the user a token to use in subsequent interactions. Since it is infeasible for attackers to guess the token, the website grants the authority of the user to any requests that include the token.

Bearer credentials create an information security conundrum for authorization mechanisms. Though they efficiently control access to restricted resources, they create vulnerabilities and introduce covert channels when used incorrectly. For example, suppose Alice shares a remotely-hosted photo with her friends by giving them a credential to access the photo. Giving a friend such a credential doesn’t disclose their friendship, but each friend that accesses the photo implicitly discloses the friendship to the hosting service. Such covert channels are pervasive, both in classic distributed authorization mechanisms like SPKI/SDSI [4], as well as in more recent ones like Macaroons [5].

Bearer credentials can also lead to vulnerabilities if they are leaked. If an attacker obtains a credential, it can exploit the authority of the credential. Thus, to limit the authority of a credential, approaches like SPKI/SDSI and Macaroons provide constrained delegation in which a newly issued credential attenuates the authority of an existing one by adding caveats. Caveats require additional properties to hold for the bearer to be granted authority. Session tokens, for example, might have a caveat that restricts the source IP address or encodes an expiration time. As pointed out by Birgisson et al. [5], caveats themselves can introduce covert channels if the properties reveal sensitive information.

FLAC is an effective framework for reasoning about bearer credentials with caveats since it captures the flow of credentials in programs as well as the sensitivity of the information the credentials and caveats derive from. We can reason about credentials and the programs that use them in FLAC with an approach similar to that used for commitment schemes. That we can do so in a straightforward way is somewhat remarkable: prior formalizations of credential mechanisms (e.g., [5], [15], [16]) usually do not consider confidentiality nor provide end-to-end guarantees about credential propagation.

III. The FLAC Principal Lattice

Like many models, FLAC uses principals to represent the authority of all entities relevant to a system. However, FLAC’s principals and their algebraic properties are richer than in most models, so we briefly review the FLAC principal model and notation. Further details are found in the earlier paper [12].

Primitive principals such as Alice, Bob, etc., are represented as elements of a (potentially infinite) set of names $\mathcal{N}$. In addition, FLAC uses $\top$ to represent a universally trusted principal and $\perp$ to represent a universally untrusted principal. The combined authority of two principals, $p$ and $q$, is represented by the conjunction $p \land q$, whereas the authority of either $p$ or $q$ is the disjunction $p \lor q$.

Unlike principals in other models, FLAC principals also represent information flow policies. The confidentiality of principal $p$ is represented by the principal $p^\rightarrow$, called $p$’s confidentiality projection. It denotes the authority necessary to learn anything $p$ can learn. The integrity of principal $p$ is represented by $p^\leftarrow$, called $p$’s integrity projection. It denotes the authority to influence anything $p$ can influence.

All authority may be represented as some combination of confidentiality and integrity. For instance, principal $p$ is equivalent to the conjunction $p^\rightarrow \land p^\leftarrow$, and in fact any FLAC principal can be written $p^\rightarrow \land q^\leftarrow$ for some $p$ and $q$. The closure of the set of names $\mathcal{N}$ plus $\top$ and $\perp$ under the operators $\land, \lor, \leftarrow, \rightarrow$ forms a lattice $\mathcal{L}$ ordered by an acts-for relation $\Rightarrow$, defined by the inference rules in Figure 1. We write operators $\leftarrow, \rightarrow$ with higher precedence than $\land, \lor$; for instance, $p \land q^\leftarrow$ is equal to $p^\rightarrow \land (p \land q)^\leftarrow$. Projections distribute over $\land$ and $\lor$ so, for example, $(p \land q)^\leftarrow = (p^\rightarrow \land q^\leftarrow)$. The confidentiality and integrity authority of principals are disjoint, so the confidentiality projection of an integrity projection is $\perp$ and vice-versa: $(p^\rightarrow)^\leftarrow = \perp = (p^\leftarrow)^\rightarrow$.

An advantage of this model is that secure information flow can be defined in terms of authority. An information flow policy $p$ is at least as restrictive as a policy $q$ if $p$ has at least the confidentiality authority of $q$ and has at least the integrity authority of $q$. This relationship between the confidentiality and integrity of $p$ and $q$ reflects the usual duality seen in information flow control [17]. As in [12], we use the following shorthand for relating principals by policy restrictiveness:

\[
\begin{align*}
& p \subseteq q \triangleq (p^\rightarrow \land q^\leftarrow) \Rightarrow (q^\rightarrow \land p^\leftarrow) \\
& p \sqcup q \triangleq (p \land q)^\leftarrow \Rightarrow (p \lor q)^\rightarrow \\
& p \sqcap q \triangleq (p \lor q)^\rightarrow \Rightarrow (p \land q)^\leftarrow
\end{align*}
\]

Thus, $p \subseteq q$ indicates the direction of secure information flow: from $p$ to $q$. The information flow join $p \sqcup q$ is the

---

2Using $\mathcal{N}$ as the set of all names is convenient in our formal calculs, but a general-purpose language based on FLAC may wish to dynamically allocate names at runtime. Since knowing or using a principal’s name holds no special privilege in FLAC, this presents no fundamental difficulties. To use dynamically allocated principals in type signatures, however, the language’s type system should support types in which principal names may be existentially quantified.

3FLAC defines an additional set of operators called ownership projections, which we omit here to simplify our presentation.
least restrictive principal that both $p$ and $q$ flow to, and the information flow meet $p \cap q$ is the most restrictive principal that flows to both $p$ and $q$.

Finally, in FLAM, the ability to "speak for" another principal is an integrity relationship between principals. This makes sense intuitively, because speaking for another principal acts for another principal as the integrity necessary to speak for that principal. Given a principal expressed in normal form\(^4\) as $q^\rightarrow \wedge r^\rightarrow$, the voice of that principal is

$$\nabla(q^\rightarrow \wedge r^\rightarrow) \triangleq q^\rightarrow \wedge r^\rightarrow$$

For example, the voice of Alice, $\nabla(Alice)$, is Alice\(^-\). The voice of Alice's confidentiality $\nabla(Alice^\rightarrow)$ is also Alice\(^-\).

**IV. FLOW-LIMITED AUTHORIZATION CALCU LUS**

FLAC uses information-flow to reason about the security implications of dynamically computed authority. Like previous information-flow type systems [18], FLAC incorporates types for reasoning about information flow, but FLAC's type system goes further by using Flow-Limited Authorization [12] to ensure that principals cannot use FLAC programs to exceed their authority, or to leak or corrupt information. FLAC is based on DCC [2], but unlike DCC, FLAC supports reasoning about authority deriving from the evaluation of FLAC terms. In contrast, all authority in DCC derives from trust relationships defined by a fixed, external lattice of principals. Thus, using an approach based on DCC in systems where trust relationships change dynamically could introduce vulnerabilities like delegation loopholes, probing and poaching attacks, and authorization side channels [12].

\[^4\]In normal form, a principal is the conjunction of a confidentiality principal and an integrity principal. See [12] for details.

\[^5\]In addition to the derivation label, the rules in [12] also include a query label that represents the confidentiality and integrity of a FLAM query context. The query label is unnecessary in FLAC, and hence omitted here, because we use FLAM judgments only in the type system—these “queries” only occur at compile time and do not make information flows.

\[^6\]The same pc label could also be used to control implicit flows through assignments if FLAC were extended to support mutable references.
and security of control flow. Viewed as an authorization logic,
FLAC’s type system has the unique feature that it expresses
deduction constrained by an information flow context. For
instance, if we have ϕ → ψ then (via APP) we may
derive ψ in a context with integrity p⁺, but not in contexts
that don’t flow to p⁻. This feature offers needed control over
how principals may apply existing facts to derive new facts.

Many FLAC terms are standard, such as pairs (e₁, e₂),
projections proj i e, variants inj i e, polymorphic type abstrac-
tion, Λ X . e, and case expressions. Function abstraction, λ(x : s)[pc].e, includes a pc label that constrains the information
flow context in which the function may be applied. The rule
APP ensures that function application respects these policies,
requiring that the robust FLAM judgment Π; pc ⊢ pc ⊆ pc' holds.
This judgment ensures that the current program counter
label, pc, flows to the function label, pc'..

Branching occurs in case expressions, which conditionally
evaluate one of two expressions. The rule CASE ensures
that both expressions have the same type and thus the same
protection level. The premise Π; pc ⊢ pc ≤ s ensures that this
type protects the current pc label.⁷

Like DCC, FLAC uses monadic operators to track depen-
dencies. The monadic unit term (η₁ v) (UNITM) says that a
value v of type s is protected at level ℓ. This protected value
has the type ℓ says s, meaning that it has the confidentiality
and integrity of principal ℓ. Computation on protected values
must occur in a protected context (“in the monad”), expressed
using a monadic bind term. The typing rule BINDM ensures
that the result of the computation protects the confidentiality
and integrity of protected values. For instance, the expression
bind x = (η₁ v) (η₁ x) is only well-typed if ℓ' protects
values with confidentiality and integrity ℓ. Since case expres-
sions may use the variable x for branching, BINDM raises the
pc label to pc ∪ ℓ to conservatively reflect the control-flow
dependency.

⁷This premise simplifies our proofs, but does not appear to be strictly
necessary; BINDM ensures the same property.

![Fig. 4: FLAC operational semantics](image)

![Fig. 5: FLAC type system](image)

Protection levels are defined by the set of inference rules
in Figure 7, adapted from [22]. Expressions with unit type
(P-UNIT) do not propagate any information, so they protect
information at any ℓ. Product types protect information at ℓ if
both components do (P-PAIR). Function types protect informa-
tion at ℓ if the return type does (P-FUN), and polymorphic
types protect information at whatever level the abstracted type
does (P-TFUN). If a type s already protects information at ℓ,
then ℓ' says s still does (P-LBL1). Finally, if ℓ flows to ℓ',

Table:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Premise</th>
<th>Conclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Π; Γ; e ⊢ e⁺</td>
<td></td>
<td>Π; Γ; e⁺ ⊢ e⁺</td>
</tr>
<tr>
<td>Π; Γ; e ⊢ e⁺</td>
<td></td>
<td>Π; Γ; e⁺ ⊢ e⁺</td>
</tr>
<tr>
<td>Π; Γ; e ⊢ e⁺</td>
<td></td>
<td>Π; Γ; e⁺ ⊢ e⁺</td>
</tr>
<tr>
<td>Π; Γ; e ⊢ e⁺</td>
<td></td>
<td>Π; Γ; e⁺ ⊢ e⁺</td>
</tr>
</tbody>
</table>

Diagram:

![Diagram](image)
This is secure since ensure the integrity of dynamic authorization computations secrets or corrupt data. The premises of the A could use delegation values to create new flows that reveal evidence for authorization would be insecure since attackers.

The difference is that the assumption terms evaluate to evidence securely to read " assumes a trust relationship that allows delegation context. In this case, the expression says that principal whose security is affected. For instance, to make the assumption p q, the evidence represented by the term e must have at least the integrity of the voice of q, written ∇(q). Since the pc bounds the restrictiveness of the dependencies of e, this ensures that only information with integrity ∇(q) or higher may influence the evaluation of e. The third premise, requires that the principal p has sufficient integrity to be trusted to enforce q’s confidentiality, q→. This premise means that q permits data to be relabeled from q→ to p→.

Assumption terms evaluate to where expressions (rule E-ASSUME). To simplify the formalization, these expressions are not part of the source language but are generated by the evaluation rules. The term e where v records that e is evaluated in a context which includes the delegation v. The rule WHERE gives a typing rule for where terms; though similar to ASSUME, it requires only that there exist a sufficiently trusted label pc’ such that subexpression e type-checks. In the proofs in Section VII, we choose pc’ using the typing judgment of the source-level assume that generates the where term.

V. EXAMPLES REVISITED

We can now implement our examples from Section II in FLAC. Using FLAC ensures that authority and information flow assumptions are explicit, and that programs using these abstractions are secure with respect to those assumptions. In this section, we discuss at a high level how FLAC types help enforce specific end-to-end security properties for commitment schemes and bearer credentials. Section VII formalizes the semantic security properties of all well-typed FLAC programs.

A. Commitment Schemes

Figure 8 contains the essential operations of a one-round commitment scheme—commit, receive, and open—

P-UNIT

P-PAIR

P-FUN

P-TFUN

P-LBL1

P-LBL2

Fig. 6: Inference rules for robust assumption, adapted from FLAM [12].
implemented in FLAC. Typically, a principal $p$ commits to a value and sends it to $q$, who receives it. Later, $p$ opens the value, revealing it to $q$. The commit operation takes a value of any type (hence $\forall X$) with confidentiality $p^\leftarrow$ and produces a value with confidentiality and integrity $p$. In other words, $p$ endorses [23] the value to have integrity $p^\rightarrow$.

Attackers should not be able to influence whether principal $p$ commits to a particular value. The $pc$ constraint on commit ensures that only principal $p$ and principals trusted with at least $p$'s integrity, $p^\rightarrow$, may apply commit to a value. Furthermore, if the programmer omitted this constraint or instead chose $\bot^\leftarrow$, say, then commit would be rejected by the type system. Specifically, the assume term would not type-check via rule ASSUME since the pc does not act for $\nabla(p^\leftarrow) = p^\rightarrow$.

Next, principal $q$ accepts a committed value from $p$ using the receive operation. The receive operation endorses the value with $q$'s integrity, resulting in a value at $p \land q^\leftarrow$, the confidentiality of $p$ and the integrity of both $p$ and $q$.

As with the commit operation, FLAC ensures that receive satisfies important information security properties. Other principals, including $p$, should not be able to influence which values $q$ receives—otherwise an attacker could use receive to subvert $q$’s integrity, using it to endorse arbitrary values. The $pc$ constraint on receive ensures in this case that only $q$ may apply receive. Furthermore, the type of $x$ requires received values to have the integrity of $p$. Errors in either of these constraints would result in a typing error, either due to ASSUME as before, or due to BINDM, which requires that $p$ must flow to $p \land q^\leftarrow$.

Additionally, receive accepts committed values with confidentiality at most $p^\rightarrow$. This constraint ensures that $q$ does not receive values from $p$ that might depend on $q$’s secrets: unopened commitments, for example. In cryptographic protocols, this property is usually called non-malleability [25], and is important for scenarios in which security depends on the independence of values. Consider a sealed-bid auction where participants submit their bids via commitment protocols. Suppose that $q$ commits a bid $b$, protected by label $q$. Then $p$ could theoretically influence a computation that computes a value $b + 1$ with label $p \land q^\rightarrow$ since that label protects information at $q^\leftarrow$, but only has $p^\rightarrow$ integrity. If $q$ received values from $p$ that could depend on $q$’s secrets, then $p$ could outbid $q$ by 1 without ever learning the value $b$.

Finally, open reveals a committed value to $q$ by relabeling a value from $p \land q^\leftarrow$ to $p^\rightarrow \land q$, which is readable by principal $q$ but retains the integrity of both $p$ and $q$. Since open accepts a value protected by the integrity of both $p$ and $q$ and returns a value with the same integrity, the opened value must have been previously committed by $p$ and received by $q$. Since the open operation reveals a value with confidentiality $p^\rightarrow$, it should only be invoked by principals that are trusted to speak for $p^\leftarrow$. Otherwise, $q$ could open $p$’s commitments. Hence, the pc label of open is $\nabla(p^\rightarrow)$. For $p = Alice$, say, the pc label would be Alice$^\leftarrow$. FLAC ensures these constraints are specified correctly; otherwise, open’s implementation could not produce a value with label $p^\rightarrow \land q$.

The implementation requires two assume terms. The outer term establishes that principals speaking for $q^\leftarrow$ also speak for $p^\rightarrow$ by creating an integrity relationship between their voices. With this relationship in place, the inner term may reveal the commitment to $q$.

In DCC, functions are not annotated with pc labels and may be applied in any context. So a DCC function analogous to open might have type

$$
dcc\text{-open} : \forall X. p \land q^\leftarrow \rightarrow p^\rightarrow \land q \rightarrow X
$$

However, dcc\text{-open} would not be appropriate for a commitment scheme since any principal could use it to relabel information from $p$-confidential ($p^\rightarrow$) to $q$-confidential ($q^\leftarrow$).

To simplify the presentation of our commitment scheme operations, we make the assumption that $q$ only receives one value. Therefore, $p$ can only open one value, since only one value has been given the integrity of both $p$ and $q$. A more general scheme can be achieved by pairing each committed value with a public identifier that is endorsed along with the value, but remains public. If $q$ refuses to receive more that one commitment with the same identifier$^{12}$, $p$ will be unable to open two commitments with the same value since it cannot create a pair that has the integrity of both $p$ and $q$, even if $p$ has multiple committed values (with different identifiers) to choose from. We present the simpler one-round

$^{10}$We make the reasonable assumption that an untrusted programmer cannot modify high-integrity code, thus the influence of attackers is captured by the pc and the protection levels of values. Enforcing this assumption is beyond the scope of FLAC, but has been explored in [24].

$^{11}$i.e., it satisfies the ASSUME premise $\Pi; pc \parallel \nabla(p^\leftarrow) = \nabla(q^\leftarrow)$.

$^{12}$For cryptographic commitment schemes, the commitment ciphertext itself could act as a public identifier, and $q$ could rely on cryptographic assumptions that distinct values cannot (with high probability) have the same identifier instead of explicitly checking whether the identifier has been used before.
commitment scheme above since it captures the essential information security properties of commitment while avoiding the tedious digression of defining encodings for numeric values and numeric comparisons.

The real power of FLAC is that the security guarantees of well-typed FLAC functions like those above are compositional. The FLAC type system ensures the security of both the functions themselves and the programs that use them. For instance, the code should be rejected because it would permit q to open p’s commitments:

\[ \Lambda X. \lambda (x: p \land q^\leftarrow) \text{ says } X \right] (q^\leftarrow). \text{ assume } (q \Rightarrow p) \text{ in open } x \]

FLAC’s guarantees make it possible to state general security properties of all programs that use the above commitment scheme, even if those programs are malicious. For example, suppose we have \( p_c p = \forall (q), p_c q = \forall (q) \), and

\[ \Gamma_{cro} = \text{commit, receive, open, } x: p^\rightarrow \text{ says } s, y: p \land q^\leftarrow \text{ says } s \]

Intuitively, \( p_c p \) and \( p_c q \) are execution contexts under the control of \( p \) or \( q \), respectively. \( \Gamma_{cro} \) is a typing context for programs using the commitment scheme.\(^{13}\) The variable \( x \) represents an uncommitted value with \( p \)’s confidentiality, whereas \( y \) is a committed value. Since we are interested in properties that hold for all principals \( p \) and \( q \), we want the properties to hold in an empty delegation context: \( \Pi = \emptyset \).

Below, we omit the delegation context altogether for brevity.

Using results presented in Section VII, we can prove that:

- **q cannot receive a value that hasn’t been committed.**
  For any \( e \) and \( s’ \) such that \( \Gamma_{cro}: p_c e \vdash e : p \land q^\leftarrow \text{ says } s’ \), the value that \( e \) computes is independent of \( x \).

- **q cannot learn a value that hasn’t been opened.**
  For any \( e, \ell \), and \( s’ \) such that \( \Gamma_{cro}: p_c e \vdash e : \ell \land q^\leftarrow \text{ says } s’ \), the value that \( e \) computes is independent of \( x \) and \( y \).

- **p cannot open a value that hasn’t been received.**
  For any \( e \) such that \( \Gamma_{cro}: p_c e \vdash e : p^\rightarrow \land q \text{ says } s’ \), the value that \( e \) computes is independent of \( x \).

For the first two properties, we consider programs using our commitment scheme that \( q \) might invoke, hence we consider FLAC programs that type-check in the \( \Gamma_{cro}: p_c e \) context. In the first property, we are concerned with programs that produce values protected by policy \( p \land q^\leftarrow \). Since such programs produce values with the integrity of \( p \) but are invoked by \( q \), we want to ensure that no program exists that enables \( q \) to obtain a value with \( p \)’s integrity that depends on \( x \), which is a value without \( p \)’s integrity. The second property concerns programs that produces values at \( \ell \land q^\leftarrow \) for any \( \ell \}; these values are readable by \( q \). Therefore, we want to ensure that no program exists that enables \( q \) to produce such a value that depends on \( x \) or \( y \), which are not readable by \( q \).

The final property considers programs that \( p \) might invoke to produce values at \( p^\rightarrow \land q \), thus we consider FLAC programs that type-check in the \( \Gamma_{cro}: p_c p \) context. Here, we want to ensure that no program invoked by \( p \) can produce a value at \( p^\rightarrow \land q \) that depends on \( x \), an unreceived value. Complete proofs of these properties are found in Appendix B.

### B. Bearer Credentials

We can also use FLAC to implement bearer credentials, our second example of a dynamic authorization mechanism. We represent a bearer credential with authority \( k \) in FLAC as a term with the type

\[ \forall X. k^\rightarrow \text{ says } X \vdash k \vdash k^\rightarrow \text{ says } X \]

which we abbreviate as \( k \vdash k^\rightarrow \). These terms act as bearer credentials for a principal \( k \) since they may be used as a proxy for \( k \)’s confidentiality and integrity authority. Recall that \( k^\rightarrow = k^\rightarrow \land \bot^\rightarrow \) and \( k^\rightarrow = k^\rightarrow \land \bot^\rightarrow \). Then secrets protected by \( k^\rightarrow \) can be declassified to \( \bot^\rightarrow \), and untrusted data protected by \( \bot^\rightarrow \) can be endorsed to \( k^\rightarrow \). Thus this term yields the full authority of \( k \), and if \( pc = \bot \), the credential may be used in any context—any “bearer” may use it. From such credentials, more restricted credentials can be derived. For example, the credential \( k \vdash k^\rightarrow \vdash \bot^\rightarrow \) grants the bearer authority to declassify \( k \)-confidential values, but no authority to endorse values.

We postpone an in-depth discussion of terms with types of the form \( k^\rightarrow \vdash k^\rightarrow \) until Section VI-B, but it is interesting to note that an analogous term in DCC is only well-typed if \( k \) is equivalent to \( \bot \). This is because the function takes an argument with \( k \)’s confidentiality and no integrity, and produces a value with \( k \)’s integrity and no confidentiality. Suppose \( L \) is a security lattice used to type-check DCC programs with suitable encodings for \( k \)’s confidentiality and integrity. If a DCC term has a type analogous to \( k \Rightarrow k^\rightarrow \), then \( L \) must have the property \( k^\rightarrow \subseteq \bot \Rightarrow k^\rightarrow \). This means that \( k \) has no confidentiality and no integrity. That FLAC terms may have this type for any principal \( k \) makes it straightforward to implement bearer credentials and demonstrates a useful application of FLAC’s extra expressiveness.

The \( pc \) of a credential \( k^\rightarrow \vdash k^\rightarrow \vdash k \) acts as a sort of caveat: it restricts the information flow context in which the credential may be used. We can add more general caveats to credentials by wrapping them in lambda terms. To add a caveat \( \phi \) to a credential with type \( k \vdash k^\rightarrow \vdash k \), we use a wrapper:

\[ \lambda (x: k \vdash k^\rightarrow \vdash k). X. \lambda (y: \phi). [pc, \Lambda X. \lambda (y: \phi). [pc, X] X \]

which gives us a term with type

\[ \forall X. \phi \vdash k \vdash k^\rightarrow \vdash X \vdash k \vdash k^\rightarrow \vdash X \]

This requires a term with type \( \phi \) (in which \( X \) may occur) to be applied before the authority of \( k \) can be used. Similar wrappers allow us to chain multiple caveats; i.e., for caveats \( \phi_1 \ldots \phi_n \), we obtain the type

\[ \forall X. \phi_1 \ldots \phi_n \vdash \ldots \phi_n \vdash k \vdash X \vdash k \vdash k \]

which abbreviates to

\[ k \vdash \phi_1 \times \ldots \times \phi_n \vdash k \]

\(^{13}\)For presentation purposes, we have omitted the types of commit, receive, and open in \( \Gamma_{cro} \). Their types are as defined previously.
Like any other FLAC terms, credentials may be protected by flow information policies. So a credential that should only be accessible to Alice might be protected by the type \( \text{Alice} \rightarrow \text{RomCom} \) (\( k \overset{\phi, \text{Alice}}{\rightarrow} k' \)). This confidentiality policy ensures the credential cannot accidentally be leaked to an attacker. A further step might be to constrain uses of this credential so that only Alice may invoke it to relabel information. If we require \( \text{pc} = \text{Alice} \rightarrow \text{RomCom} \), this credential may only be used in contexts trusted by Alice: \( \text{Alice} \rightarrow \text{RomCom} \) (\( k \overset{\phi, \text{Alice}}{\rightarrow} k' \)).

A subtle point about the way in which we construct caveats is that the caveats are polymorphic with respect to \( k \). This means that each caveat may constrain what types \( X \) may be instantiated with. For instance, suppose \( \text{isEduc} \) is a predicate for educational films; it holds (has a proof term with type \( \text{isEduc} X \)) for types like \( \text{Bio} \) and \( \text{Doc} \), but not \( \text{RomCom} \). Adding \( \text{isEduc} X \) as a caveat to a credential would mean that the bearer of the credential could use it to access biographies and documentaries, but could not use it to access romantic comedies. Since no term of type \( \text{isEduc} \text{RomCom} \) could be applied, the bearer could only satisfy \( \text{isEduc} X \) by instantiating \( X \) with \( \text{Bio} \) or \( \text{Doc} \). Once \( X \) is instantiated with \( \text{Bio} \) or \( \text{Doc} \), the credential cannot be used on a \( \text{RomCom} \) value. Thus we have two mechanisms for constraining the use of credentials: information flow policies to constrain propagation, and caveats to establish prerequisites and constrain the types of data covered by the credential.

As a more in-depth example of using such credentials, suppose Alice hosts a file sharing service. For a simpler presentation, we use free variables to refer to these files; for instance, \( x_1 : (k_1 \text{ says ph}) \) is a variable that stores a photo (type \( \text{ph} \)) protected by \( k_1 \). For each such variable \( x_1 \), Alice has a credential \( k_1 \overset{\text{Alice}}{\rightarrow} k_1' \), and can give access to users by providing this credential or deriving a more restricted one. To access \( x_1 \), Bob does not need the full authority of Alice or \( k_1 \)—a more restricted credential suffices:

\[
\lambda(c : k_1 \overset{\text{Alice}}{\rightarrow} k_1') \text{Bob} \rightarrow \wedge k_1' \text{ph} \). \\
\text{bind } x'_1 = c ~ x_1 \text{ in } (\eta_{\text{Bob} \rightarrow \wedge k_1'} x'_1)
\]

Here, \( c \) is a credential \( k_1 \overset{\text{Bob}}{\rightarrow} \text{Bob} \rightarrow \wedge k_1' \text{ph} \) whose polymorphic type has been instantiated with the photo type \( \text{ph} \). This credential accepts a photo protected at \( k_1 \) and returns a photo protected at \( \text{Bob} \rightarrow \wedge k_1' \), which Bob is permitted to access.

The advantage of bearer credentials is that access to \( x_1 \) can be provided to principals other than \( k_1 \) in a decentralized way, without changing the policy on \( x_1 \). For instance, suppose Alice wants to issue a credential to Bob to access resources protected by \( k_1 \). Alice has a credential with type \( k_1 \overset{\text{Alice}}{\rightarrow} k_1' \), but she wants to ensure that only Bob (or principals Bob trusts) can use it. In other words, she wants to create a credential of type \( k_1 \overset{\text{Bob}}{\rightarrow} k_1' \), which needs Bob’s integrity to use.

Alice can create such a credential using a wrapper that derives a more constrained credential from her original one.

\[
\lambda(c : k_1 \overset{\text{Alice}}{\rightarrow} k_1')[\text{Alice}]. \\
\text{bind } x'_1 = c ~ x_1 \text{ in } (\eta_{\text{Bob} \rightarrow \wedge k_1'} x'_1)
\]

Then Bob can use this credential to access \( x_1 \) by deriving a credential of type \( k_1 \overset{\text{Bob}}{\rightarrow} \text{Bob} \rightarrow \wedge k_1' \text{ph} \) using the function

\[
\lambda(c : k_1 \overset{\text{Bob}}{\rightarrow} k_1')[\text{Bob}]. \\
\text{bind } y' = c ~ \text{ph} ~ y \text{ in } (\eta_{\text{Bob} \rightarrow \wedge k_1'} y')
\]

which can be applied to obtain a value readable by Bob. Bob can also use this credential to share photos with friends. For instance, the function

\[
\lambda(c : k_1 \overset{\text{Bob}}{\rightarrow} k_1')[\text{Bob}]. \\
\text{assume } (\text{Carol} \rightarrow \text{Bob}) \text{ in } \\
\text{bind } x'_1 = c ~ \text{ph} ~ x_1 \text{ in } (\eta_{\text{Carol} \rightarrow \wedge k_1'} x'_1)
\]

creates a wrapper around a specific photo \( x_1 \). Only principals trusted by Carol may invoke the wrapper, which produces a value of type \( \text{Carol} \rightarrow \wedge k_1' \text{ph} \), permitting Carol to access the photo.

The properties of FLAC let us prove many general properties about such bearer-credential programs; here, we examine three properties. For \( i \in \{1..n\} \), let

\[
\text{bind } x_i = k_i \text{ says } s_i, c_i : \text{Alice says } (k_i \overset{\text{Alice}}{\rightarrow} k_i')
\]

where \( k_i \) is a primitive principal protecting the \( i \)th resource of type \( s_i \), and \( c_i \) is a credential for the \( i \)th resource and protected by Alice. Assume \( k_i \notin \{\text{Alice, Friends, p}\} \) for all \( i \) where \( p \) represents a (potentially malicious) user of Alice’s service, and \( \text{Friends} \) is a principal for Alice’s friends, (e.g., \( \text{Friends} = (\text{Bob} \wedge \text{Carol}) \)). Also, define \( \text{pc}_p = p \rightarrow \text{Bob} \wedge \text{pc}_A = \text{Alice} \rightarrow \text{Bob} \).

- \( p \) cannot access resources without a credential. For any \( e, \ell \), and \( s' \) such that \( \Gamma_{bc} : p_c : (k_i \overset{\text{Bob}}{\rightarrow} k_i') \); \( \text{pc}_p : e : \ell \cap p \rightarrow \text{says } s' \), the value of \( e \) is independent of \( x_i \) for all \( i \).
- \( p \) cannot use unrelated credentials to access resources. For any \( e, \ell \), and \( s' \) such that

\[
\Gamma_{bc} : p_c : (k_i \overset{\text{Bob}}{\rightarrow} k_i') ; \text{pc}_p : e : \ell \cap p \rightarrow \text{says } s' \]

the value \( e \) computes is independent of \( x_i \) for \( i \neq 1 \).
- Alice cannot disclose secrets by issuing credentials. For all \( i \) and \( j \neq 1 \), define

\[
\Gamma'_{bc} = x_i : k_i \text{ says } s_i, c_i : \text{Alice says } (k_i \overset{\text{Alice}}{\rightarrow} k_i'), \\
c_p : \text{Friends says } (k_j \overset{\text{Alice}}{\rightarrow} k_j')
\]

Then if \( \Gamma'_{bc} : p_c : e : \ell \cap p \rightarrow \text{says } (k_j \overset{\text{Alice}}{\rightarrow} k_j') \) for some \( e, \ell \), and \( s' \), the value of \( e \) is independent of \( x_i \).

These properties demonstrate the power of FLAC’s type system. The first two ensure that credentials really are necessary.
for \( p \) to access protected resources, even indirectly. In the first, \( p \) has no credentials, and the type system ensures that
\( p \) cannot invoke a program that produces a value \( p \) can read
(represented by \( \ell \mapsto p \)) that depends on any variable \( x_i \). In the
second, a credential \( c_p \) with type \( k_i \xrightarrow{\rho} k_i \) is accessible to \( p \), but \( p \) cannot use it to access other variables. The third
property eliminates covert channels like the one discussed in
Section II-B. It implies that credentials issued by Alice do
not leak information, in this case about Alice’s friends. By
implementing bearer credentials in FLAC, we can demonstrate
these three properties with relatively little effort.

VI. FLAC PROOF THEORY

A. Properties of says

FLAC’s type system constrains how principals apply ex-
isting facts to derive new facts. For instance, a property of
says in other authorization logics (e.g., Lampson et al. [1]
and Abadi [2]) is that implications that hold for top-level
expressions also hold for propositions of any principal \( \ell \):

\[ \vdash (s_1 \xrightarrow{\rho} s_2) \rightarrow (\ell \text{ says } s_1 \rightarrow \ell \text{ says } s_2) \]

The \( \rho \) annotations on FLAC function types refine this property. Each implication (in other words, each function) in FLAC
is annotated with an upper bound on the information flow
cost it may be invoked within. To lift such an implication to operate on propositions protected at label \( \ell \), the label \( \ell \) must flow to the \( \rho \) of the implication. Thus, for all \( \ell \) and \( s_i \),

\[ \vdash (s_1 \xrightarrow{\rho \downarrow \ell} s_2) \xrightarrow{\rho} (\ell \text{ says } s_1 \xrightarrow{\rho} \ell \text{ says } s_2) \]

This judgment is a FLAC typing judgment in logical form,
where terms have been omitted. We write such judgments with
an empty typing context (as above) when the judgment is valid
for any \( \Pi, \Gamma \), and \( \rho \). A judgment in logical form is valid if a
proof term exists for the specified type, proving the type is
inhabited. The above type has proof term

\[ \lambda(f: (s_1 \xrightarrow{\rho \downarrow \ell} s_2))[[\rho]]. \]

\[ \lambda(x: \ell \text{ says } s_1)[[\rho]]. \text{bind } x' = x \text{ in } (\eta_\ell f x') \]

In order to apply \( f \), we must first \text{bind } x \text{, so according to}
rules \text{BINDM and APP, the function } f \text{ must have a label at}
least as restrictive as } \rho \sqcup \ell. \text{ All theorems of DCC can be}
obtained by encoding them as FLAC implications with \( \rho = \top \rightarrow \), the highest bound. Since any principal \( \ell \) flows to \( \top \rightarrow \),
such implications may be applied in any context.

These refinements of DCC’s theorems are crucial for sup-
porting applications like commitment schemes and bearer
credentials. Recall from Sections V-A and V-B that the security
of these mechanisms relied in part on restricting the \( \rho \)
to a specific principal’s integrity. Without such refinements,
principal \( q \) could open principal \( p \)’s commitments using \text{open},
or create credentials with \( p \) authority: \( p \mapsto \xrightarrow{\rho} p \).

Other properties of \text{says} common to DCC and other logics
(cf. [26] for examples) are similarly refined by \( \rho \) bounds.

Two examples are: \( \vdash s \xrightarrow{\rho} \ell \text{ says } s \) which has proof term:

\[ \lambda(x: s)[[\rho]]. (\eta_\ell s) \]

\[ \vdash \ell \text{ says } (s_1 \xrightarrow{\rho \downarrow \ell} s_2) \xrightarrow{\rho} (\ell \text{ says } s_1 \xrightarrow{\rho} \ell \text{ says } s_2) \]

with proof term:

\[ \lambda(f: \ell \text{ says } (s_1 \xrightarrow{\rho \downarrow \ell} s_2))[[\rho]]. \text{bind } x' = x \text{ in } \]

\[ \lambda(y: \ell \text{ says } s_1)[[\rho]]. \text{bind } y' = y \text{ in } (\eta_\ell x' y') \]

As in DCC, chains of \text{says} are commutative in FLAC:

\[ \vdash \ell_1 \text{ says } \ell_2 \text{ says } s \xrightarrow{\rho} \ell_2 \text{ says } \ell_1 \text{ says } s \]

with proof term

\[ \lambda(x: \ell_1 \text{ says } \ell_2 \text{ says } s)[[\rho]]. \]

\[ \text{bind } y = x \text{ in } \text{bind } z = y \text{ in } (\eta_{\ell_2} (\eta_\ell_z)) \]

In some logics with different interpretations of \text{says} (e.g.,
CDC [27]) differently ordered chains are distinct, but here we
find commutativity appealing since it matches the intuition
from information flow control. When principal \( \ell_1 \) says that \( \ell_2 \)
says \( s \), we should protect \( s \) with a policy at least as restrictive
as both \( \ell_1 \) and \( \ell_2 \), i.e., the principal \( \ell_1 \sqcup \ell_2 \). Since \( \sqcup \) is
commutative, who said what first is irrelevant.

B. Dynamic Hand-off

Many authorization logics support delegation using a “hand-
off” axiom. In DCC, this axiom is actually a provable theorem:

\[ \vdash (q \text{ says } (p \Rightarrow q)) \rightarrow (p \Rightarrow q) \]

where \( p \Rightarrow q \) is shorthand for

\[ \forall X. (p \text{ says } X \Rightarrow q \text{ says } X) \]

However, \( p \Rightarrow q \) is only inhabited if \( p \sqsubseteq q \) in the security
lattice. Thus, DCC can reason about the consequences of \( p \sqsubseteq q \)
(whether it is true for the lattice or not), but a DCC program
cannot produce a term of type \( p \Rightarrow q \) unless \( p \sqsubseteq q \).

FLAC programs, on the other hand, can create new trust
relationships from delegation expressions using assume terms.
The type analogous to \( p \Rightarrow q \) in FLAC is

\[ \forall X. (p \text{ says } X \xrightarrow{\rho} q \text{ says } X) \]

which we wrote as \( p \xrightarrow{\rho} q \) in Section V-B. FLAC programs
construct terms of this type from proofs of authority, repre-
sed by terms with acts-for types. This feature enables a
more general form of hand-off, which we state formally below.

**Proposition 1** (Dynamic hand-off). For all \( \ell \) and \( \rho \), let \( pc = \ell \rightarrow \land (p \rightarrow ) \land q \rightarrow \)

\[(\nabla(q \rightarrow) \equiv \nabla(p \rightarrow)) \xrightarrow{\rho} (p \sqsubseteq q) \xrightarrow{\rho} \]

\[ \forall X. (p \text{ says } X \xrightarrow{\rho} q \text{ says } X) \]
Proof term.

\[ \lambda (p : \text{assume}(q : (p \sqsubseteq q))[\text{pc}]) \]
\[ \lambda (p : (p \sqsubseteq q))[\text{pc}] \]

\text{assume} \ p \text{ in assume} \ p \text{ bind} \ x' = x \in (\eta_q \ x') \]

The principal \( p \) is the integrity of both \( p \) and \( q \). The two assumptions are proofs of authority with acts-for types: a proof of \( \bigwedge (\eta_q \ x') \) and a proof of \( p \sqsubseteq q \). The principal \( p \) ensures that the proofs have sufficient integrity to be used in assume terms since it has the integrity of both \( p \) and \( q \). Note that low-integrity or confidential delegation values must first be bound before the above term may be applied. Thus the principal would reflect the protection level of both assumptions. Principals \( \ell \) and \( p \) are unconstrained.

Dynamic hand-off terms give FLAC programs a level of expressiveness and security not offered by other authorization logics. Observe that \( p \) may be chosen independently of the other principals. This means that although the principal \( p \) prevents low-integrity principals from creating hand-off terms, a high-integrity principal may create a hand-off term and provide it to an arbitrary principal. The principal \( p \) in FLAC, then, are similar to capabilities since even untrusted principals may use them to change the protection level of values. Unlike in most capability systems, however, the propagation of hand-off terms can be constrained using information flow policies.

Terms that have types of the form in Proposition 1 illustrate a subtlety of enforcing information flow in an authorization mechanism. Because these terms relabel information from one protection level to another protection level, the transformed information implicitly depends on the proofs of authorization. FLAC ensures that the information security of these proofs is protected—like that of all other values—even as the policies of other information are being modified. Hence, authorization proofs cannot be used as a side channel to leak information.

VII. Semantic Security Properties of FLAC

A. Delegation Invariance

FLAC programs dynamically extend trust relationships, enabling new flows of information. Nevertheless, well-typed programs have end-to-end semantic properties that enforce strong information security. These properties derive primarily from FLAC’s control of the delegation context. The A\text{ssume} rule ensures that only high-integrity proofs of authorization can extend the delegation context, and furthermore that such extensions occur only in high-integrity contexts.

That low-integrity contexts cannot extend the delegation context turns out to be a crucial property. This property allows us to state a useful invariant about the evaluation of FLAC programs. Recall that assume terms evaluate to \text{where} terms in the FLAC semantics. Thus, FLAC programs typically compute values containing a hierarchy of nested \text{where} terms. The terms record the values whose types were used to extend the delegation context during type checking.

For a well-typed FLAC program, we can prove that certain trust relationships could not have been added by the program. Therefore, if these relationships exist, they must have existed in the original delegation context.

Lemma 1 (Delegation invariance). Suppose \( \Pi; \Gamma; p \vdash e : s \) such that \( e \rightarrow e' \) \text{where} \( v \). Then for some \( \ell, p', q', \) and \( \Pi' \), we have \( \Pi; \Gamma; p \vdash v : \ell \) \text{says} \( p' \sqsubseteq q' \) and \( \Pi'; \Gamma; p \vdash e' : s \). Furthermore, for all \( p \) and \( q \) such that \( p \sqsubseteq q \), \( q \) has a useful invariant.

Proof. See Appendix A.

First, Lemma 1 says that at each step of evaluation, there exists a \( \Pi' \) such that \( e' \) is well-typed. Moreover, this \( \Pi' \) has a useful invariant. If \( p \) does not speak for a principal \( q \), then \( \Pi \) and \( \Pi' \) must agree on the trust relationships of \( q \).

B. Noninterference

Lemma 1 is critical for our proof of noninterference, a result that states that public and trusted outputs of a program cannot depend on restricted (secret or untrustworthy) information. Our proof of noninterference for FLAC programs relies on a proof of subject reduction under a bracketed semantics, based on the proof technique of Pottier and Simonet [20]. This technique is relatively standard, so we omit it here. The complete proof of subject reduction is in our technical report [28]; proofs for other results are found in Appendix A.

In other noninterference results based on bracketed semantics, including [20], noninterference follows almost directly from the proof of subject reduction. This is because the subject reduction proof shows that evaluating a term cannot change its type. In FLAC, however, subject reduction alone is insufficient; evaluation may enable flows from secret or untrusted inputs to public and trusted types.

To see how, suppose \( e \) is a well-typed program according to \( \Pi; \Gamma; x : s; p \vdash e : s' \). Furthermore, let \( H \) be a principal such that \( \Pi; p \vdash H \leq s \) and \( \Pi; p \not\vdash H \leq s' \). In other words, \( x \) is a “high” variable (more restrictive; secret and untrusted), and \( e \) evaluates to a “low” result (less restrictive; public and trusted). In [20], executions that differ only in secret or untrusted inputs must evaluate to the same value, since otherwise the value would not be well typed. In FLAC, however, if the \( p \) has sufficient integrity, then an assume term could cause \( \Pi'; p \vdash H \leq s' \) to hold in a delegation context \( \Pi' \) of a subterm of \( e \). The key to proving our result relies on using Lemma 1 to constrain the assumptions that can be added to \( \Pi' \). Thus noninterference in FLAC is dependent on \( H \) and its relationship to \( p \) and the type \( s' \).

Theorem 1 states that for some principal \( H \) that flows to \( s \) but not \( \ell \) says \text{bool}, if \( p \) has low integrity relative to \( \bigwedge (H^{s'}) \) and the integrity of \( \ell \), and if the evaluation of \( e \) differs only in the value of \( s'-\text{typed} \) inputs, the computed values are equal.14

14It is standard for noninterference proofs in languages with higher-order functions to restrict their results to non-function types (cf. [20], [11], [29]). In this paper, we prove noninterference for boolean types, encoded as \text{bool} = (unit + unit). With an appropriate equivalence relation on terms, this noninterference result can be lifted to more general types.
**Theorem 1** (Noninterference). Let $\Pi; \Gamma, x : s; p \vdash e : \ell$ says $bool$ such that

1) $\Pi; pc \vdash H \leq s$
2) $\Pi; pc \not\vdash H \leq \ell$ says $bool$
3) $\Pi; pc \not\vdash H^{\ell} \leq \Delta(H^{-}) \wedge \ell^{\ell}$

Then $e[x \mapsto v_{1}] \rightarrow^{*} v'_{1}$ and $e[x \mapsto v_{2}] \rightarrow^{*} v'_{2}$ implies $v'_{1} = v'_{2}$.

*Proof.* See Appendix A.

Condition 1 identifies $s$ as a “high” type—at least as restricted as $H$. Condition 2 identifies $\ell$ says $bool$ as a “low” type, to which information labeled $H$ should not flow. Condition 3 identifies $pc$ as having low integrity compared to the voice of $H^{\rightarrow}$ and $\ell^{\ell}$, the integrity of the expression $e$. If $e$ evaluates to $v'_{1}$ and $v'_{2}$, then $v'_{1} = v'_{2}$.

Noninterference is a key tool for obtaining many of the security properties we seek. For instance, noninterference is essential for verifying the properties of commitment schemes discussed in Section V-A. The proofs of these properties are described in Appendix B.

**C. Robust declassification**

Using our noninterference result, we obtain a more general semantic security property for FLAC programs. That property, robust declassification [30], requires disclosures of secret information to be independent of low-integrity information. Robust declassification permits some confidential information to be disclosed to an attacker, but attackers can influence neither the decision to disclose information nor the choice of what information is disclosed. Therefore, robust declassification is a more appropriate security condition than noninterference when programs are intended to disclose information.

Programs and contexts that meet the requirements of Theorem 1 trivially satisfy robust declassification since no information is disclosed. In higher-integrity contexts where the $pc$ speaks for $H^{\rightarrow}$ (and thus may influence its trust relationships), FLAC programs exhibit robust declassification.

Following Myers et al. [31], we extend our set of terms with a “hole” term $\_\_\_\_\_\_$ representing portions of a program that are under the control of an attacker. We extend the type system with the following rule for holes with lambda-free types:

\[
[HOLE] \quad \Pi; pc \vdash H^{\ell} \leq t \quad \Pi; pc \vdash H^{\ell} \not\vdash \Delta(pc) \\
\Pi; \Gamma; pc \vdash [\_\_\_\_] : t
\]

We write $e[\_\_\_\_]$ to denote a program $e$ with holes. Let an attack be a vector $\vec{a}$ of terms and $e[\vec{a}]$ be the program where $a_{i}$ is substituted for $e_{i}$. An attack $\vec{a}$ is a fair attack [30] on a well-typed program with holes $e[\_\_\_\_]$ if the program $e[\vec{a}]$ is also well typed. Unfair attacks give the attacker enough power to break security directly, without exploiting existing declassifications.

**Theorem 2** (Robust declassification). Given a program $e[\_\_\_\_]$ such that $\Pi; \Gamma, x : s; p \vdash e[\_\_\_\_] : \ell$ says $bool$, where the following conditions hold.\(^{15}\)

1) $\Pi; pc \vdash H \leq s$
2) $\Pi; pc \not\vdash H \leq \ell$ says $bool$
3) $\Pi; pc \not\vdash H^{\ell} \not\vdash \Delta(H^{-}) \vee \ell^{\ell}$
4) $\Pi; pc \not\vdash pc \not\vdash H^{\ell}$

Choose any $\vec{a}$ and $\vec{b}$ such that $\Pi; \Gamma, x : s; pc \vdash e[\vec{a}] : \ell$ says $bool$ and $\Pi; \Gamma, x : s; pc \vdash e[\vec{b}] : \ell$ says $bool$. Then, suppose $e[\vec{a}][x \mapsto v_{1}] \rightarrow^{*} v'_{1}$ for $i \in \{1, 2\}$ such that $v'_{1} \simeq v'_{2}$. Then if $e[\vec{b}][x \mapsto v_{2}] \rightarrow^{*} v''_{i}$ for $i \in \{1, 2\}$, $v''_{1} \simeq v''_{2}$.

*Proof.* See Appendix A.

Our formulation of robust declassification is more general than previous definitions since it permits some endorsements, albeit restricted to untrusted principals that cannot influence the trust relationships of $\ell^{\ell}$, the integrity of the result. Previous definitions of robust declassification [31], [30] forbid endorsement altogether; qualified robustness [31] permits endorsement but offers only possibilistic security.

**VIII. RELATED WORK**

Many languages and systems for authorization or access control have combined aspects of information security and authorization (e.g., [32], [33], [34], [8], [35], [9]) in dynamic settings. However, almost all are susceptible to security vulnerabilities that arise from the interaction of information flow and authorization [12]: probing attacks, delegation loopholes, poaching attacks, and authorization side channels. DCC [11], [2] has been used to model both authorization and information flow, but not simultaneously. DCC programs are type-checked with respect to a static security lattice, whereas FLAC programs can introduce new trust relationships during evaluation, enabling more general applications.

Boudol [36] defines terms that enable or disable flows for a lexical scope, similar to assume terms, but does not restrict their usage. Rx [8] and RTI [9] use labeled roles to represent information flow policies. The integrity of a role restricts who may change policies. However, information flow in these languages is not robust [31]; attackers may indirectly affect how flows change when authorized principals modify policies.

Some prior approaches have sought to reason about the information security of authorization mechanisms. Becker [37] discusses probing attacks that leak confidential information to an attacker. Garg and Pfennig [38] present a logic that ensures assertions made by untrusted principals cannot influence the truth of statements made by other principals.

Previous work has studied information flow control with higher-order functions and side effects. In the SLam calculus [39], implicit flows due to side effects are controlled via indirect reader annotations on types. Zdancewic and Myers [40] and Flow Caml [20] control implicit flows via $pc$ annotations.

\(^{15}\) Condition 3 is strengthened from the version published in CSF to add a needed requirement that $H^{\ell} \not\vdash \ell^{\ell}$ does not hold. This is a reasonable condition because otherwise the result would effectively have low integrity, allowing attacks to affect it directly.
on function types. FLAC also controls side effects via a \( pc \) annotation, but here the side effects are changes in trust relationships that define which flows are permitted. Tse and Zdancewic [22] also extend DCC with a program-counter label but for a different purpose: their \( pc \) tracks information about the protection context, permitting more terms to be typed.

DKAL* [41] is an executable specification language for authorization protocols, simplifying analysis of protocol implementations. FLAC may be used as a specification language, but FLAC offers stronger guarantees regarding the information security of specified protocols. Errors in DKAL* specifications could lead to vulnerabilities. For instance, DKAL* provides no intrinsic guarantees about confidentiality, which could lead to unauthorized side channels or probing attacks.

The Jif programming language [21], [42] supports dynamically computed labels through a simple dependent type system. Jif also supports dynamically changing trust relationships through operations on principal objects [43]. Because the signatures of principal operations (e.g., to add a new trust relationship) are missing the constraints imposed by FLAC, authorization can be used as a covert channel. FLAC shows how to close these channels in languages like Jif.

Dependently-typed languages are often expressive enough to encode authorization policies, information flow policies, or both. The \( F^* \) [44] type system is capable of enforcing information flow and authorization policies. Typing rules like those in FLAC could probably be encoded within its type system, but so could incorrect, insecure rules. Thus, FLAC contributes a model for encodings that enforce strong information security. Aura [45] embeds a DCC-based proof language and type system in a dependently-typed general-purpose functional language. As in DCC, Aura programs may derive new authorization proofs using existing proof terms and a monadic bind operator. However, since Aura only tracks dependencies between proofs, it is ill-suited for reasoning about the end-to-end information-flow properties of authorization mechanisms.

IX. CONCLUSION

Existing security models do not account fully for the interactions between authorization and information flow. The result is that both the implementations and the uses of authorization mechanisms can lead to insecure information flows that violate confidentiality or integrity. The security of information flow mechanisms can also be compromised by dynamic changes in trust. This paper has proposed FLAC, a core programming language that coherently integrates these two security paradigms, controlling the interactions between dynamic authorization and secure information flow. FLAC offers strong guarantees and can serve as the foundation for building software that implements and uses authorization securely. Further, FLAC can be used to reason compositionally about secure authorization and secure information flow, guiding the design and implementation of future security mechanisms.

ACKNOWLEDGMENTS

We thank Mike George, Elaine Shi, and Fred Schneider for helpful discussions, our anonymous reviewers for their comments and suggestions, and Jed Liu and Matt Stillerman for feedback on early drafts. This work was supported by grant N00014-13-1-0089 from the Office of Naval Research, by MURI grant FA9550-12-1-0400, and by a grant from the National Science Foundation (C CF-0964409). This paper does not necessarily reflect the views of any of these sponsors.

REFERENCES


Syntax extensions
\[ v ::= \ldots \mid (v \mid v) \]

Typing extensions
\[ \Pi; \Gamma; \mathsf{pc} \vdash e : s \quad \Pi; \Gamma; \mathsf{pc} \vdash e_2 : s \]

Evaluation extensions
\[ e_1 \rightarrow e'_1 \quad e_2 \rightarrow e'_2 \quad \{i, j\} = \{1, 2\} \]

Lemma 2 (Soundness).
If \( e \rightarrow^* e' \) then \( [e]_1 \rightarrow [e']_1 \) and \( [e]_2 \rightarrow [e']_2 \).

Proof. By inspection of the rules in Figure 4 and Figure 9.

Lemma 3 (Completeness).
If \( [e]_1 \rightarrow^* v_1 \) and \( [e]_2 \rightarrow^* v_2 \), then there exists some \( v \) such that \( e \rightarrow^* v \).

Proof. Assume \( [e]_1 \rightarrow^* v_1 \) and \( [e]_2 \rightarrow^* v_2 \). The extended set of rules in Figure 9 always move brackets out of subterms, and therefore can only be applied a finite number of times. Therefore, by Lemma 2, if \( e \) diverges, either \([e]_1\) or \([e]_2\) diverge; this contradicts our assumption.

It remains to be shown that if the evaluation of \( e \) gets stuck, either \([e]_1\) or \([e]_2\) gets stuck. This is easily proven by induction on the structure of \( e \). Therefore, since we assumed \( [e]_1 \rightarrow^* v_1 \), then \( e \) must terminate. Thus, there exists some \( v \) such that \( e \rightarrow^* v \).

Lemma 4 (Robust transitivity).
If \( \Pi; \ell \parallel p \parallel q \) and \( \Pi; \ell \parallel q \parallel r \), then \( \Pi; \ell \parallel p \parallel q \parallel r \).

Proof. This is a consequence of the FLAM’s Factorization Lemma [12]. See [46] for Coq proof.

Lemma 5 (Voices).
If \( \Pi; \ell \parallel p \parallel q \) then \( \Pi; \ell \parallel \nabla(p) \parallel \nabla(q) \).

Proof. By induction on the derivation of \( \Pi; \ell \parallel p \parallel q \).
and each $\langle p \triangleright q \mid pc; \ell \rangle \in \Pi$ has $\Pi; \ell \Vdash \nabla(p^\rightarrow) \triangleright \nabla(q^\rightarrow)$, so $\langle p \triangleright q \mid pc; \ell \rangle \in \Pi$ implies $\Pi; \ell \Vdash \nabla(p) \triangleright \nabla(q)$. The remaining cases are trivial.

**Lemma 6** (pc reduction). If $\Pi; \Gamma; pc \vdash e : s$ and $\Pi; pc \Vdash pc \subseteq pc'$, then $\Pi; \Gamma; pc \vdash e : s$.

**Proof.** By induction on the derivation of $\Pi; \Gamma; pc \vdash e : s$ and Lemma 4.

**Theorem 3** (Subject reduction). Suppose $\Pi; \Gamma; pc \vdash e : s$ and $[e]_i \rightarrow [e']_i$. If $i \in \{1, 2\}$ then assume $\Pi; pc \Vdash H \subseteq pc$. Then $\Pi; pc \vdash e' : s$.

**Proof.** By induction on the derivation of $[e]_i \rightarrow [e']_i$. See the technical report [28] for details.

**Lemma 1** (Delegation invariance). Suppose $\Pi; \Gamma; pc \vdash e : s$ such that $e \Rightarrow e'$ where $v$. Then for some $p'$, and $\varphi'$, and $\Pi'$, we have $\Pi; pc \vdash v : \varphi'$. Then $\Pi; pc \vdash e' : s$. Furthermore, for all $p$ and $q$ such that $\Pi; pc \not\vdash \nabla(q)$,

$$\Pi; pc \Vdash p \triangleright q \iff \Pi'; pc \Vdash p \triangleright q$$

**Proof.** If $e'$ is not a where term, choose $\Pi' = \Pi$. Otherwise $e' = \langle e'' \rangle$ where $v$, and $\Pi' = \Pi; [p' \triangleright q' \mid pc; \ell]$. Assume $\Pi; pc \Vdash p \triangleright q$, then $\Pi; pc \Vdash p \triangleright q$ by R-Weak. In the other direction, assume $\Pi'; pc \Vdash p \triangleright q$, but for contradiction, also assume that $\Pi; pc \not\Vdash p \triangleright q$. By Theorem 3, we have $\Pi; pc \vdash e''$ where $v$. By Where with $pc' = pc$, $\Pi; \Gamma; pc \vdash v : \varphi'$. By Lemma 5. But $\Pi' \vdash \nabla(q') \triangleright \nabla(q)$ is impossible $\Pi; pc \not\Vdash \nabla(q)$, a contradiction.

Therefore $\Pi; pc \not\Vdash \nabla(q') \triangleright \nabla(q)$, and for all $p''$ such that $\Pi; pc \vdash p'' \triangleright q'$, we have $\Pi; pc \not\Vdash p'' \triangleright q'$. Thus, since $p$ did not act for $q$ in $\Pi; pc \not\Vdash p \triangleright q$, it also does not act for $q$ in $\Pi'$; $\Pi' \vdash \nabla(q)$, which contradicts our assumption.

**Theorem 1** (Noninterference). Let $\Pi; \Gamma, x : s; pc \vdash e : s \equiv \ell$ says bool such that

1) $\Pi; pc \vdash H \subseteq s$

2) $\Pi; pc \not\Vdash H \subseteq \ell$ says bool

3) $\Pi; pc \not\Vdash \nabla(H^\rightarrow) \triangleright \ell^\rightarrow$

Then $e[x \rightarrow v_1] \rightarrow^* v_1'$ and $e[x \rightarrow v_2] \rightarrow^* v_2'$ implies $v_1' = v_2'$.

**Proof.** Assume $v_1 \neq v_2$ and $e[x \rightarrow v_i] \rightarrow^* v_i'$ for $i \in \{1, 2\}$.

By Lemma 3, there is some $v'$ such that $e[x \rightarrow (v_1 \mid v_2)] \rightarrow^* v'$.

We prove $\langle v'_1 \rangle_1 = \langle v'_2 \rangle_2$ by showing, via induction on the structure of $v'$, that $v'$ contains no bracketed terms. Without loss of generality, assume $v'_1 = u_1$ where $w_1$. By Theorem 3 and Lemma 1, and WHERE with $pc = pc$, there exists a $\Pi'$ such that $\Pi'; \Gamma; pc \vdash u_1 : s$ and

$$\Pi; pc \Vdash pc \triangleright \nabla(H^\rightarrow) \triangleright \ell^\rightarrow$$

Therefore, since $\Pi; pc \not\Vdash H \subseteq \ell$ says bool. By assumption, $e[x \rightarrow v_i] \rightarrow^* v_i'$ therefore $e'[y \rightarrow b_i'] \rightarrow^* v_i'$. Then Theorem 1 implies $v_i'' = v_i''$.

**Theorem 2** (Robust declassification). Given a program $e[\bullet]$ such that $\Pi; \Gamma; x : s; pc \vdash e[\bullet] : s \equiv \ell$ says bool, where the following conditions hold

1) $\Pi; pc \vdash H \subseteq s$

2) $\Pi; pc \not\Vdash H \subseteq \ell$ says bool

3) $\Pi; pc \not\Vdash \nabla(H^\rightarrow) \triangleright \ell^\rightarrow$

4) $\Pi; pc \not\Vdash pc \triangleright \ell^\rightarrow$

Choose any $\bar{a}$ and $\bar{b}$ such that $\Pi; \Gamma, x : s; pc \not\vdash e[\bar{a}] : s \equiv \ell$ says bool and $\Pi; \Gamma, x : s; pc \not\vdash e[\bar{b}] : s \equiv \ell$ says bool. Then, suppose $e[\bar{a}][x \rightarrow v_i] \rightarrow^* v_i'$ for $i \in \{1, 2\}$ such that $v_i' \approx v_i''$. Then if $e[\bar{b}][x \rightarrow v_i] \rightarrow^* v_i'$ for $i \in \{1, 2\}$, $v_i'' \approx v_i''$.

**Proof.** Assume $v_1 \neq v_2$ and $e[\bar{a}][x \rightarrow v_i] \rightarrow^* v_i'$ such that $v_i' \approx v_i''$, and $e[\bar{b}][x \rightarrow v_i] \rightarrow^* v_i'$ for $i \in \{1, 2\}$. We want to show that $v_1'' \approx v_2''$.

Suppose for contradiction $e[\bar{b}][x \rightarrow v_i] \rightarrow^* v_i'$ for $i \in \{1, 2\}$ but $v_i'' \neq v_i''$. Then $\bar{b}$ must contain some element $b_j$ such that $b_j[x \rightarrow v_i] \rightarrow^* b_j'$ and $b_j \neq b_j$, otherwise $v_i'$ and $v_i''$ could not have been equal.

By induction on $\Pi; \Gamma, x : s; pc \vdash e[\bullet] : s$ and Lemma 6, there exist $\Pi'$ and $\Gamma'$ where $\Pi' \supseteq \Pi$ and $\Gamma' \supseteq \Gamma$, $x : s$ such that $\Pi'; \Gamma; pc \vdash e[\bullet] : s$. Furthermore, extending the context preserves types, so we also have $\Pi'; \Gamma', y ; s; pc \vdash e' : \ell$ says bool. Next, we need to meet the three conditions of the theorem. For condition 1), since $b_j[x \rightarrow v_i] \not\approx b_j[x \rightarrow v_2]$, by BRACKET and Theorem 3, we have $\Pi; pc \vdash H \subseteq s_j$.

For conditions 2) and 3), we can use Lemma 1 to relate the extended assumption context $\Pi'$ to the original (smaller) assumption context $\Pi$. We know that for all $r$,

$$\Pi; pc \vdash r \triangleright \ell^\rightarrow \iff \Pi'; pc \vdash r \triangleright \ell^\rightarrow$$

Therefore, since $\Pi; pc \not\Vdash pc \triangleright \ell^\rightarrow$, we have $\Pi'; pc \not\Vdash pc \triangleright \ell^\rightarrow$ and thus $\Pi'; pc \not\Vdash \nabla(H^\rightarrow) \triangleright \ell^\rightarrow$. Similarly, we also have $\Pi'; pc \not\Vdash H \subseteq \ell$ says bool. By assumption, $e[\bar{b}][x \rightarrow v_i] \rightarrow^* v_i''$ therefore $e'[y \rightarrow b_j'] \rightarrow^* v_i''$. Then Theorem 1 implies $v_i'' = v_i''$.

**APPENDIX B**

**COMMITMENT SCHEME VERIFICATION**

To prove the desired properties of commitment schemes for boolean values, let $s = \text{bool}$ and recall:

$\Gamma_{\text{ero}} = \text{commit}, \text{receive}, \text{open}, x : p^\rightarrow \text{ says s}, y : p \land q^\rightarrow \text{ says s}$

- $q$ cannot receive a value that hasn’t been committed. Let $H = p^\rightarrow \land q^\rightarrow$. For any $e$ and $\Gamma_{\text{ero}}; pc \vdash e : p \land q^\rightarrow$ says bool, observe that $\Pi; pc \vdash H \subseteq$
\( p \rightarrow \text{says bool}, \Pi; \text{pc}_q \not\models H^\rightarrow \subseteq p^\rightarrow, \Pi; \text{pc}_q \not\models H^\leftarrow \subseteq (p \land q)^\rightarrow, \) and \( \Pi; \text{pc}_q \not\models \text{pc}_q \models \nabla(H^\rightarrow) \land (p \land q)^\leftarrow. \) Therefore, by Theorem 1, if \( e[x \mapsto v_1] \rightarrow^* v'_1 \) and \( e[x \mapsto v_2] \rightarrow^* v'_2, \) then \( v'_1 \simeq v'_2. \)

- **q cannot learn a value that hasn't been opened.** Let \( H = p^\rightarrow \land q^\rightarrow. \) For any \( e, \ell, \) and \( \Gamma_{cro}; \text{pc}_q \vdash e : \ell \cap q^\rightarrow \text{says bool}, \) observe that both \( \Pi; \text{pc}_q \vdash H \leq p^\rightarrow \text{says bool} \) and \( \Pi; \text{pc}_q \vdash H \leq p \land q^\rightarrow \text{says bool}. \) Therefore, Theorem 1 applies as above for both \( x \) and \( y. \) Thus if \( e[x \mapsto v_1] \rightarrow^* v'_1 \) and \( e[x \mapsto v_2] \rightarrow^* v'_2, \) then \( v'_1 \simeq v'_2. \) and if \( e[x \mapsto v_1] \rightarrow^* v''_1 \) and \( e[x \mapsto v_2] \rightarrow^* v''_2, \) then \( v''_1 \simeq v''_2. \)

- **p cannot open a value that hasn't been received.** Let \( H = p^\rightarrow \land q^\rightarrow. \) For any \( e \) and \( \Gamma_{cro}; \text{pc}_p \vdash e : p^\leftarrow \land q \text{ says bool, observe that } \Pi; \text{pc}_p \vdash H \leq p^\rightarrow \text{ says bool, } \Pi; \text{pc}_p \not\models H^\rightarrow \subseteq q^\rightarrow, \Pi; \text{pc}_p \not\models H^\leftarrow \subseteq (p \land q)^\rightarrow, \) and \( \Pi; \text{pc}_p \not\models \text{pc}_p \models \nabla(H^\rightarrow) \land (p \land q)^\leftarrow. \) Therefore, by Theorem 1, if \( e[x \mapsto v_1] \rightarrow^* v'_1 \) and \( e[x \mapsto v_2] \rightarrow^* v'_2, \) then \( v'_1 \simeq v'_2. \)