Information Flow Control for Distributed Trusted Execution Environments

The Harvard community has made this article openly available. Please share how this access benefits you. Your story matters

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Citable link</td>
<td><a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:40614411">http://nrs.harvard.edu/urn-3:HUL.InstRepos:40614411</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at <a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA">http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA</a></td>
</tr>
</tbody>
</table>

Information Flow Control for Distributed Trusted Execution Environments

Anitha Gollamudi
Stephen Chong
and
Owen Arden

TR-01-19

Computer Science Group
Harvard University
Cambridge, Massachusetts
Abstract—Distributed applications cannot assume that their security policies will be enforced on untrusted hosts. Trusted execution environments (TEEs) combined with cryptographic mechanisms enable execution of known code on an untrusted host and the exchange of confidential and authenticated messages with it. TEEs do not, however, establish the trustworthiness of code executing in a TEE. Thus, developing secure applications using TEEs requires specialized expertise and careful auditing.

This paper presents DFLATE, a core security calculus for distributed applications with TEEs. DFLATE offers high-level abstractions that reflect both the guarantees and limitations of the underlying security mechanisms they are based on. The accuracy of these abstractions is exhibited by asymmetry between confidentiality and integrity in our formal results: DFLATE enforces a strong form of noninterference for confidentiality, but only a weak form for integrity. This reflects the asymmetry of the security guarantees of a TEE: a malicious host cannot access secrets in the TEE or modify its contents, but they can suppress or manipulate the sequence of its inputs and outputs. Therefore DFLATE cannot protect against the suppression of high-integrity messages, but when these messages are delivered, their contents cannot have been influenced by an attacker.

Index Terms—Information flow control, language-based security, trusted execution environment, enclaves, distributed systems, security

I. INTRODUCTION

Many applications rely on security checks in compilers and runtime systems to enforce security policies. In distributed decentralized settings (where applications are distributed, entities involved in the application may be mutually distrustling, and no single node is trusted by all entities), the effectiveness of such checks is limited: local security checks cannot ensure that a remote host will protect confidential information it receives. Encryption can ensure that an untrusted host cannot reveal secrets in the TEE or modify its contents, but they can suppress or manipulate the sequence of its inputs and outputs. Therefore DFLATE cannot protect against the suppression of high-integrity messages, but when these messages are delivered, their contents cannot have been influenced by an attacker.

This technical report supplements the CSF 2019 publication [26] with additional details.

1Fully homomorphic encryption [22] can permit such computation, but at great cost to performance.
channel to the enclave. Alice uses this channel to provide decryption and signing keys to the enclave (messages 4 and 5). Later, she can use these keys to exchange encrypted and signed inputs and outputs with the enclave (messages 6-9) without repeating the remote attestation protocol.

Omitting or improperly executing any of the above steps can undermine Alice’s security. If the remote attestation is omitted, Alice has no guarantee that the enclave code (and not some malicious version of it) is running nor that code execution is protected from Bob. If Alice fails to encrypt (or sign) inputs to the enclave, or uses keys that are accessible to Bob, then Bob can learn (or modify) the inputs. Similarly, if the enclave fails to properly encrypt and sign outputs, Bob may be able to read or modify them.

Fortunately, the security and correctness of the first three messages is mostly independent of the application. So a relatively simple (but trustworthy) library API or language extension can provide remote attestation capabilities to applications and eliminate programmer errors.

But even with remote attestation and proper encryption and authentication, Alice’s security may still be undermined. Although Bob cannot decrypt messages between Alice and the enclave, he does see each encrypted message when it is transmitted and may be able to infer secret information based on the sequence of exchanged messages. For example, the pseudocode below sends an encrypted and signed message msg from within an enclave over channel ch if h is true.

\[
\text{if } h \text{ then send } ch (\text{enc} (\text{sign} \text{ msg})) \text{ else ()}
\]

Because of the TEE and the cryptographic mechanisms, Bob cannot directly access h or msg, but he can infer the value of h based on whether a message is sent. The above code might also be problematic in terms of integrity: if Bob can influence the value of h, he can suppress the message. Similar code might permit Bob to replay messages or permute the message order.

**Information-flow control (IFC)** is well suited to protect against these kinds of vulnerabilities because it enables end-to-end semantic guarantees such as noninterference, which ensures an attacker cannot infer secret information from public outputs. However, existing IFC languages cannot precisely model the security guarantees and limitations of TEEs.

There are two key challenges to enforcing IFC in a decentralized distributed setting that employs encryption, signatures, and TEEs. The first challenge is to (symbolically) represent the security guarantees of the cryptographic mechanisms without abstracting away the power of the attacker to permute, suppress, or infer secrets from the message sequence. Security models of existing distributed IFC systems (Fabric [29] and DStar [43]) are insufficiently precise. Encryption and digital signatures allow secret or high-integrity messages to be sent over untrusted channels. For example, Alice could sign and send a message to the enclave over a channel controlled by Bob; if the enclave receives the message it knows (by verifying the signature) that it is from Alice, even though Bob could suppress the message. In Fabric and DStar, the only sound policy (that doesn’t ignore a potential attack) expresses that both Alice and Bob might have influenced the message. In other words, they are too coarse-grained to distinguish the attacker’s influence on control flow from its influence on data flow. Consequently, their enforcement mechanisms cannot determine if code respects the programmer’s intended policy.

This scenario arises in any nontrivial application using TEEs, since the main benefit of TEEs is to run computation on potentially malicious nodes. So IFC must be able to reason about protected data flowing through untrusted nodes.

The second challenge is to design high-level abstractions that accurately reflect the guarantees of TEEs in a decentralized distributed setting. Currently, developers integrate TEEs into their applications using low-level library APIs. Using these libraries correctly may require a different skill set from that needed for the rest of the application. A better approach would be to design high-level programming abstractions for TEEs that don’t burden the developer with low-level implementation details. Code expressed with these abstractions can be used to synthesize low-level implementations, shifting trust from application developers to the compiler.

Finding the right security abstraction for TEEs in decentralized settings is challenging. TEEs ensure that specific code is running securely, but, as discussed above, do not ensure the trustworthiness of the code. So different entities may trust different enclaves (perhaps based on who wrote the enclave code or analysis of the code). TEE mechanisms don’t hide the existence of messages to and from an enclave, nor guarantee message delivery. A suitable TEE abstraction must reflect these limitations on communication and allow entities to express their trust in specific TEEs and entities.

DFLATE addresses these challenges. DFLATE has sufficiently fine-grained information-flow control to distinguish (and usefully reason about) important TEE use cases. DFLATE provides language abstractions for TEEs, distribution, and security principals that can ensure security while enabling applications to benefit from the powerful features of TEEs.

DFLATE is the first language to enforce end-to-end information security for distributed applications with TEEs. We prove that well-typed DFLATE programs enjoy noninterference guarantees. Confidentiality noninterference [23] ensures that an attacker cannot infer secret information from public outputs. Integrity noninterference ensures that an attacker cannot influence high-integrity outputs by modifying low-integrity inputs.

Integrity is dual to confidentiality [10], and thus most systems that protect confidentiality noninterference also protect integrity noninterference. However, DFLATE provides asymmetric guarantees for confidentiality and integrity. This asymmetry reflects inherent limitations of TEEs. The confidentiality
and integrity of the contents of inputs and outputs to TEEs can be cryptographically protected, but neither the TEE itself nor cryptographic mechanisms can prevent the host of the TEE from suppressing or manipulating the sequence of inputs and outputs. Hence, we derive strong noninterference results for confidentiality, but weaker results for integrity that hold only when messages are not suppressed.

II. MOTIVATING THE DFLATE DESIGN

DFLATE is a high-level language designed to be implemented using cryptographic mechanisms and trusted execution environments. Designing an IFC model in this setting is subtly different than designing a general IFC model. In this section we motivate three design features of DFLATE that are informed by cryptography and TEEs.

A. Fine-grained policies for secure communication

Suppose Alice sends a message to Carol via Bob, who is only partially trusted by Alice and Carol. Figure 2(a) illustrates the scenario where no cryptographic mechanisms are used to enforce information security, similar to the model of Fabric and DStar. Sending message A1 to Carol is secure only if Alice permits Bob to learn the contents of A1 and Carol permits Bob to (potentially) modify the contents of A1 en route. Figure 2(b) illustrates the same scenario, but Alice additionally signs the message and encrypts it with Carol’s public key. In this case, Bob can neither learn nor modify the contents of A1. However, Bob does learn of the existence of A1. Furthermore, although Bob cannot modify A1, he could replace it with a previously signed message A2, or could choose to send no message at all.

Most existing IFC abstractions do not distinguish these two scenarios and instead enforce policies conservatively using checks similar to Figure 2(a). This lack of precision effectively ignores guarantees offered by cryptographic mechanisms for communication over untrusted channels.

DFLATE distinguishes the ability to disclose or modify messages sent over a channel from the ability to observe channel traffic and influence or suppress message sequences. In DFLATE, the security of a channel is specified using two policies. One policy governs the confidentiality and integrity of the contents of messages sent over the channel, and the other governs the confidentiality and integrity of contexts in which the channel may be used. A node may receive a message that it can’t read or modify; this can be enforced by signing and encrypting the message. A node should not send a message to an untrusted node in a secret context (even if the message is public), and should not rely on a message from an untrusted node in a high-integrity context (even if the message contents are trusted).

B. Decentralized and distributed trust management

DFLATE’s abstractions are based directly on the capabilities of the underlying cryptographic and TEE mechanisms, which allows stronger assumptions and finer-grained reasoning about what information flows and actions are possible than most previous IFC models. Two places where DFLATE’s design is influenced by the underlying mechanisms are clearance bounds and computation principals.

DFLATE’s type system associates a clearance bound [38] with every node, which restricts what data may be used and produced by computations on that node. Based on trust relationships between the node and other principals, the clearance bound reflects which cryptographic keys the node has access to, and thus models the ability of a node to digitally sign values and decrypt encrypted values. In Figure 2(b), Bob does not have access to Alice’s decryption key, so any computation that attempts to read and compute with Alice’s data would exceed Bob’s clearance. Similarly, Bob would be unable to produce a new message with Alice’s integrity using a DFLATE program, modeling Bob’s inability to access Alice’s signing key.

For each source-level DFLATE computation e that will execute in a TEE, DFLATE defines a unique computation principal t. Code running in a TEE is subject to clearance bounds of the computation principal rather than of the node executing the TEE. DFLATE permits principals to express their trust in code running in a TEE by expressing trust in the corresponding computation principal t. Therefore Alice can express trust in an enclave running on Bob’s node, allowing it to perform computation on her secrets even if Bob is not trusted to do so. DFLATE also provides protection in the other direction: if Bob doesn’t trust Alice or the enclave, Alice can’t use the enclave to leak Bob’s secrets or influence his data.

C. Observability of TEE interactions

TEEs introduce additional subtlety into information flow control design. TEEs provide guarantees similar to those of a trusted third party, but executing code in a TEE on an untrusted node is not equivalent to executing code on a trusted node.

Consider our previous examples, but where Bob executes application code in an enclave E (Figure 2(c)). Although the code executes within an enclave, Bob can still observe and manipulate incoming and outgoing messages, as in Figure 2(b).

Most distributed IFC approaches (e.g., [29, 43]) ignore an attacker’s ability to analyze traffic over communication channels. This is somewhat defensible for attackers with a limited view of the network, or when nodes use obfuscating techniques like TOR [16]. With TEEs, however, ignoring this ability is not as reasonable: in Figure 2(c), Bob is the only available conduit to E. Communicating over an observed untrusted channel is fundamental to the TEE abstraction. DFLATE ensures that programs capture the ability of a host to mediate communication with its enclaves, and enables reasoning about the security of these situations. For node-to-node communication, DFLATE makes similar assumptions to previous models: only the sender and the receiver observe the communication.

III. THE DFLATE LANGUAGE

A. FLAM principal algebra

Security policies in DFLATE are based on the Flow-Limited Authorization Model (FLAM) [6], a principal algebra and logic for reasoning simultaneously about authorization and information flow control policies. Entities in a distributed application (e.g., Alice, Bob, etc.) are represented by names in a set of

2Using LIO-style clearance bounds as a proxy for access to cryptographic keys was first introduced in CLIO [41].
primitive principals \( N \). The FLAM algebra provides operations for constructing composite principals from this base set. A FLAM principal refers to the authority of the entity (or entities) represented by that principal. A principal \( p \)'s authority consists of confidentiality authority, the authority necessary to learn \( p \)'s secrets, and integrity authority, the authority necessary to influence information trusted by \( p \). Authority projections of the form \( p^\pi \) where \( \pi \in \{\to, \leftarrow, \neg\} \) allow us to represent the partial authority of a principal. For example, the principal \( p^\to \) denotes a principal with only the confidentiality authority of \( p \), and \( p^\leftarrow \) denotes a principal with only the integrity authority of \( p \). The combined authority of principals \( p \) and \( q \) is represented by the conjunction \( p \land q \), and the selective authority of principals \( p \) and \( q \) (i.e., the individual authority of either \( p \) or \( q \)) is represented by the disjunction \( p \lor q \). The universally trusted principal (with the most authority) is represented by \( \top \), and the universally distrusted principal (with the least authority) is \( \bot \).

The complete set \( P \) of FLAM principals for any setting is given by the closure of the operations \( \land, \lor, \leftarrow, \to \) over the set of primitive principals \( N \), extended with \( \top \) and \( \bot \). Principals in this set are related by a preorder \( \triangleright \), the “acts for” relation, which orders principals by increasing trust. The equivalence classes\(^3\) of \( \triangleright \) form a distributive lattice with \( \top \) and \( \bot \) as most and least trusted elements, and with \( \land \) and \( \lor \) as join and meet operations.

The trust ordering \( \triangleright \) also induces an ordering on principals specifying safe information flows. We write \( p \sqsubseteq q \) when information labeled \( p \) may safely flow to principal \( q \). The flows-to relation also forms a distributive lattice with \( \bot \to \top \) (public and trusted) as the least restrictive element, and \( \top \to \bot \) (secret and untrusted) as the most restrictive element. The flows-to relation and joins and meets in the information flow lattice are defined in terms of their authority lattice counterparts:

\[
\begin{align*}
\text{p} \sqsubseteq \text{q} & \iff \text{p}^\to \triangleright \text{q}^\to \text{and} \text{q}^\to \triangleright \text{p}^\leftarrow \\
\text{p} \land \text{q} & \iff (\text{p}^\to \land \text{q}^\to) \land (\text{p}^\leftarrow \lor \text{q}^\leftarrow) \\
\text{p} \lor \text{q} & \iff (\text{p}^\to \lor \text{q}^\to) \land (\text{p}^\leftarrow \land \text{q}^\leftarrow)
\end{align*}
\]

Every principal \( p \) is equivalent (under the trust ordering) to a principal in normal form, \( q^\to \land r^\leftarrow \), i.e., the conjunction of a confidentiality authority and an integrity authority. The voice

\(^3\)One way to remember what each arrow means is to think of confidentiality as secrets “coming from” \( p \), and integrity as information “accepted by” \( p \).

\(^4\)Principals \( p \) and \( q \) are in the same equivalence class if and only if \( p \triangleright q \) and \( q \triangleright p \).

Fig. 3: DFLATE syntax

of a principal \( p \), \( \nabla(p) \), is the integrity authority necessary to act on the behalf of the principal. Formally, if \( q^\to \land r^\leftarrow \) is the normal form of \( p \), then \( \nabla(p) = (q^\to \land r^\leftarrow) = q^\to \land r^\leftarrow \).

B. DFLATE syntax and local semantics

The DFLATE language is inspired by the Flow-Limited Authorization Calculus (FLAC) [5]. Like FLAC, DFLATE is a core calculus and secure programming model that enforces strong information security guarantees. DFLATE extends FLAC with distributed computation, communication, and TEEs, and the DFLATE type system is more compatible with implementations that use cryptographic enforcement mechanisms. This makes DFLATE a more suitable basis for the formal analysis of decentralized distributed applications, or as a core programming model for a general-purpose secure distributed programming language.

Figure 3 shows the DFLATE syntax. Principals are used both to specify the information flow policies on data and to represent the authority of the entities in the distributed application. Metavariables \( p, q, \ell, \) and \( \pi \) range over principals. We assume the set of primitive principals \( N \) includes computation principals \( t \) and nodes \( n \), representing, respectively, code executed in a TEE and host machines. Nodes and computation
pl, D ⊢ e → e′

[DE-APP]  pl, D ⊢ (λ(x:τ)[pc, Θ, P, II]. e) v → e[v/x]

[DE-UNITM]  pl, D ⊢ ηℓ v → ηℓ v

[DE-BINDM]  pl, D ⊢ bind x = ηℓ v in e → e[v/x]

[DE-ASSUME]  pl, D ⊢ assume v in e → e where v

[DE-TEE]  pl, D ⊢ TEE′ s → runTEE′ s

[DE-WHILE]  pl, D · v ⊢ e → e′  

pl, D ⊢ e where v → e′ where v

[DE-SEND]  pl, D ⊢ send ν v then e → send ν v′ then e

where e′ = export_del(D, v) noTEE(v)

export_del is a function such that if D = ⟨p1 ≽ q1⟩ · · · ⟨pn ≽ qn⟩ then

export_del(D, e) = e where (p1 ≽ q1) . . . where (pn ≽ qn).

The protection mechanism is left abstract, but DFLATE’s design is consistent with standard cryptographic mechanisms like semantically secure asymmetric encryption [32] and existentially unforgeable signature schemes [24]. Intuitively ηℓ e evaluates e to a value, and then encrypts and signs the value with keys appropriate for ℓ to protect it. Protected value ηℓ v represents the encrypted and signed value v (see rule DE-UNITM). For example, ηAlice·−ARob·ν represents value ν signed by Alice and encrypted with Bob’s key. A protected value may flow to places that would be insecure for the unprotected value to go. A protected value can be used only via a monadic bind term bind x = ηℓ v in e, which binds v to variable x in e (rule DE-BINDM). This is analogous to decrypting and verifying the signature of protected value ηℓ v.

Expression TEE′ s represents a TEE that will execute computation s. Syntactic category s (omitted in Figure 3) consists of expressions without TEE or spawn terms. This syntactically prevents nested or forking TEE code and reflects restrictions in existing TEE mechanisms. Each expression s is uniquely identified by a computation principal t, which can be thought of as a hash of the code s and can be used to identify a TEE. Assuming that t uniquely identifies s is compatible with the trust assumptions of most TEE designs: code is securely measured and the hash is unique up to collisions, which occur with negligible probability. Rule DE-TEE evaluates the source-level TEE term to the intermediate value runTEE′ s. Note that the t in runTEE′ s is related to the source-level expression s; additional steps evaluate s, but t remains fixed.

C. Distributed semantics

Process ⟨n, e⟩ is expression e running on node n. A distributed configuration ⟨n₁, e₁⟩ · · · ⟨nᵢ, eᵢ⟩ is the parallel composition of processes ⟨nᵢ, eᵢ⟩. Without loss of generality, we assume that each node nᵢ in a distributed configuration is unique. We assume standard structural equivalence for distributed configurations and use metavariable D to range over distributed configurations.

Rules for distributed configurations are presented in Figure 5 and have the form \( D \Rightarrow D′ \). Some of the rules use evaluation contexts [17] for sequential evaluation: \( \langle n, e \rangle \) is an expression...

All inference rules are given in Appendix A.
with subexpression $e$ that can be reduced. Evaluation contexts are standard and defined in Appendix A.

Rule PAR-STEP states that a distributed configuration takes a step whenever one of its processes takes a step. Note that the sequential evaluation of a process uses the initial delegation sequence $D_{init}$, although the process may use additional delegations via assume and where terms.

Processes communicate via channels. Channel endpoints are unidirectional: an endpoint can be used to send or receive values, but not both. Communication is synchronous: a send block until there is a matching receive, and a receive blocks until a message is available. Channels are not first-class and we ensure that a channel endpoint is used by at most one process. This restriction prevents certain races that are both difficult for programmers to reason about as well as potential covert channels. Indeed, even though the distributed semantics are non-deterministic, because of the careful management of channel endpoints, there can never be a race between two sends on the same channel or between two receives on the same channel. Thus our distributed semantics is confluent.

Rule PAR-SEND-RECV matches up a process that is sending on channel $\nu$ with a process that is receiving on $\nu$. For bookkeeping purposes in the proof, the value sent over the channel is a where term that includes all delegations in use by the sender. Rule DE-SEND ensures that delegations are included in the value before the communication occurs. We allow closures to be sent over channels, but the type system carefully ensures that the closure can not contain inappropriate channel endpoints nor can the closure contain TEE code.

Suppose node $n_1$ is sending a value $v$ over the channel $\nu$ and node $n_2$ is ready to receive it. Observe that the result of stepping $\text{send } ch \ v$ then $e$ with rule PAR-SEND-RECV results in the expression $e; \Box$ and $\text{recv } ch \ as \ x \ in \ e'$ becomes $\ell[x \rightarrow v]; \Box$. The $; \Box$ term is used to denote the end of the process: $e; \Box$ reduces to an output value $v'; \Box$. While $v'; \Box$ is a valid expression, output values are not in the syntactic category of internal values $v$ in Figure 3. Our type system ensures that well-typed programs never use output values as internal values. This restriction merely ensures that the continuation of sending or receiving process is a subterm of the send or receive. It does not affect the expressiveness of the language, only the structure.

This design helps simplify type system constraints that track the influence of sent and received messages on control flow.

Term $\text{spawn } \bowtie n \left( pl, ch_1 [pc_1; \tau_1], ch_2 [pc_2; \tau_2] \right), e_1 \ then \ e_2$ spawns expression $e_1$ as a new process on node $n$ and continues as $e_2$ (rule PAR-SPAWN). Expressions $e_1$ and $e_2$ may refer to channel variables $ch_1$ and $ch_2$, which, when the process is spawned, will be replaced with fresh channels, enabling the parent and child processes to communicate. Channel type annotations $pc_1$, $\tau_1$, $pc_2$, and $\tau_2$ restrict how channels may be used. Place $pl$ indicates the intended endpoint of the newly created channel: if the newly spawned process is on the same host as the parent, then $pl$ may indicate a computation principal $t$ that is the intended endpoint. This enables a pattern where a parent process can spawn a child process that executes a TEE, and the parent process can communicate with the TEE.

IV. Threat Model

The DFLATE type system statically enforces information-flow control policies on data processed by DFLATE programs. In order to understand various design choices in the type system, it is necessary to understand the attacker model.

We assume that some conjunction of principals (denoted $A$ for “attacker”) are malicious. Since nodes are principals, this also permits us to express that nodes are compromised. Intuitively, the security guarantees that we will provide (Section VII) are based on the idea that “you can be hurt only by those you trust.” That is, if $A$ is the malicious principal and $p$ is a “good principal” (i.e., a principal that doesn’t trust $A$), then $A$ can not violate the security concerns of $p$. We assume all processes start execution with common trust assumptions, i.e., the initial delegation sequence $D_{init}$.

For confidentiality, we assume that a good principal provides confidential input to a program and that the attacker observes the output of the program (namely, the final value computed on a compromised node). For integrity, we assume that the attacker provides untrustworthy input to a program and that a good principal consumes the output of the program. We thus use an “input/output” observational model.

We also consider a stronger observational model for confidentiality, where the attacker is able to observe the execution trace on a compromised node. However, the attacker cannot observe the contents of a ciphertext for which it does not have a decryption key: the attacker cannot distinguish values $\eta_? v$ and $\eta_? v'$ (which represent values $v$ and $v'$ encrypted and signed by principal $\ell$) if the attacker does not have the authority to decrypt $\eta_? v$ and $\eta_? v'$. Similarly, the attacker cannot observe the contents of a TEE unless it has sufficient authority to access the keys of the corresponding computation principal.

We ignore covert channels, including timing, termination, memory accesses by TEEs, and speculative-execution channels. Orthogonal techniques (e.g., [44, 34, 28]) can mitigate some of these concerns, and we expect some covert channels related to TEEs to be addressed in future TEE designs.

We assume that cryptographic mechanisms, TEE implementations, and the compiler and runtime system are correct. We assume that node-to-node communication is secure and unobserved by other principals, i.e., we do not consider network-level adversaries. Tools such as Tor [15] can be used to make it harder for network-level adversaries to observe the presence of node-to-node communication. We do, however, assume that communication with a TEE is observed by the host node. In DFLATE we use symbolic cryptography but do not treat keys as values in the language. We thus assume that an attacker has access to some set of signing and encryption keys based on trust relationships, but do not consider a Dolev-Yao-style attacker that can learn new keys from observations.

V. The DFLATE Security Type System

DFLATE types (Figure 3) include unit, sums, products, functions, type functions, and type variables. (Functions and type functions have non-standard annotations that we describe below.) Delegation types are singleton types: each delegation type $(p \succ q)$ is inhabited by a single value $(p \succ q)$. Monadic
type \( \ell \) says \( \tau \) protects an expression of type \( \tau \) at level \( \ell \); it is the type of values such as \( \eta, v \) (where \( v \) has type \( \tau \)).

The grammar presented in Figure 3 splits types into two kinds: output types, which have the form \( \tau \sqsubseteq \omega \), and internal types of the form \( \tau \). Output types represent expressions that cannot be consumed. For example, they cannot be passed as arguments to functions. Metavariable \( \tau \) is used when either an output or an internal type is permitted. The type system ensures that expressions with output types cannot be used as internal values. This distinction in types simplifies parts of the proof but does not limit the expressiveness of the language, just the structure of it.

Channels are not first-class values but do have types of the form \( \text{chan}_{pl_1 \leftarrow pl_2} \ pc \ \tau \) and \( \text{chan}_{pl_1 \leftarrow pl_2} \ pc \ \tau \). These types specify channels that connect places \( pl_1 \) and \( pl_2 \) (either nodes or TEEs) and may exchange values of type \( \tau \) in contexts up to \( pc \). Recall that channels are uni-directional. The former type specifies a send channel, (indicated by the subscript \( pl_1 \leftarrow pl_2 \)) meaning \( pl_1 \) may use the channel to send values to \( pl_2 \), the latter specifies a receive channel (subscript \( pl_1 \leftarrow pl_2 \)) meaning \( pl_1 \) may use the channel to receive values from \( pl_2 \).

Well-typed programs do not always reduce to values, however. They may also become stuck waiting for communication: either a ready send with no corresponding recv or vice versa. To distinguish these stuck programs from those that the type system is designed to prevent, we refer to well-typed programs that become stuck waiting for communication as blocked programs.

Typing judgment \( \Pi; \Gamma; \Theta; \Pi; pl; pc \vdash e : \tau \) indicates that expression \( e \) has type \( \tau \). Delegation context \( \Pi \) contains a sequence of delegations that are valid just before executing \( e \). It is a conservative approximation of the delegation sequence \( D \) that is present at run time. The delegation context is extended by assume and where terms. Variable typing context \( \Gamma \) maps variables to types. Variables may have only internal types, so all mappings in \( \Gamma \) have the form \( x : \tau \). Channel variable scope is maintained using the channel environment \( \Theta \). Principal \( pl \) indicates the place the term is typed at, either a node \( n \) or computation principal \( t \). Program counter level \( pc \) is an upper bound (in the information-flow ordering \( \sqsubseteq \)) on the decision to execute \( e \), and also a lower bound on observable side-effects of \( e \).

The core DFLATE typing rules are presented in Figures 6 and 7 present some of the key DFLATE typing rules. Rules in Figure 6 are adapted from FLAC, and those in Figure 7 cover DFLATE’s distributed computation and TEE extensions. Premises of these rules are either typing judgments or judgments that specify required relationships between principals, or between principals and types.

Acts-for judgments have the form \( \Pi \vdash p \gg q \) and require that \( p \) has at least as much authority as \( q \) in delegation context \( \Pi \). (Alternatively, that assuming the delegations in \( \Pi \), \( q \) trusts \( p \).) Recall that \( \gg \) is defined in terms of \( \gg \) so using the same rules we may also derive judgments of the form \( \Pi \vdash p \sqsubseteq q \). Intuitively, if \( \Pi \vdash p \sqsubseteq q \) information labeled with \( p \) can flow to information labeled \( q \), since (given the delegations in \( \Pi \)) the confidentiality and integrity of \( q \) is at least as restrictive as that of \( p \). Both of these judgments are simplified versions of the corresponding FLAM judgments [6], which we can use in DFLATE since delegations are reasoned about statically and thus do not provide an information channel. (FLAC could also benefit from this simplification.) Both of these forms are actually syntactic sugar for \( \Pi; \bot \wedge \top \gg; \bot \wedge \top \gg \vdash p \gg q \) in the more general FLAM judgment form \( \Pi; pc; \ell \vdash p \gg q \). The rules for deriving acts-for judgments, presented in Appendix A, are based on a fragment of the Flow-Limited Authorization Model logic [6]. Each delegation in the FLAM delegation context \( \Pi \) is labeled with a confidentiality and integrity policy. The logic establishes rules for how those delegations may be used to derive authorization judgments. The query label, \( pc \), protects the distributed authorization query by limiting communication to nodes that protect the confidentiality of \( pc \). The result label, \( \ell \), protects the confidentiality and integrity of the delegation context by limiting the delegations used to derive the judgment to those that flow to \( \ell \).

In DFLATE, authority is verified statically by the DFLATE compiler independently of any sensitive data. Therefore the query label, \( pc \), which protects the information in the acts-for query \( p \gg q \), is considered public and trusted, or \( \bot \wedge \top \gg \).

Similarly, the result of that query is based only on trustworthy information the compiler itself has provided and processed, so the result is considered public and trusted too. The benefit of embedding DFLATE’s acts-for judgment in the FLAM logic is that we can rely on FLAM’s formal properties, which have been mechanically verified [7], in our proofs. In this technical report, we formalize this embedding rigorously, correcting some technical errors in the original FLAC [5] formalization.

Type protection judgments have the form \( \Pi \vdash \ell \leq \tau \) indicating that type \( \tau \) protects information labeled with \( \ell \). Intuitively, it means that the type system ensures that any information gained by using a value of type \( \tau \) will have a security level at least as restrictive as \( \ell \). The rules for deriving type protection judgments are based on a subset of FLAC’s rules. The primary rule is DP-LBL:

\[
\text{[DP-LBL]} \quad \Pi \vdash \ell \leq \ell' \quad \Pi' \vdash \ell' \text{ says } \tau
\]

This rule connects acts-for judgments to protected types. If \( \ell \) flows to \( \ell' \), then the type \( \ell' \) says \( \tau \) protects level \( \ell \). Singleton types like unit and \( (p \gg q) \) protect any level since the type itself encodes the value: observing the runtime value carries no information. However, the type \( \tau_1 + \tau_2 \) is not protected at any level since observing the value reveals the side of the sum the value is on, even if the sides have the same type. All protection rules are given in Figure 16 in Appendix A.

DFLATE’s type protection judgment is more restrictive than both FLAC’s and the protection rules in the Dependency Core Calculus [2, 1] (which FLAC’s are based on). The restrictiveness comes from the omission of three rules. One rule, DP-LBL1, permits a level to be protected by the inner type of a says type if the outer type does not protect it.

\[
\text{[DP-LBL1]} \quad \Pi \vdash \ell \leq \tau' \quad \Pi \vdash \ell' \leq \ell \text{ says } \tau
\]
This rule is not compatible with the cryptographic mechanisms DFLATE seeks to model: it makes nested says types commutative in the sense that \( p \quad says \quad q \quad says \quad \tau \) protects the same levels as \( q \quad says \quad p \quad says \quad \tau \). Commutativity undermines the expressiveness of integrity policies since a value of type \( \tau \) signed by \( q \) then \( p \) (and thus unmodified by \( p \)) cannot be statically distinguished from a value signed by \( p \) then \( q \) (and thus unmodified by \( q \)). It also complicates reasoning about confidentiality since encryption order is not reflected statically.

A value of type \( p \quad says \quad q \quad says \quad \tau \) may have been encrypted first with \( q \)’s public key then \( p \)’s, or first with \( p \)’s then \( q \)’s. Successfully decrypting the value requires distinguishing the correct order.

The other two rules we omit are DP-Fun and DP-TFUn, which state that abstractions protect a level if the \( pc \) and return type do.

\[
[\text{DP-Fun}]
\frac{\Pi \vdash \ell \subseteq pc' \quad \Pi \vdash \ell \leq \tau_2}{\Pi \vdash \ell \leq \tau_1 \quad \pc(\Theta,\Gamma) \quad \Pi \vdash \tau_2}
\]

\[
[\text{DP-TFUn}]
\frac{\Pi \vdash \ell \subseteq pc' \quad \Pi \vdash \ell \leq \tau_1 \quad \Pi \vdash \ell \leq \tau_2}{\Pi \vdash \ell \leq \forall X[p'c',\Theta',\Gamma',\Pi'],\tau}
\]

These rules are reasonable in a setting where an attacker cannot observe raw lambda values, and information can be gained from a function value only by applying it. In a distributed setting, however, functions can be sent over channels to potentially malicious hosts, who can directly examine the encoding of an abstraction and potentially learn information.

Every DFLATE typing rule contains a clearance premise \( \Pi \vdash \text{pl} \triangleright pc \) that requires place \( pl \) to act for \( pc \). This ensures a place cannot observe or use data exceeding its authority, as discussed in Section II-B.

For function type \( \bar{\tau}_1 \rightarrow \text{pl} \rightarrow \Gamma \rightarrow \text{pl} \rightarrow \tau_2 \), level \( pc \) is the latent effect of the function (i.e., a lower-bound on the observable side-effects when the function is invoked), \( \Theta \) is the channel environment the function expects, \( \Pi \) is the delegation context the function expects, and \( P \) are the places at which the function make be invoked. Rule DT-LAM shows that the function body must be well-typed for the function’s \( pc \) and channel environment, for every place \( pl \in P \). Function application (rule DT-App) may occur only if the \( pc \) at call site flows to the latent effect of the function, the call-site place is in \( P \), and the channel environment and delegation context of the caller is compatible with the function’s channel environment and delegation context. Note that any place can receive a lambda expression but only those within \( P \) are allowed to invoke it. Channels are not first class, and so the channel environment requirement ensures that the caller has the appropriate channels available and channel variables do not escape via closures. (Type abstraction and application is similar.)

Expression \( \eta \in \varepsilon \) will evaluate \( \varepsilon \) and then protect the result at level \( \ell \) (in implementation, by signing and encrypting it). It has type \( \ell \quad says \quad \bar{\tau} \) (rule DT-UniTm) provided that \( \varepsilon \) is well-typed and the program counter level \( pc \) flows to \( \ell \). Intuitively, this premise is required because program counter level \( pc \) is an upper bound on the decision to execute the statement and on the information available in this computational context (e.g., through variables). Thus, the result of \( \varepsilon \) might be influenced by information at level \( pc \) and must be protected appropriately.

Clearance \( (\Pi \vdash \text{pl} \triangleright pc) \) ensures that place \( pl \) has appropriate integrity to sign the value. Suppose Alice wants to protect a value at Bob’s integrity by evaluating \( \eta_{\text{Alice}} \in \varepsilon \). To type check, it must be the case that \( \Pi \vdash pc \leq \text{Bob} \). By clearance we have \( \Pi \vdash \text{Alice} \triangleright pc \), and thus \( \Pi \vdash \text{Alice}'' \triangleright \text{Bob}'' \), indicating Alice has access to Bob’s signing key. Note that a principal can create protected values that are more confidential than its clearance, e.g., Alice can encrypt values using Bob’s public encryption key without having access to Bob’s decryption key.

Rule DT-Sealed permits protected values to be on nodes that would not have the authority to create them. For instance, even if Alice does not trust Bob, sealed value \( \eta_{\text{Alice}} \in \varepsilon \) is well-typed at Bob if \( v \) is well-typed. Sealed values reflect the security guarantees of cryptographic protection mechanisms: attackers cannot distinguish ciphertexts or forge signatures.

In \( \text{bind} \ x = e \in \varepsilon \), expression \( e \) evaluates to a protected value \( \eta_{\text{Alice}} \in \varepsilon \), and \( x \) is bound to \( v \in \varepsilon \). Rule DT-BindM requires that the type of \( e' \) must protect \( pc \sqcup \ell \) and \( e' \) must type check at a more restrictive level \( pc \sqcup \ell \). Clearance (for expression \( e' \)) ensures that \( pc \sqcup \ell \) does not exceed the place’s authority: the place is trusted to compute on data protected at level \( \ell \). For example, if Bob evaluates \( \text{bind} \ x = e = \eta_{\text{Alice}} \in \varepsilon' \), for \( e' \) to type check it must be the case that \( \Pi \vdash \text{Bob} \triangleright pc \sqcup \text{Alice} \). It follows that \( \Pi \vdash \text{Bob}'' \triangleright \text{Alice}'' \), indicating Bob has access to Alice’s decryption key.

DT-Assume ensures that when the delegation context is extended, there is sufficient integrity to do so. Specifically, when \( r \) delegates to \( q \), \( r \)’s security concerns may be compromised, so that we require that \( pc \Delta \ell \) for \( \Delta \)’s voice of \( r \). Premise \( \Pi \vdash \Delta(q^-) \triangleright \Delta(r^-) \) ensures robustness of the delegation, a desirable property from FLAM [6] that we also enforce.

Figure 7 shows the distributed and TEE typing rules. Rule DT-Spawn limits the channel environment of newly spawned computations to the new channels created by the parent. Only place \( pl \) has access to the send endpoint of \( ch_1 \) and the receive endpoint of \( ch_2 \). Conversely, the newly created process on node \( n \) can use the receive endpoint of \( ch_1 \) and the receive endpoint of \( ch_2 \). Spawned processes \( e \) inherit the delegation context from the parent, but not the variable context. The program counter level of the spawned process \( e_n \), \( pc' \), is at least as restrictive as the \( pc \) of the parent process. This ensures that \( e_n \) does not inadvertently reveal that it was spawned. Premise \( \Pi \vdash pc' \leq \ell' \) ensures the output of the process protects the output of the spawning process. Thus if \( pc' \) is confidential (or untrusted) the output can only be used in confidential (or untrusted) contexts.

DT-Send requires that channel \( ch \) is the send endpoint and that the expression has the correct type. The channel program counter level \( pc_{ch} \) is an upper bound on the confidentiality and integrity of the decision to send the message. This is distinct from the policy used to restrict what information can be sent in messages, which is expressed via type \( \tau \) (see Section II-A for discussion). After the message is sent, execution proceeds with \( e' \) which must type check at a program counter level that is at least as restrictive as \( pc_{ch} \). This ensures that information revealed by successfully sending a message is protected appropriately. In addition to the usual clearance premise, DT-Send also has a channel clearance premise \( \Pi \vdash pl \Delta pc_{ch} \) that...
ensures \( p \) has sufficient authority to use the channel. Finally, notice that whether or not \( e' \) has an output type \( \hat{\tau} \square \), the send term has an output type, ensuring that the continuation-passing discipline is maintained.

Rule DT-RECEIVE is similar to DT-SEND. Here, the channel direction is reversed, and the received value is mapped to variable \( x \) in the continuation. The type of channel messages \( \tau \) and the channel program counter level \( pc_{ch} \) allow the sender and receive to co-ordinate on the security and contents of messages sent over the channel.

Expression TEE\(^t\) \( e \) executes \( e \) in a TEE. Rule DT-TEE requires \( e \) to be closed (and so it cannot use variables to access data from the host node). The channel environment for the TEE is limited to endpoints for the TEE with a channel \( pc \) that protects \( pc \). This restriction ensures two properties. First, all messages into and out of a TEE pass through the TEE’s host, which reflects the operation of current TEE implementations. Second, the restriction to only channels with suitable channel \( pc \)’s ensures that any sends and receives the TEE perform also protect the \( pc \) that launched the TEE. Without this second property, hosts could use TEEs as covert channels to send messages from restrictive contexts to less restrictive ones.

Expression \( e \) executes with the integrity of \( t \) and confidentiality \( pc^- \). Rule DT-TEE differs from all other typing rules in that there is no relation between the integrity of the program counter where the TEE is executed (\( pc^- \)) and the integrity of the program counter within the TEE (\( t^- \)): this is a form of endorsement. Computation principal \( t \) is unique for a given expression \( e \) and the implementation of DFLATE can use remote attestation to ensure that the TEE is executing \( e \), even if the host is untrusted. The typing rule reflects this guarantee by type checking \( e \) at an integrity level unique to that expression. This ensures that the code \( e \) is not altered (e.g., by malware) before the execution. Thus, principals that delegate trust to \( t \) will consider the TEE trusted, but the TEE gains no additional authority over principals that do not delegate to \( t \). The confidentiality level of the information revealed by the TEE is at least that of the host and thus expression \( e \) is type checked with confidentiality \( pc^- \).

A. Examples revisited

Figure 8 presents DFLATE code for the three scenarios in Figure 2. Each program applies function \( f \) to a protected value from Alice (principal \( a \)) and outputs the result to Carol (\( c \)) using Bob (\( b \)) as an intermediate, protecting the output at level \( a \land c \), implying Alice and Carol can read it and both trust its integrity. Despite similar functionality, each program requires different trust relationships between Alice, Bob, and Carol.

Figure 8(a) is an implementation of Figure 2(a), where no cryptographic mechanisms are used. For this program to type check under some delegation context \( \Pi \), it must be the case that Alice trusts Bob and Carol completely. That is, \( \Pi \vdash b \gg a \) and \( \Pi \vdash c \gg a \). Furthermore, Carol must trust Alice and Bob with her integrity, \( \Pi \vdash a^- \gg e^- \) and \( \Pi \vdash b^- \gg e^- \). To see why, first consider the send in line 7. For this term to type check, it must be the case that \( \Pi \vdash a \subseteq a \lor b \lor c \) since, by DT-BINDM, the \( pc \) at this point is at least as restrictive as
the level \( a \) on the protected value \( \eta_a v \), and by DT-Send, this \( pc \) must flow to the channel \( pc \), \( a \lor b \land c \). If \( \Pi \vdash a \subseteq a \lor b \land c \) holds, from the definitions of \( \subseteq \), \( \sqcup \), and \( \cap \) (Section III-A), it follows that \( \Pi \vdash b^+ \triangleright a^\rightarrow \) and \( \Pi \vdash c^\rightarrow \triangleright a^\rightarrow \). A similar argument for the \texttt{recv} at line 3 implies \( \Pi \vdash c^\rightarrow \triangleright \) by definition of \( \sqcup \) and lattice absorption. Therefore, DT-UNITM requires that \( \Pi \vdash a^\rightarrow \land (a \lor b \land c)^\rightarrow \subseteq a \cap c \), which implies that \( \Pi \vdash c^\rightarrow \triangleright a^\rightarrow \) as well as the same integrity relationships implied by Figure 8(a).

Figure 8(c) is an implementation of Figure 2(c). Recall that Bob can influence the incoming and outgoing messages to the enclave \( E \) but the recipients (of messages from enclave) can detect the modifications. Thus it suffices for Alice and Carol to trust the enclave \( E \). The DFLATE program in Figure 8(c) uses a TEE to further reduce the need for mutual trust among Alice, Bob, and Carol. By running the computation in a TEE (identified as \( t \)) hosted on potentially untrusted Bob’s node \( b \) (lines 5 and 6), Alice no longer needs to delegate integrity to Carol since Carol has no influence on the computation. Since the enclave protects the result (\( \xi x \)) at line 9 on behalf of Alice and Carol, they must each delegate integrity to \( t^ \rightarrow \) (Alice’s integrity is also required for the \texttt{assume} at line 7).

\[
\Pi \vdash t^\rightarrow \triangleright a^\rightarrow \quad \Pi \vdash t^\rightarrow \triangleright c^\rightarrow \quad \Pi \vdash a^\rightarrow \triangleright c^\rightarrow
\]

After receiving \( y \) on channel \( ch_b \), the \( pc \) at line 9 is \( (a \lor b \lor t)^\rightarrow \), reflecting Bob’s influence relaying messages. In order to bind \( y \) to \( x \), the enclave must have clearance to read \( a^\rightarrow \), so Alice must delegate her confidentiality to \( t^ \rightarrow \). Since Bob is unable to modify Alice’s message, the enclave endorses Bob’s influence by assuming \( b^+ \triangleright t^\rightarrow \), and allows the result of (\( \xi x \)) to flow to Carol by assuming \( c^\rightarrow \triangleright a^\rightarrow \). These assumptions allow the body of the \texttt{bind} to type check. The below judgments show the assumptions needed inside the TEE, \( (\Pi_{tee} \vdash \text{TEE}) \) is the TEE’s delegation context at lines 8 and 9.

\[
\Pi_{tee} \vdash b^+ \triangleright t^\rightarrow \quad \Pi_{tee} \vdash c^\rightarrow \triangleright a^\rightarrow
\]

Introducing temporary delegations in a TEE using \texttt{assume} is preferable to the delegation contexts required by 8(a) or 8(b) since they are enabled only for the scope of the TEE, and the TEE guarantees that the code is executed as-is.

\footnote{Note this would still be the case if a different channel \( pc \) for \( ch_b \) were chosen. If the channel \( pc \) was \( a^\rightarrow \land (a \lor b)^\rightarrow \) instead of \( a \lor b \lor c \), the clearance requirement for the \texttt{recv} at line 5 would require \( \Pi \vdash b \triangleright a^\rightarrow \land (a \lor b)^\rightarrow \), which implies \( \Pi \vdash b^+ \triangleright t^\rightarrow \).}

\footnote{The absorption laws \( (a \lor b) \land a = a \) and \( (a \land b) \lor a = a \) for all lattice elements \( a \) and \( b \) are algebraic properties of all lattices.
VI. IMPLEMENTATION CONSIDERATIONS

In this section we discuss how DFLATE can be realized using existing cryptographic techniques and TEE mechanisms. Specifically, we identify security principals with public keys, and rely on a public key infrastructure to distribute private keys to appropriately authorized nodes. Our TEE abstraction is carefully designed to be implementable using Intel’s SGX and similar mechanisms; we describe how the remote attestation mechanism can be used by the DFLATE runtime to authenticate TEEs and provision the TEE with appropriate private keys.

A. Cryptography and Representation of Principals

We require that every primitive principal \( n \in \mathcal{N} \) (which includes nodes and computation principals) is associated with a public/private key pair where the public key can be used for encryption and verifying signatures, and the private key can be used for decryption and signing.\(^8\) There are many possible cryptographic schemes that can be used, and we do not require any specific one. We do, however, require infrastructure to store and distribute keys, which we discuss below.

A conjunction or disjunction of principals is represented by a distinct key pair. That is, the cryptographic scheme does not need to support group encryption, group signatures, etc. Instead, our key infrastructure will provide appropriate access control for private keys of conjuncts and disjuncts of principals such as Alice \& Bob and Alice \lor Bob \lor Carol.

Computation principals \( t \in \mathcal{T} \) are identified by a secure hash of (the bytecode representation of) the corresponding computation, and are associated with a key pair. We describe below how a TEE executing the code corresponding to computation principal \( t \) is provisioned with the key pair for \( t \).

Value \( \pi_p v \) represents value \( v \) encrypted and signed by \( p \).\(^9\) The value \( \pi_p v \) is implemented by first encrypting \( v \) (using the appropriate key for \( p^-\)), and then signing the result (using the appropriate key for \( p^-\)). Conversely, evaluation of \( \text{bind } x = \pi_p v \; \text{in } e \) verifies then decrypts. We ensure that places (i.e., nodes and TEEs) that need to perform decryption and signing have access to the appropriate keys; see below.

Delegations (\( p \gg q \)) are run-time values, and are implemented as a statement “\( q \) delegates to \( p \)” that is signed appropriately (i.e., signed by the principal \( \nabla(q) \)).

We assume that node-to-node communication is secure and unobservable, which can be achieved using tools such as Tor [16] or Riffle [27].

B. TEE Implementation

Intel’s SGX is the most widely deployed TEE mechanism, although other TEE implementations exist (e.g., Sanctum [14]). Modulo security vulnerabilities\(^10\) and the need to trust Intel, SGX is suitable for implementing DFLATE’s TEE abstraction.

To start executing \( \text{TEE}^t e \), first an SGX enclave is created with the DFLATE runtime. SGX’s remote attestation mechanism can be used to prove that the enclave is running the DFLATE runtime. Once a remote party knows it is communicating with an instantiation of the DFLATE runtime, the DFLATE runtime can state that it is executing computation \( e \) whose hash is \( t \).

C. DFLATE Runtime

The DFLATE runtime system is responsible for executing DFLATE code, establishing communication channels between nodes, dynamically type-checking values (especially closures) that are received over channels, interacting with the SGX mechanisms and our key management infrastructure, and other tasks required to support execution of DFLATE programs.

The DFLATE runtime needs to be able to execute inside an SGX enclave. Current SGX SDK support is limited to C and C++, so the DFLATE runtime would be most easily implemented in C or C++. However, DFLATE code is represented as bytecode that is executed by the DFLATE runtime. This is necessitated by the ability to send closures over channels, but also simplifies our use of SGX remote attestation protocols.

D. Key Distribution

Computation at a place will need to encrypt, decrypt, sign, and verify data. While encryption and signature verification use the public part of a key pair, decryption and signing require that the place possess appropriate private keys. Fortunately, the clearance premises in the typing rules ensure that a well-typed program at place \( pl \) will need to perform decryptions and signatures only for principals \( p \) such that \( \Pi_{init} \models pl \gg \nabla(p) \) (where \( \Pi_{init} \) is the initial delegation context and \( \nabla(p) \) is the authority required to act on behalf of \( p \)).

When an enclave is created for computation principal \( t \), the enclave does not initially have the private key for \( t \), nor for any other principals \( p \) such that \( \Pi_{init} \models t \gg \nabla(p) \). Thus the enclave must be provisioned with appropriate keys at run time.

To address this, we require a global key master component that can store key pairs and allow nodes and enclaves to acquire the private keys that they are authorized to have. Moreover, the key master creates key pairs as needed for conjuncts and disjuncts of principals. The key master can be implemented as a distributed service to reduce trust in any single entity.

Node \( n \) can request the private key for principal \( p \) from the key master by proving that it is \( n \) (i.e., that it possesses the private key for \( n \)), whereupon the key master will check that \( \Pi_{init} \models n \gg \nabla(p) \), and, if so, securely send \( n \) the private key for \( p \). Since we can conservatively approximate the principals occurring in a computation, node \( n \) could be provisioned with the appropriate private keys before execution, or the implementation could allow \( n \) to request private keys lazily during execution.\(^11\)

However, for a computation principal \( t \), the provisioning of private keys is slightly different, and must be performed at run time. First, the key master and the SGX enclave engage in a series of attestations to ensure that the enclave is running a trusted version of DFLATE. Once the key master confirms that the enclave is running DFLATE, \( t \) is instantiated, and the key master provides the appropriate private keys to the enclave. Once the enclave possesses these keys, it may begin evaluating \( t \).

\(^8\)The public key will likely be a tuple of an encryption key and a verification key, and similarly for the private key.

\(^9\)By contrast, term \( \pi_p e \) will evaluate \( e \) and then encrypt and sign the result.

\(^10\)Recent security vulnerabilities discovered in SGX [40] appear to be implementation issues rather than fundamental concerns.

\(^11\)Care must be taken to ensure that the decision to communicate with the key master does not reveal confidential information.
remote attestation protocol. Once the key master has proof that the enclave is running the DFLATE runtime, it establishes a secure channel with the enclave. The DFLATE runtime then informs the key master it is executing the code corresponding to computation principal \( t \), and requests private keys. Notably, this is the only place that the SGX remote attestation protocol is needed in our proposed DFLATE implementation: secure communication between a node and a TEE can be established using keys for DFLATE principals. Each enclave needs to run the remote attestation protocol only once, with the key master, in order to acquire keys for DFLATE principals.

VII. Security Guarantees

DFLATE’s type system enforces information-flow policies expressed using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees. DFLATE permits expressions using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees. DFLATE permits expressions using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees. DFLATE permits expressions using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees. DFLATE permits expressions using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees. DFLATE permits expressions using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees. DFLATE permits expressions using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees. DFLATE permits expressions using the FLAM principal algebra, and thus enjoys noninterference-based security guarantees.

However, downgrading in DFLATE is carefully controlled and restricted: well-typed \( \text{assume} \) terms can only execute in contexts with sufficient integrity, and endorsement of TEEs reflect measurement and verification of code executing in a TEE. We thus expect that well-typed DFLATE programs satisfy a variety of expressive noninterference-based security guarantees, based on controlled downgrading (e.g., \([12, 25, 8, 9, 13, 3]\)), suitably adapted to be consistent with our threat model IV.

To demonstrate that DFLATE does indeed enjoy noninterference-based properties, we state and prove two variants of noninterference. The first (Theorem 1) uses a “batch-job” model, and holds for confidentiality and integrity. In a batch-job model, inputs are provided at the beginning of execution, and outputs are provided if and when the program terminates \([31]\). For our purposes, we regard the input as being data on one node (thus modeling that node possessing confidential information, or that node containing untrustworthy data) and the output as the final result on a specific node. Even though the execution of a DFLATE program involves nodes interacting with each other over channels, the batch model ensures that ultimate result of the program is appropriately secure.

The second (Theorem 2) uses a stronger observational model where an attacker observes the internal state of a compromised node, but holds only for confidentiality. It does not hold for integrity, due to asymmetry in security guarantees inherent in distributed decentralized applications that use TEEs.

A. Batch-Job Noninterference

We state noninterference with respect to a security level \( H \). Intuitively, for confidentiality, inputs labeled \( H \) (or a more restrictive security level) are regarded as confidential inputs, and we are concerned with ensuring that no information about them is revealed in outputs observable by an attacker, i.e., an entity that can observe outputs at level \( \ell \) where it is not the case that \( H \) can flow to \( \ell \). For integrity, inputs labeled \( H \) are regarded as low-integrity and we want to ensure they do not influence high-integrity outputs (i.e., outputs at level \( \ell \)).

Since we are stating noninterference, we are concerned only with executions where there is no downgrading from \( H \) (or above) to \( \ell \). However, we do not want to rule out all downgrading, as delegations and TEEs are central to DFLATE’s expressiveness. Instead, we assume that for a given process \( \langle n_k, e_k \rangle \) in a well-typed distributed configuration \( \mathcal{D} \), we have a delegation approximation \( \hat{\Pi}_k^\mathcal{D} \) that over-approximates delegations that the process may make during execution.\(^{13}\) See Appendix B for a formal definition.

Suppose all processes in \( \mathcal{D} = \langle n_1, e_1 \rangle \parallel ... \parallel \langle n_m, e_m \rangle \) are well-typed, and the \( i \)th process takes an input value protected by \( H \) (i.e., it has a free variable of type \( H \) says \( \tau \)) and the \( j \)th process produces a value of type \( \ell \) says bool. Moreover, suppose the delegation approximations for the processes ensure that they never downgrade from \( H \) (i.e., \( \hat{\Pi}_k^\mathcal{D} \) permits the same flows from \( H \) as \( \Pi_{\text{init}} \)). If we have two executions of \( \mathcal{D} \) where the input to the \( i \)th process is replaced with different values, then the result of the \( j \)th process will be the same. We state this formally. Proofs of theorems are in Appendix C.

Theorem 1 (Batch-Job Noninterference). Let \( H \) and \( \ell \) be security levels such that \( \Pi_{\text{init}} \not\models H \subseteq \ell \). Let \( \mathcal{D} = \langle n_1, e_1 \rangle \parallel ... \parallel \langle n_m, e_m \rangle \) such that for all \( k \in 1...m \) we have

\[
\Pi_{\text{init}}; \Gamma_k; \Theta_k; n_k; pc_k \vdash e_k; \tau_k,
\]

where \( \tau_j = \ell \) says bool and \( x : H \) says \( \tau \in \Gamma_i \).

Assume that no process downgrades from \( H \), i.e., \( \forall k \in 1...m \). \( \forall \ell'. \Pi_{\text{init}} \not\models H \subseteq \ell' \iff \hat{\Pi}_k^\mathcal{D} \not\models H \subseteq \ell' \). For all \( v_1 \) and \( v_2 \), and all \( z \in \{1, 2\} \) such that

\[
\Pi; \Gamma_i; \Theta_i; n_i; pc_i \vdash v_z : H \text{ says } \tau,
\]

let \( \mathcal{D}_z = \langle n_1, e_1 \rangle \parallel ... \parallel \langle n_i, e_i \{v_z/x\} \rangle \parallel ... \parallel \langle n_m, e_m \rangle \).

If \( \mathcal{D}_1 \Rightarrow^* \langle n_1, e_1 \rangle \parallel ... \parallel \langle n_i, v_j' \rangle \parallel ... \parallel \langle n_m, e_m \rangle \) and \( \mathcal{D}_2 \Rightarrow^* \langle n_1, e_1' \rangle \parallel ... \parallel \langle n_j, v_j' \rangle \parallel ... \parallel \langle n_m, e_m' \rangle \) then \( v_j' = v_j' \).

B. Noninterference for Stronger Observational Model

We also prove a stronger confidentiality noninterference result for an attacker that is able to observe the execution of a process at a compromised node. Intuitively, the attacker sees the sequence of expressions (with stuttering removed, since we ignore timing channels) but cannot see the contents of protected values or TEEs for which the node does not have the decryption key. Recall (from Section VI) that node \( n \) has access to keys for all principals \( p \) such that \( \Pi_{\text{init}} \not\models n \triangleright \nabla(p) \). Thus, the attacker cannot observe the contents of protected value \( \eta_{\ell} \) if \( \Pi_{\text{init}} \not\models n \triangleright \nabla(\ell^*) \), nor see the contents of a TEE for computation principal \( \ell \) if \( \Pi_{\text{init}} \not\models n \triangleright \nabla(\ell^*) \).

The formal definitions of the process trace of node \( n \) and equivalence of process traces are provided in Appendix B. We say that two process traces are equivalent to node \( n \) if \( n \) is unable to distinguish them.

\(^{12}\) Weakening confidentiality is called declassification \([37]\); weakening integrity is called endorsement \([11]\).

\(^{13}\) A straightforward static analysis can be used to compute delegation approximations, but any over-approximation suffices for the security condition.
Our stronger noninterference result is similar to the result of Theorem 1, but holds only for confidentiality.

**Theorem 2 (Compromised-node Noninterference).** Let $H^\rightarrow$ and $n_j$ be security levels such that $\Pi_{init} \not\triangleright n_j \triangleright H^\rightarrow$. Let $D = \langle n_1,\ell_1 \rangle \cdots \langle n_m,\ell_m \rangle$ such that for all $k \in 1..m$ we have

\[\Pi_{init}:\Gamma_k;\Theta_k;n_k;pc_k \vdash e_k : n_k,\]

where $x : H^\rightarrow$ says $\tau \in \Gamma_k$.

Assume that no process downgrades from $H^\rightarrow$, i.e., $\forall k \in 1..m, \forall \ell$. $\Pi_{init} \not\triangleright H^\rightarrow \subseteq \ell \iff \Pi'_k \triangleright H^\rightarrow \subseteq \ell$. For all $v_1$ and $v_2$, and all $z \in \{1,2\}$ such that

\[\Pi;\Gamma_i;\Theta_i;n_i;pc_i \vdash v_z : H^\rightarrow \text{says } \tau,\]

let $D_z = \langle n_1,\ell_1 \rangle \cdots \langle n_i,\ell_i \rangle \langle v_2/x \rangle \cdots \langle n_m,\ell_m \rangle$.

Then for all executions $D_1 \Longrightarrow^* D'_1$ and $D_2 \Longrightarrow^* D'_2$ the process traces of node $n$ are equivalent.

An equivalent of Theorem 2 does not hold for integrity. To see why, consider the following well-typed program that is running on node $n_j$ and outputs $\eta_\ell \text{ true}$ for all inputs $x$.

\[\lambda_{true} \text{ bind } u = x \text{ in } (\lambda_{unit} u)\]

where

\[\lambda_{true} = \lambda(\_;()|\ell,\emptyset,\mathcal{P},\Pi_\lambda).\eta_\ell \text{ true}\]

and

\[\lambda_{unit} = \lambda(\_;\text{bool}|\ell,\emptyset,\mathcal{P},\Pi_\lambda).()\]

Let the input $x$ be controlled by an adversary (say $H^\rightarrow$). Then a high integrity observer (say $\ell'$) can observe the following traces when given the inputs $H^\rightarrow \text{says } true$ and $H^\rightarrow \text{says } false$.

Trace on $S_1$

1. $(n_j,\lambda_{true};\lambda_{unit \text{ true}})$
2. $(n_j,\lambda_{true}();)$
3. $(n_j,\eta_\ell \text{ true})$

Trace on $S_2$

\[\text{case } u \text{ of } \langle n_1,\text{ in}_{j_1}(x),\text{ send } ch() \text{ then } () \rangle \mid \langle n_2,\text{ recv } ch(y) \text{ as } y \text{ in } () \rangle\]

On the left, the attacker node binds low-integrity input $x$ (of type $H^\rightarrow \text{says } \text{bool}$) to $u$ and branches on the value, sending on channel $ch$ in one branch and receiving on channel $ch'$ in the other. On the right, a high-integrity node is engaged in communication with $n_1$ and terminates after receiving a message. For inputs $x = \eta_\ell \text{ in}_{j_1}()$, process $n_2$ terminates, but for $x = \eta_\ell \text{ in}_{j_2}()$ it blocks, thus distinguishing the executions.

The weaker integrity result validates our goal of faithfully expressing the power of attackers to suppress messages without eclipsing the guarantees provided by the cryptographic mechanisms and TEEs. DFLATE cannot protect against the suppression of high-integrity messages, but for all programs that result in high-integrity messages, Theorem 1 guarantees their contents have not been influenced by an attacker.

### VIII. Related Work

#### A. Enclaves and Information Flow

Gollamudi and Chong [25] use enclaves to enforce information flow policies against low-level attackers that can inject arbitrary code into non-enclave parts of a program. DFLATE uses enclaves to enforce confidentiality and integrity against low-level attackers in a distributed setting. Our current noninterference results model passive attackers; we leave more powerful attacker models for future work.

In CFLOW, Fournet et al. [20] compile a sequential imperative program into a distributed program, preserving its security properties using cryptographic techniques. A straightforward security type system enforces noninterference. Fournet and Planul [18] extend CFLOW to use Trusted Platform Modules (TPM) and remote attestation to minimize the TCB while preserving noninterference. DFLATE programs are explicitly distributed at the source level via spawn, send, and recv terms. CFLOW’s communication channels are always public and untrusted whereas DFLATE channels specify separate policies for the presence of a message and its contents. CFLOW’s TPM is trusted and has a fixed integrity level, but TEEs in DFLATE have distinct integrity and confidentiality levels, allowing TEEs to be trusted than their host.

Subramanyan et al. [39] provide a formal foundation for the remote execution of enclaves and use it to prove that two remote enclave executions emit observationally equivalent traces if the attacker provides the same inputs in both executions. DFLATE uses the high-level guarantees of TEEs and proves end-to-end semantic guarantees (noninterference) of distributed applications using enclaves.

#### B. Communication Channels and Cryptography

Zdancewic et al. [42] securely partition a program into subprograms that communicate to simulate the original program. The resulting distributed program prevents read channels, which leak information when a remote read request occurs for a secret reason. DFLATE’s channel pc annotations protect against similar leaks.

Fournet and Rezk [19] use a security type system to enforce the correct use of cryptographic primitives for controlled downgrading. Compiling DFLATE to this language would ensure DFLATE’s monadic abstractions are implemented securely.

Wysteria [36] is a language for writing secure multiparty computation protocols. *Wires* in Wysteria express the idea of data ownership and are comparable to the monadic unit types in DFLATE. However, because Wysteria models communication implicitly through variable binding, it does not detect insecure flows that arise due to explicit communication.

Gazeau et al. [21] enforce confidentiality (but not integrity) of the client data in the cloud. Like our assumptions regarding access to cryptographic keys, their security guarantee relies on honest nodes denying access to attacker nodes.

Fabric [29] and DStar [43] use static and dynamic mechanisms to enforce IFC for distributed programs. They use cryptographic protocols to establish secure channels between nodes, but unlike DFLATE, do not allow high-integrity or secret data to flow through untrusted hosts.
Our channel design is similar to Rafnsson et al. [35], who also distinguish the presence of a message from the contents of a message. DFLATE channel policies are decentralized in that the security of a channel is relative to each principal rather than a centralized security lattice.

IX. Conclusion

DFLATE offers high-level security abstractions for decentralized, distributed applications that use cryptography and trusted execution environments. These abstractions accurately reflect the strengths and limitations of these mechanisms without exposing low-level implementation details. DFLATE is suitable for formal analysis of decentralized distributed applications and as a core programming model for a general-purpose secure distributed programming language. We have formalized DFLATE’s semantics and shown that the type system enforces two variants of noninterference: the stronger variant holds only for confidentiality, reflecting the asymmetry in the security guarantees of the underlying mechanisms.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. 1565387. This material is based upon work supported by the Air Force Office of Scientific Research under award number FA9550-16-1-0351. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation or the United States Air Force.

References


Fig. 9: Complete DFLATE syntax

Fig. 10: Evaluation Contexts (E). Define $T[e]$ as substituting hole (in $T$) with expression $e$.

APPENDIX A

We present the full syntax (Figure 9), evaluation contexts (Figure 10), evaluation rules (Figures 11, 12, 13, 14), robust assumptions (Figure 15), type protection rules (Figure 16), and typing rules (Figures 17, 18, 19).

APPENDIX B

Definition B.1 (Delegation Approximation Contains All Delegations). Let $S$ be the well-typed distributed system

\[ \Pi_{init}; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1 : \tau_1 \quad \cdots \quad \Pi_{init}; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m : \tau_m \]

Also let the process executing on node $p_i$ evaluate to a value. That is,

\[ \langle p_i, e_i \rangle \quad \cdots \quad \langle p_i, e_i \rangle \quad \cdots \quad \langle p_i, e_i \rangle \]

The delegation approximation $\Pi^P$ of the process $\langle p_i, e_i \rangle$ is the union of the set of all delegations in the initial delegation.
\[ \text{[DE-CASE']} \quad pl, D \vdash e \rightarrow e' \quad \text{[DE-CASE1]} \quad pl, D \vdash (\text{case } (inj_1 v) \text{ of } inj_1(x). e_1 | inj_2(x). e_2) \rightarrow e_1[x/v] \quad \text{[DE-CASE2]} \quad pl, D \vdash (\text{case } (inj_2 v) \text{ of } inj_1(x). e_1 | inj_2(x). e_2) \rightarrow e_2[x/v] \]

**Fig. 12:** DFLATE evaluation step for case terms

\[ \text{[DW-APP]} \quad pl, D \vdash (v \text{ where } (a \triangleright b)) v' \rightarrow (v v') \text{ where } (a \triangleright b) \quad \text{[DW-TAPP]} \quad pl, D \vdash (v \text{ where } (a \triangleright b)) \not\tau \rightarrow (v \not\tau) \text{ where } (a \triangleright b) \]

\[ \text{[DW-UNPAIR]} \quad pl, D \vdash \text{proj}_1 ((v_1, v_2) \text{ where } (a \triangleright b)) \rightarrow (\text{proj}_1 (v_1, v_2) \text{ where } (a \triangleright b)) \]

\[ \text{[DW-CASE]} \quad pl, D \vdash (\text{case } (v \text{ where } (a \triangleright b)) \text{ of } inj_1(x). e_1 | inj_2(x). e_2) \rightarrow (\text{case } v \text{ of } inj_1(x). e_1 | inj_2(x). e_2) \text{ where } (a \triangleright b) \]

\[ \text{[DW-UNITM]} \quad pl, D \vdash \eta v \text{ where } (a \triangleright b) \rightarrow (\eta v \text{ where } (a \triangleright b)) \]

\[ \text{[DW-BINDM]} \quad pl, D \vdash \text{bind } x = (v \text{ where } (a \triangleright b)) \text{ in } e \rightarrow (\text{bind } x = v \text{ in } e) \text{ where } (a \triangleright b) \]

\[ \text{[DW-ASSUME]} \quad pl, D \vdash \text{assume } (v \text{ where } (a \triangleright b)) \text{ in } e \rightarrow (\text{assume } v \text{ in } e) \text{ where } (a \triangleright b) \]

\[ \text{[DW-TEE]} \quad pl, D \vdash \text{runTEE}^i (\hat{v} \text{ where } (a \triangleright b)) \rightarrow (\text{runTEE}^i \hat{v}) \text{ where } (a \triangleright b) \]

\[ \text{[DW-HALT]} \quad pl, D \vdash (\hat{v} \text{ where } (a \triangleright b)); \square \rightarrow (\hat{v}; \square \text{ where } (a \triangleright b)) \]

**Fig. 13:** Propagation of where terms

\[ \text{[PAR-STEP]} \quad \langle p_1, e_1, \Pi, m_1 \rangle || \cdots || \langle p_i, e_i, \Pi, m_i \rangle || \cdots || \langle p_m, e_m, \Pi, m_m \rangle \implies \langle p_1, e_1, \Pi, m_1 \rangle || \cdots || \langle p_i, e_i, \Pi, m_i \rangle || \cdots || \langle p_m, e_m, \Pi, m_m \rangle \]

\[ e_i = T\text{[spawn } \oplus (pl, ch_1 | pc_1; \tau_1), ch_2 | pc_2; \tau_2). e \text{ then } e'] \quad e'_i = T\text{[sigma } ch_1[ch_2/v]; e] \]

\[ \text{[PAR-SPAWN]} \quad \langle p_1, e_1 \rangle || \cdots || \langle p_i, e_i \rangle || \cdots || \langle p_m, e_m \rangle \implies \langle p_1, e_1 \rangle || \cdots || \langle p_i, e_i \rangle || \cdots || \langle p_m, e_m \rangle \]

\[ \text{[PAR-SEND-RECV]} \quad \langle p_1, e_1 \rangle || \cdots || \langle p_i, e_i \rangle || \cdots || \langle p_j, e_j \rangle || \cdots || \langle p_m, e_m \rangle \implies \langle p_1, e_1 \rangle || \cdots || \langle p_i, e_i \rangle || \cdots || \langle p_j, e_j \rangle || \cdots || \langle p_m, e_m \rangle \]

**Fig. 14:** DFLATE distributed semantics

\[ \text{[DP-UNIT]} \quad \Pi \vdash \ell \leq \text{unit} \quad \text{[DP-HALT]} \quad \Pi \vdash \ell \leq \hat{\Pi} \]

\[ \text{[DP-PAIR]} \quad \Pi \vdash \ell \leq \tau_1 \quad \Pi \vdash \ell \leq \tau_2 \quad \text{[DP-LALT]} \quad \Pi \vdash \ell \leq \ell' \text{ says } \not\tau \]

**Fig. 16:** Type protection levels

\[ \text{context } \Pi \text{ and those that are assumed during the evaluation of the process } \langle p_1, e_1 \rangle. \]

**Proposition 1.** Let $S$ be the well-typed distributed system from Definition B.1. If $\Pi^D_p$ is the delegation approximation of the process $\langle p_1, e_1 \rangle$, then the following hold.

1) If

\[ \langle p_1, e_1 \rangle || \cdots || \langle p_i, e_i \rangle || \cdots || \langle p_m, e_m \rangle \]

then $\Pi^D_p; \Gamma; \Theta; p_1; p_i \vdash e_i : \tau_i$

2) $\forall \ell, \hat{\ell}. \Pi \not\vdash \ell \leq \ell' \implies \Pi^D_p \not\vdash \ell \leq \ell'$

3) $\forall \ell, \hat{\ell}. \Pi^D_p \not\vdash \ell \leq \ell' \implies \Pi \not\vdash \ell \leq \ell'$

**Fig. 15:** FLAC Robust Assumption

context $\Pi$ and those that are assumed during the evaluation of the process $\langle p_1, e_1 \rangle$. 

context $\Pi$ and those that are assumed during the evaluation of the process $\langle p_1, e_1 \rangle$. 

context $\Pi$ and those that are assumed during the evaluation of the process $\langle p_1, e_1 \rangle$. 

context $\Pi$ and those that are assumed during the evaluation of the process $\langle p_1, e_1 \rangle$.
more confidentiality than the attacker. This precisely models that an attacker, with restricted access to cryptographic keys, cannot distinguish ciphertexts. We lift the observation function to a process executing on node \( n \) as below.

\[
O(n, e, \Pi, A) = \langle n, O(e, \Pi, A) \rangle
\]

We define the trace of a process using the observation function.

**Definition B.3 (Process Trace of a Node).** Let \( S \) be the well-typed distributed system as follows.

\[
(p_1, e_1) || \cdots || (p_i, e_i) || \cdots || (p_m, e_m) \Rightarrow^* (p_1, e_1^k) || \cdots || (p_j, e_j^k) || \cdots || (p_m, e_m^k)
\]

Then process trace of node \( p_j \) with respect to a delegation context \( \Pi \) and an attacker at level \( \ell \), denoted as \( Tr(S, p_j, \Pi, \ell) \), is the sequence of the expressions reduced on that node as observed by the attacker. That is, \( O(p_j, e_j), \Pi, \ell \), . . . , \( O(p_j, e_j^k), \Pi, \ell \) where \( \ell \) is the trace concatenation operator.

Note that a trace may contain consecutive duplicates because it remains the same in those steps when other processes are scheduled to evaluate. The definition of trace deduplication is provided in Appendix C. We assume that the attacker associated with the node \( p_j \). The trace is computed as follows:

\[
Tr(S, p_j, \hat{\Pi}_j, p_j) = O(p_j, e_j), \hat{\Pi}_j, p_j), \ldots, O(p_j, e_j^k), \hat{\Pi}_j, p_j)
\]

where \( \hat{\Pi}_j \) is the delegation approximation of the process running on node \( p_j \). Intuitively, this is an approximation of the actual trace observed by an attacker during the execution of a process on the node \( p_j \). Note that this is safe because it assumes the largest set of delegations that an attacker can influence. Two traces are equivalent if they are equal after applying the observation function and removing the duplicates.

**Definition B.4 (Trace Equivalence).** Two traces, \( T_{r1} \) and \( T_{r2} \), are equivalent, denoted as \( T_{r1} \approx T_{r2} \), if they are equal after removing the duplicates. That is

\[
T_{r1} \approx T_{r2} \iff U(T_{r1}) = U(T_{r2})
\]

We use these formal definitions to instantiate a stronger confidentiality attacker. Our noninterference result against this attacker generalizes the results stated in Theorem 1. Informally, it states that the attacker with limited confidentiality authority cannot distinguish between traces from executions differing in secret inputs. Theorem 2 formally states the noninterference result against this attacker.
\[ \Pi; \Gamma; \theta; p; \ell ; \text{\textbf{DT-UNITM}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \Gamma; \theta; p; \ell ; \text{\textbf{DT-SEALEDM}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \Gamma; \theta; p; \ell ; \text{\textbf{DT-BINDM}} \quad \Pi \vdash \ell \leq \tau \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \Gamma; \theta; p; \ell ; \text{\textbf{DT-ASSUMEm}} \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \Gamma; \theta; p; \ell ; \text{\textbf{DT-WHEREm}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \Gamma; \theta; p; \ell ; \text{\textbf{DT-HALTM}} \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \Gamma; \theta; p; \ell ; \text{\textbf{DT-HALTM2}} \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]

\[ \Pi; \theta; p; \ell ; \text{\textbf{DT-SPAWNM}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \theta; p; \ell ; \text{\textbf{DT-SENDM}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \theta; p; \ell ; \text{\textbf{DT-SENDDELm}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \theta; p; \ell ; \text{\textbf{DT-RECEIVEm}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \theta; p; \ell ; \text{\textbf{DT-TEEm}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \theta; p; \ell ; \text{\textbf{DT-TEEGm}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]
\[ \Pi; \theta; p; \ell ; \text{\textbf{DT-SYS}} \quad \Pi \vdash \ell \quad \Pi \vdash p \vdash \ell \quad \Pi \vdash p \vdash \ell \]

\[ \forall i \in 1 \ldots n \quad \Pi \vdash \theta; i; p; \ell \quad \Pi \vdash \ell \quad \Pi \vdash \ell \quad \Pi \vdash \ell \]

Fig. 18: DFLATE typing rules for secure operations

\[ \forall i \in 1 \ldots n \quad \Pi \vdash \theta; i; p; \ell \quad \Pi \vdash \ell \quad \Pi \vdash \ell \quad \Pi \vdash \ell \quad \Pi \vdash \ell \quad \Pi \vdash \ell \quad \Pi \vdash \ell \]

Fig. 19: DFLATE typing rules for spawn and communication primitives
\[pl, D \vdash e_i \rightarrow e_i' \quad e_j = e_j \quad \{i, j\} = \{1, 2\}\]

\[pl, D \vdash (e_1 \mid e_2) \rightarrow (e_1' \mid e_2')\]

\[v_i \in \{\lambda(x: \tau_i)[pc_i, \Theta_i, \Pi_i]. e_i, \lambda(x: \tau_i)[pc_i, \Theta_i, \Pi_i]. e_i\} \quad i \in \{1, 2\} \quad e_{oi} = \begin{cases} e_i[x \mapsto [v_j]] & \text{if } v_i \text{ has no where} \\ e_i[x \mapsto [v_j]] & \text{o.w} \end{cases}\]

\[pl, D \vdash (v_1 \mid v_2) v \rightarrow (e_{o1} \mid e_{o2})\]

\[v_i \in \{\LambdaX[pc_i, \Theta_i, \Pi_i]. e_i, \LambdaX[pc_i, \Theta_i, \Pi_i]. e_i\} \quad i \in \{1, 2\} \quad e_{oi} = \begin{cases} e_i[X \mapsto \tau] & \text{if } v_i \text{ has no where} \\ e_i[X \mapsto \tau] & \text{o.w} \end{cases}\]

\[pl, D \vdash (v_1 \mid v_2) \tau \rightarrow (e_{o1} \mid e_{o2})\]

\[pl, D \vdash \text{proj}_{x} ((v_{11}, v_{12}) \mid (v_{21}, v_{22})) \rightarrow (v_{11} \mid v_{21})\]

\[v_i \in \{\pi_{t_i}, v', \pi_{t_i}, v' \mid v''\} \quad i \in \{1, 2\} \quad e_{oi} = \begin{cases} [e_i][x \mapsto v_j'] & \text{if } v_i \text{ has no where} \\ [e_i][x \mapsto v_j'] & \text{o.w} \end{cases}\]

\[pl, D \vdash \text{bind } x = (v_1 \mid v_2) \text{ in } e \rightarrow (e_{o1} \mid e_{o2})\]

\[v_i \in \{\pi_{t_i}, v', \pi_{t_i}, v' \mid v''\} \quad i \in \{1, 2\} \quad e_{oi} = \begin{cases} [e_i][x \mapsto v_j'] & \text{if } v_i \text{ has no where} \\ [e_i][x \mapsto v_j'] & \text{o.w} \end{cases}\]

\[pl, D \vdash \text{bind } x = (v_1 \mid v_2) \text{ in } e \rightarrow (e_{o1} \mid e_{o2})\]

\[v_k = \{\text{inj}_1 v_k, \text{inj}_1 v_k \mid v_k\} \quad k \in \{1, 2\} \quad \{i, j\} = \{1, 2\} \quad e_{ok} = \begin{cases} [e_i][x \mapsto v_k] & \text{if } v_k \text{ has no where} \\ [e_i][x \mapsto v_k] & \text{o.w} \end{cases}\]

\[pl, D \vdash \text{case } \text{inj}_1 v_1 \mid \text{inj}_1 v_2 \text{ of inj}_1(x). e_1 \mid \text{inj}_2(x). e_2 \rightarrow (e_{o1} \mid e_{o2})\]

\[pl, D \vdash \text{assume } (v_1 \mid v_2) \text{ in } e \rightarrow ([e_1] \mid [e_2] \text{ where } v_2)\]

\[\hat{v} ::= \ldots (\hat{v} \mid \hat{v})\]

\[e ::= \ldots (e \mid e)\]

**APPENDIX C**

**DFlATE Noninterference Proofs**

We use Pottier and Simonet [33] technique to prove noninterference. At a high-level, the techniques involves extendin the calculus to have bracketed expressions and values that represent two different executions. Proving noninterference for DFlATE program entails proving that the individual projections of the final bracketed values are equal for inputs that are confidential and have less integrity.

Figure 20 shows evaluation extensions. Nesting of bracketed expressions isn’t allowed. Figure 22 defines projection. Typing extensions shown in Figure 23.
Fig. 21: DFLATE Evaluation extensions for system
\[ [e]_i = \begin{cases} 
\hat{v}_i & \text{if } e = (\hat{v}_1 \mid \hat{v}_2) \\
x & \text{if } e = x \\
[e]_i \mid [e']_i & \text{if } e = e \mid e' \\
\langle [e_1]_i, [e_2]_i \rangle & \text{if } e = \langle e_1, e_2 \rangle \\
\eta \ell [e]_i & \text{if } e = \eta \ell e \\
[e]_i \tau & \text{if } e = e \tau \\
\text{proj}_j [e]_i & \text{if } e = \text{proj}_j e \\
\text{case } [v]_i \text{ of inj}_1(x). [e_1]_i \mid \text{inj}_2(x). [e_2]_i & \text{if } e = \text{case } v \text{ of inj}_1(x). e_1 \mid \text{inj}_2(x). e_2 \\
\text{bind } x = [e]_i \text{ in } [e']_i & \text{if } e = \text{bind } x = e \text{ in } e' \\
\text{assume } [e]_i \text{ in } [e']_i & \text{if } e = \text{assume } e \text{ in } e' \\
\text{send } ch [e]_i \text{ then } e_{\text{sk}} & \text{if } e = \text{send } ch \text{ e then } e_{\text{sk}} \\
\text{recv } ch \text{ as } x \text{ in } [e']_i & \text{if } e = \text{recv } ch \text{ as } x \text{ in } e' \\
\text{\bullet} & \text{if } e = (\bullet \mid e) \text{ and } i = 1 \\
\text{or } e = (e \mid \bullet) \text{ and } i = 2 & \text{otherwise} \\
e & \text{otherwise} 
\end{cases} \]

Fig. 22: Projection for bracketed expressions. \textbullet\ denotes empty expression.

\[
\text{[DT-BRACKET]} \quad \Pi \vdash (H^\leq \sqcup pc) \subseteq pc' \quad \Pi; \Gamma; \Theta; p; pc' \vdash e_1 : \tau \\
\Pi; \Gamma; \Theta; p; pc \vdash e_2 : \tau \\
\Pi \vdash H^\leq \tau \\
e_1 \text{ is not a value \lor } e_2 \text{ is not a value} \\
\Pi; \Gamma; \Theta; p; pc \vdash (e_1 \mid e_2) : \tau
\]

\[
\text{[DT-BRACKET-WHERE]} \\
\Pi; \Gamma; \Theta; p; pc \vdash \hat{v}_1 \text{ where } \hat{v}_1' : \tau \\
\Pi; \Gamma; \Theta; p; pc \vdash \hat{v}_2 \text{ where } \hat{v}_2' : \tau \\
\Pi \vdash H^\leq \tau \\
\Pi; \Gamma; \Theta; p; pc \vdash (\hat{v}_1 \mid \hat{v}_2) : \tau
\]

\[
\text{[DT-BRACKET-VALUES]} \\
\Pi \vdash H^\leq \tau \\
\Pi; \Gamma; \Theta; p; pc \vdash \hat{v}_1 : \tau \\
\Pi; \Gamma; \Theta; p; pc \vdash \hat{v}_2 : \tau \\
\hat{v}_1 \text{ not where term } \hat{v}_2 \text{ not where term} \\
\Pi; \Gamma; \Theta; p; pc \vdash (\hat{v}_1 \mid \hat{v}_2) : \tau
\]

Fig. 23: DFLATE Typing Extensions

22
A. Adequacy

We prove that the bracketed semantics are adequate – sound and complete. By soundness, we mean that given a step in the bracketed execution, then at least one of the left or right projections take one or more steps such that they are in relation with the bracketed execution. By completeness, we mean that given a left and right execution, we can construct a corresponding bracketed execution. We now prove the soundness of the bracketed semantics.

Lemma 1 (Soundness for Single Thread). If \( p, D \vdash e \rightarrow e' \) then \( p, D \vdash [e]_k \rightarrow^* [e']_k \) for some \( k \in \{1, 2\} \).

Proof. Inducting on the step relation. Interesting cases are described below.

**Case BD-STEP:** Since \( p, D \vdash (e_1 | e_2) \rightarrow (e'_1 | e'_2) \), we have that \( p, D \vdash e_k \rightarrow e'_k \). Since \( e_k = [e]_k \) and \( e'_k = [e']_k \), we have that \( p, D \vdash [e]_k \rightarrow [e']_k \).

**Case BD-APP:** First consider the case when there is no where term surrounding the function. That is, given \( p, D \vdash (\lambda(x:τ_1)[pc_1, Θ_1, P_1, Π_1].e_1 | \lambda(x:τ_2)[pc_2, Θ_2, P_2, Π_2].e_2) v \rightarrow (e_1[x \mapsto [v]_1] | e_2[x \mapsto [v]_2]) \). For \( k \in \{1, 2\} \), we have to prove that

\[
p, D \vdash (\lambda(x:τ_k)[pc_k, Θ_k, P_k, Π_k].e_k) v_k \rightarrow e_k[x \mapsto [v]_k]
\]

This is straightforward from DE-APP. Thus both left and right executions take a step.

Next, we consider the case in which the function is surrounded by where terms. Without loss of generality, let

\[
p, D \vdash ((\lambda(x:τ_1)[pc_1, Θ_1, P_1, Π_1].e_1) v' \rightarrow ((e_1[x \mapsto [v]_1]) where v'_1 | e_2[x \mapsto [v]_2]) \]

We have to prove that

\[
p, D \vdash (\lambda(x:τ_1)[pc_1, Θ_1, P_1, Π_1].e_1) v \rightarrow (e_1[x \mapsto [v]_1] where v'_1 \rightarrow e_1[x \mapsto [v]_1] where v'_1
\]

The first step relation follows from W-APP and DE-APP. The second step relation is straightforward from DE-APP. Hence proved.

**Case BD-TAPP:** Similar to above case. Straightforward from DE-TAPP.

**Case BD-UNPAIR:** Straightforward from DE-UNPAIR.

**Case BD-BINDM1:** Straightforward from DE-BINDM.

**Case BD-BINDM3:** Same as above.

**Case BD-CASE:** Straightforward from DE-CASE1 and DE-CASE2.

**Case BD-ASSUME:** Straightforward from DE-ASSUME

Lemma 2 (Soundness for System). If \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, e_i \rangle \| \cdots \| \langle p_n, e_m \rangle \rightarrow^* \langle p_1, e'_1 \rangle \| \cdots \| \langle p_i, e'_i \rangle \| \cdots \| \langle p_n, e'_m \rangle \) then \( \langle p_1, [e_1]_k \rangle \| \cdots \| \langle p_i, [e_i]_k \rangle \| \cdots \| \langle p_n, [e_m]_k \rangle \) \rightarrow \langle p_1, [e'_1]_k \rangle \| \cdots \| \langle p_i, [e'_i]_k \rangle \| \cdots \| \langle p_n, [e'_m]_k \rangle \) for \( k \in \{1, 2\} \).

Proof. We induct on the system step relation.

**Case PAR-STEP:** From the premises of PAR-STEP, we have that \( p_i, D_{init} \vdash e_i \rightarrow e'_i \). Invoking soundness for single process (Lemma 1), we have that \( p_i, D_{init} \vdash [e_i]_k \rightarrow [e'_i]_k \) for some \( i \in \{1 \ldots m\} \) and for all \( k \in \{1, 2\} \). Thus, we have

\[
\langle p_1, [e_1]_k \rangle \| \cdots \| \langle p_i, [e_i]_k \rangle \| \cdots \| \langle p_n, [e_m]_k \rangle \rightarrow \langle p_1, [e'_1]_k \rangle \| \cdots \| \langle p_i, [e'_i]_k \rangle \| \cdots \| \langle p_n, [e'_m]_k \rangle.
\]

**Case PAR-SPAWN:** Straightforward from the projection of premises.

**Case PAR-SEND-RECv:** Straightforward from the projection of premises.

**Case BD-BP-STEP-L:** If \( n = m \) and \( j = i \), the case is a straightforward application of Lemma 1 (soundness of single process).

If \( n = m \) and \( j \neq i \), then from the premise, we have that \( \langle p_i, [e_i]_1 \rangle \| \cdots \| \langle p_j, [e_j]_1 \rangle \rightarrow \langle p_i, [e'_i]_1 \rangle \| \cdots \| \langle p_j, [e'_j]_1 \rangle \) where \( [e_i]_1 = e_i_1 \). Similarly, we have that \( \langle p_i, [e_i]_2 \rangle \| \cdots \| \langle p_j, [e_j]_2 \rangle \rightarrow \langle p_i, [e'_i]_2 \rangle \| \cdots \| \langle p_j, [e'_j]_2 \rangle \) where \( [e_1]_2 = e_2 \). Remaining terms are unchanged.

If \( n \neq m \) then remaining terms unchanged, we have that \( \langle p_i, [e_i]_1 \rangle \rightarrow \langle p_i, [e'_i]_1 \rangle \| \cdots \| \langle p_n, [e'_m]_1 \rangle \) and \( \langle p_i, [e_i]_2 \rangle \rightarrow \langle p_i, [e'_i]_2 \rangle \| \cdots \| \langle p_n, [e'_m]_2 \rangle \). Hence proved.

**Case BD-BP-STEP-R:** Proof similar to above case.

**Case BD-BP-SPAWN-L:** Proof similar to the last case \( (n \neq m) \) of BD-BP-STEP-L.

**Case BD-BP-SPAWN-R:** Proof similar to the last case \( (n \neq m) \) of BD-BP-STEP-L except that we now reason for taking the step on the right execution.

**Case BD-BP-SEND-RECv-L:** Remaining terms unchanged, we have that \( \langle p_i, T_i[\text{send } ν as \ x in e_i] \rangle \rightarrow \langle p_i, T_i[e_{sn}] \rangle \) \| \( \langle p_j, T_i[\text{recv } ν as \ x in e_i] \rangle \rightarrow \langle p_j, T_i[e_{sn}[x \mapsto ν]] \rangle \). The right project of the process running on \( p_i \) and \( p_j \) remains unchanged. Hence proved.
Case BD-PAR-SEND-RECV-R: Similar to above case but the right projection takes a step and left projection remains unchanged.
Case BD-PAR-SEND-RECV-L: Similar to the case BD-PAR-SEND-RECV-L.
Case BD-PAR-RECVR-SEND-R: Similar to the case BD-PAR-SEND-RECV-L.

Before proving completeness, we prove if the bracketed term is stuck then either left or right execution are stuck.

**Lemma 3** (Stuck Expressions for Single Thread). If \( \langle p, e \rangle \) gets stuck then \( \langle p, [e]_i \rangle \) is stuck for some \( i \in \{1, 2\} \).

**Proof.** We prove by induction on the structure of \( e \) that if \( \langle p, e \rangle \) gets stuck then \( \langle p, [e]_i \rangle \) is stuck for some \( i \in \{1, 2\} \).

**Case \( \hat{v} \):** By assumption, \( e \) is not a value.
**Case \( x \):** No reduction for a variable. Hence \( [x]_i \) is stuck as well.
**Case \( e' \):** Since BD-APP and DE-APP are not applicable, it follows that \( e \) is not of the form \( \lambda (x: \tau)[pc', \Theta', \mathcal{P}, \Pi]^*, e_1 \mid \lambda (x: \tau)[pc', \Theta', \mathcal{P}, \Pi]^*, e_2 \) or \( \lambda (x: \tau)[pc', \Theta', \mathcal{P}, \Pi]^*, e \). Thus \([e]_i \) is stuck as well.
**Case \( \eta e \):** Since \( e \) is stuck, applying induction hypothesis it follows that \([e]_i \) is also stuck and so \([\eta e]_i \) is also stuck.

**Case \( \text{proj} \), \( \text{inj} \):** Similar to the above case.
**Case \( \tau \):** Since BD-TAPP and DE-TAPP are not applicable, it follows that \( e \) is not of the form \((v_1 \mid v_2) \) or \( \Lambda X[pc, \Theta, \mathcal{P}, \Pi]^*, e \).
Thus \([e]_i \) \( \tau \) is stuck as well.

**Case \( e \text{ of inj}_{j}(x), e_1 \mid \text{inj}_{j}(x), e_2 \):** Since BD-CASE and DE-CASE are not applicable, it follows that \( e \) is not of the form \((\text{inj}_{j} v_1 \mid \text{inj}_{j} v_2) \) or \( \text{inj}_{j} v \).
It follows that \([e]_i \) \( \text{inj}_{j}(x), e_1 \mid \text{inj}_{j}(x), e_2 \) is also stuck.

**Case \( \text{bind} \ x = v \text{ in } e' \):** Similar to the above case.
**Case \( \text{assume } e \text{ in } e' \):** Similar to the above case.

**Case \( \text{TEE}^t \):** Cannot get stuck.

**Case \( \text{runTEE}^t e \):** Applying induction to \( e \), we have that \( \text{runTEE}^t e \) is stuck for some \( i \in \{1, 2\} \).

**Case \( \eta e \):** Cannot get stuck.

**Case \( \text{Bracket} \):** \( e = (e_1 \mid e_2) \). The only way this gets stuck is if both \( e_1 \) and \( e_2 \) get stuck. This is a contradiction.

**Case Other:** Remaining expressions do not take a step (single thread step relation \( \rightarrow \)).

**Lemma 4** (Stuck Expressions for System). If \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_n, e_n \rangle \) gets stuck then the configuration \( \langle p_1, [e_1]_k \rangle \| \cdots \| \langle p_i, [e_i]_k \rangle \| \cdots \| \langle p_n, [e_n]_k \rangle \) for some \( k \in \{1, 2\} \).

**Proof.** Induction on the structure of the system configuration.

**Case \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, [\text{send } \nu \text{ v then } e_{sk}] \rangle \| \cdots \| \langle p_n, e_n \rangle \):** There is no matching \( T'[\text{recv } \nu \text{ as x in e}] \) on any other process, otherwise it would have taken a step using PAR-SEND-RECV. Thus it is stuck for all \( k \in \{1, 2\} \).

**Case \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, [\text{recv } \nu \text{ as x in e}] \rangle \| \cdots \| \langle p_n, e_n \rangle \):** There is no matching \( T'[\text{recv } \nu \text{ as x in e}] \) on any other process, otherwise it would have taken a step using BD-PAR-SEND-RECV-L. Thus it is stuck for \( k = 1 \).

**Case \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, [\text{recv } \nu ] \rangle \| \cdots \| \langle p_n, e_n \rangle \):** There is no matching \( T'[\text{recv } \nu ] \) on any other process, otherwise it would have taken a step using BD-PAR-SEND-RECV-L. Thus it is stuck for \( k = 1 \).

**Case \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, [\text{send } \nu \text{ v then e}_{sk}] \rangle \| \cdots \| \langle p_n, e_n \rangle \):** There is no matching \( T'[\text{send } \nu \text{ v then e}_{sk}] \) on any other process, otherwise it would have taken a step using BD-PAR-SEND-RECV-R. Thus \( k = 2 \).

**Case \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, [\text{recv } \nu ] \rangle \| \cdots \| \langle p_n, e_n \rangle \):** There is no matching \( T'[\text{recv } \nu ] \) on any other process, otherwise it would have taken a step using BD-PAR-SEND-RECV-R. Thus \( k = 2 \).

**Case \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, [\text{send } \nu \text{ v then e}_{sk}] \rangle \| \cdots \| \langle p_n, e_n \rangle \):** There is no matching \( T'[\text{send } \nu \text{ v then e}_{sk}] \) on any other process, otherwise it would have taken a step using BD-PAR-SEND-RECV-R. Thus \( k = 2 \).

**Case \( \text{Spawn} \):** Always takes a step and cannot be stuck.

**Case Other:** We have that all processes are stuck. Invoking Lemma 3 on each process, we have that each process is stuck for some \( k \in \{1, 2\} \).

We now prove the completeness of the bracketed semantics.

**Lemma 5** (Completeness). If \( \langle p_1, [e_1]_k \rangle \| \cdots \| \langle p_i, [e_i]_k \rangle \| \cdots \| \langle p_n, [e_n]_k \rangle \Rightarrow^* \langle p_1, [e'_1]_k \rangle \| \cdots \| \langle p_i, [e'_i]_k \rangle \| \cdots \| \langle p_n, [e'_n]_k \rangle \) for all \( k \in \{1, 2\} \) then there exists a \( \hat{v}_i \) such that \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, e_i \rangle \| \cdots \| \langle p_n, e_n \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \| \cdots \| \langle p_i, \hat{v}_i \rangle \| \cdots \| \langle p_n, e'_n \rangle \).
Proof. From the rules in Figure 20, the brackets are always propagated outside, so they can only be applied finite number of times. If the system is stuck, then from Lemma 4, we have that either left or right executions are stuck. This is contradicting our assumption. Thus the system will not get stuck. Hence it must terminate to some value.

B. Proofs for Non-Interference

Before proving Theorem 1 and Theorem 2, we prove few supporting lemmas required for proving the type preservation.

Lemma 6 (Closed Values in Send). Let $\Pi; \emptyset; p_1; p_2; \ldots; p_n; \psi_1; \psi_2; \ldots; \psi_m \vdash e_1: \tau_1 \mid \cdots \mid e_i: \tau_i \mid \cdots \mid \Pi; \emptyset; \Theta; p_1; p_2; \ldots; p_n; \psi_1; \psi_2; \ldots; \psi_m \vdash e_i: \tau_i \mid \cdots \mid \Pi_{m}; \emptyset; \Theta_{m}; p_{m_1}; p_{m_2}; \ldots; p_{m_n}; \psi_{m_1}; \psi_{m_2}; \ldots; \psi_{m_n} \vdash e_{m_i}: \tau_{m_i}$. If $\langle p_i, e_i \rangle \mid \cdots \mid \langle p_i, e_i \rangle \mid \cdots \mid \langle p_i, e_i \rangle \Rightarrow \ast \langle p_i, e_i \rangle \mid \cdots \mid \langle p_i, \Pi_{m_i} [\text{send} \nu v \text{ then } e_{m_i}] \rangle \mid \cdots \mid \langle p_i, e_i \rangle \rangle$ then $\emptyset; \emptyset; p_i; p_i' \vdash e: \tau$.

Proof. The only case where unbound variables appear is in closures. However, the top level program is closed and so all variables are $\beta$-substituted before getting reduced to $v$.

Lemma 7 (Clearance). Let $\Pi; \Gamma; \Theta; p; p_c \vdash e: \tau$. Then $\Pi \vdash p \equiv p_c$.

Proof. Proof is by straightforward induction on the typing judgment.

Lemma 8 (Robust Assumption). If $\Pi \vdash p_c \equiv \nabla(b)$, then $\Pi \cdot (a \equiv b) \vdash p_c \equiv \nabla(b)$ for any $a, b \in \mathcal{L}$.

Lemma 9 (Robust Protection). If $\Pi \vdash p_c \equiv \tau$, then $\Pi \cdot (a \equiv b) \vdash p_c \equiv \tau$ for any $a, b \in \mathcal{L}$.

Lemma 10 (Π Extension). If $\Pi; \Gamma; \Theta; p; p_c \vdash e: \tau$ then $\Pi \cdot (p \equiv q); \Gamma; \Theta; p; p_c \vdash e: \tau$ for any $p, q \in \mathcal{L}$.

Proof. Proof is by induction on the derivation of the typing judgment.

Case DT-VAR: Straightforward from the corresponding typing judgment.

Case DT-UNIT: Straightforward from the corresponding typing judgment.

Case DT-DEL: Straightforward from the corresponding typing judgment.

Case DT-LAM: Straightforward from the corresponding typing judgment.

Case DT-APP: Straightforward from the corresponding typing judgment.

Case DT-TAPP: Straightforward from the corresponding typing judgment.

Case DT-PAIR: Straightforward from the corresponding typing judgment.

Case DT-UNPAIR: Straightforward from the corresponding typing judgment.

Case DT-INJ: Straightforward from the corresponding typing judgment.

Case DT-CASE: Straightforward from the corresponding typing judgment.

Case DT-UNITM: Straightforward from the corresponding typing judgment.

Case DT-BINDM: Straightforward from the corresponding typing judgment.

Case DT-ASSUME: Given $\Pi; \Gamma; \Theta; p; p_c \vdash \text{assume } e \text{ in } e': \tau$. From the premises,

$$\Pi; \Gamma; \Theta; p; p_c \vdash e: (a \equiv b) \quad (1)$$

$$\Pi \vdash p_c \equiv \nabla(b) \quad (2)$$

$$\Pi \vdash \nabla(a) \equiv \nabla(b^-) \quad (3)$$

$$\Pi \cdot (a \equiv b); \Gamma; \Theta; p; p_c \vdash e': \tau \quad (4)$$

Applying inductive step to (1) and (4), we have $\Pi \cdot (a \equiv b); (p \equiv q); \Gamma; \Theta; p; p_c \vdash e': \tau$ and $\Pi \cdot (p \equiv q); \Gamma; \Theta; p; p_c \vdash e: (a \equiv b)$. Applying Lemma 8 to premises (C-B) and (C-B) we have $\Pi \cdot (p \equiv q) \equiv p_c \equiv \nabla(b)$ and $\Pi \cdot (p \equiv q) \equiv \nabla(a) \equiv \nabla(b^-)$.

Hence proved.

Case DT-WHERE: Similar to the proof of case DT-ASSUME.

Case DT-BRACKET: Applying induction to the premises of DT-BRACKET gives us that $\Pi \cdot (a \equiv b); \Gamma; \Theta; p; p_c \vdash (e_1 | e_2): \tau$.

Case DT-BRACKET-VALUES: Similar to above case.

Case DT-SPAWN: Applying induction to premises, we have the conclusion.

Case DT-SEND: Applying induction to premises, we have the conclusion.

Case DT-SEEKDEL: Applying induction to premises, we have the conclusion.

Case DT-RECEIVE: Applying induction to premises, we have the conclusion.

Case DT-TEE: Applying induction to premises, we have the conclusion.

Case DT-TEEG: Applying induction to premises, we have the conclusion.

Case DT-HALT: Applying induction to premises, we have the conclusion.

Case DT-HALT2: Applying induction to premises, we have the conclusion.

□
The following lemma is required to prove the type preservation. It says that a expression \( e \) well-typed at \( pc \) is still well-typed at a reduced \( pc' \) that satisfies the clearance.

**Lemma 11** (PC Reduction). Let \( \Pi; \Gamma; \Theta; p; pc \vdash e : \tau \). For all \( pc, pc' \), such that \( \Pi \vdash pc' \subseteq pc \) and \( \Pi \vdash p \gg pc' \), then \( \Pi; \Gamma; \Theta; p; pc' \vdash e : \tau \) holds.

**Proof.** Proof is by induction on the derivation of the typing judgment.

**Case DT-VAR:** Straightforward from the corresponding typing judgment.

**Case DT-UNIT:** Straightforward from the corresponding typing judgment.

**Case DT-DEL:** Straightforward from the corresponding typing judgment.

**Case DT-CHANNEL:**

**Case DT-LAM:** Straightforward from the corresponding typing judgment.

**Case DT-APP:** Given, \( \Pi; \Gamma; \Theta; p; pc \vdash e : e' : \tau \). From DT-App, we have

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; pc \vdash e : \tau_1 & \quad \text{PC}'' \Theta', P, \Pi \quad \tau_2 \quad \text{(5)} \\
\Pi; \Gamma; \Theta; p; pc \vdash e' : \tau_1 & \quad \text{(6)} \\
\Pi \vdash pc \subseteq pc'' & \quad \text{(7)} \\
\Pi \vdash p \gg pc & \quad \text{(8)} \\
\Theta \mid \text{dom}(\Theta') = \Theta' & \quad \text{(9)} \\
\forall (p \gg q) \in \Pi'. \, \Pi \vdash p \gg q & \quad \text{(10)}
\end{align*}
\]

Since \( \Pi \vdash p \gg pc' \), Applying induction to the premises we have \( \Pi; \Gamma; \Theta; p; pc' \vdash e : \tau_1 \) and \( \Pi; \Gamma; \Theta; p; pc \vdash e' : \tau_1 \). From R-TRANS, we have \( \Pi \vdash pc' \subseteq pc'' \). Hence we have all the premises.

**Case DT-UNITM:** Straightforward from the corresponding typing judgment.

**Case DT-APP:** Similar to DT-App case.

**Case DT-PAR:** Straightforward from the corresponding typing judgment.

**Case DT-UNPAIR:** Straightforward from the corresponding typing judgment.

**Case DT-APPL:** Straightforward from the corresponding typing judgment.

**Case DT-ASSUME:** Straightforward from the corresponding typing judgment.

**Case DT-ASSME:** Straightforward from the corresponding typing judgment.

**Case DT-BINDM:** Before applying induction to the premises, we have to prove that \( \Pi \vdash p \gg pc' \cup \ell \). Applying clearance (Lemma 7) to the premise \( \Pi; \Gamma, x : \tau'; \Theta; p; pc \cup \ell \vdash e' : \tau \), we have that \( \Pi \vdash p \gg pc \cup \ell \) and this implies \( \Pi \vdash pc' \cup \ell \subseteq pc \cup \ell \). Hence we can apply induction to the premise and the rest of the proof os straight forward.

**Case DT-ASSUME:** Given, \( \Pi; \Gamma; \Theta; p; pc \vdash \text{assume } e \in e' : \tau \). From DT-ASSUME, we have

\[
\begin{align*}
\Pi; \Gamma; \Theta; pl; pc \vdash e : (p \gg q) & \quad \text{(11)} \\
\Pi \vdash pc \gg \nabla(q) & \quad \text{(12)} \\
\Pi \vdash \nabla(p^-) \gg \nabla(q^-) & \quad \text{(13)} \\
\Pi \cdot (p \gg q); \Theta; p; pc \vdash e' : \tau & \quad \text{(14)} \\
\Pi \vdash p \gg pc & \quad \text{(15)}
\end{align*}
\]

Applying inductive hypothesis to (11) and (14) we have \( \Pi; \Gamma; \Theta; p; pc' \vdash e : (p \gg q) \). Applying inductive hypothesis to (14), we have \( \Pi \cdot (p \gg q); \Theta; p; pc' \vdash e' : \tau \). Since \( \Pi \vdash pc' \subseteq pc \), we have \( \Pi \vdash pc' \gg \nabla(q) \). Combining, we have all the premises for DT-ASSUM and thus

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; pc' \vdash \text{assume } e \in e' : \tau
\end{align*}
\]

**Case DT-WHERE:** Given, \( \Pi; \Gamma; \Theta; p; pc \vdash e \text{ where } v : \tau \). From DT-WHERE, we have

\[
\begin{align*}
\Pi; \Gamma; \Theta; pl; pc \vdash v : (p \gg q) & \quad \text{(16)} \\
\Pi \vdash pc \gg \nabla(q) & \quad \text{(17)} \\
\Pi \vdash \nabla(p^-) \gg \nabla(q^-) & \quad \text{(18)} \\
\Pi \cdot (p \gg q); \Gamma; \Theta; pc \vdash e : \tau & \quad \text{(19)}
\end{align*}
\]

Applying inductive hypothesis to (16) and (19) (and weakening delegation context (Lemma 10)), we have \( \Pi; \Gamma; \Theta; p; pc' \vdash v : (p \gg q) \) and \( \Pi \cdot (p \gg q); \Gamma; \Theta; pc' \vdash e : \tau \). Using R-TRANS on (17), we have \( \Pi \vdash pc' \gg \nabla(q) \) and so \( \Pi \vdash pc' \gg \nabla(q) \).
Combining, we have all the premises for \texttt{T-WHERE} and thus
\[ \Pi; \Gamma; \Theta; p_i; \text{pc} \vdash e \text{ where } v : \tau \]

**Case DT-TEE:** Given \( \Pi; \Gamma; \Theta; p; \text{pc} \vdash \text{TEE}^t e : \tau \). From the premise, we have
\[ \Pi; \emptyset; \Theta; t; t^t \wedge \text{pc}^- \vdash e : \tau \]

Before applying induction to the premises, we have to prove that \( \Pi \vdash t \succ t^t \wedge \text{pc}^- \). From clearance (Lemma 7, we have that \( \Pi \vdash t \succ t^t \wedge \text{pc}^- \). Combined with \( \Pi \vdash \text{pc} \subseteq \text{pc} \), we have that
\[ \Pi \vdash t \succ t^t \wedge \text{pc}^- \]

We now use straightforward induction.
**Case DT-TEEG:** Similar to above case.
**Case DT-HALT:** Applying induction to premises, we have the conclusion.
**Case DT-HALT2:** Applying induction to premises, we have the conclusion.

**Case DT-RECEIVE:** Given \( \Pi; \Gamma; \Theta; pl; \text{pc} \vdash \text{recv ch as } x \text{ in } e^t : \tau \). We therefore have the premises
\[
\Pi; \Gamma; \Theta; pl; \text{pc} \vdash ch : \text{chan}_{p \rightarrow q} \text{pc}_{ch} \tau \\
\Pi; \Gamma; x : \tau; \Theta; p; \text{pc}'' \vdash e : \tau' \\
\Pi \vdash \text{pc} \subseteq \text{pc}'' \\
\Pi \vdash \text{pc}_{ch} \subseteq \text{pc}'' \\
\Pi \vdash \text{pc} \subseteq \text{pc}_{ch} \\
\Pi \vdash p \succ \text{pc} \\
\Pi \vdash p \succ \text{pc}_{ch}
\]

From DT-CHAN, we have
\[ \Pi; \Gamma; \Theta; p; \text{pc} \vdash \text{chan}_{p \rightarrow q} \text{pc}'' \tau \]

Using R-TRANS, from (22) and (24), we have
\[ \Pi \vdash \text{pc} \subseteq \text{pc}'' \]

and
\[ \Pi \vdash \text{pc} \subseteq \text{pc}_{ch} \]

Thus \( \Pi; \Gamma; \Theta; p; \text{pc} \vdash \text{recv ch as } x \text{ in } e^t : \tau \)

**Case DT-SEND:** Proof similar to above case

**Case DT-SENDDEL:** Proof similar to above case except that values can be well-typed under empty delegation set.

**Case DT-SPAWN:** Given \( \Pi; \Gamma; \Theta; p; \text{pc} \vdash \text{spawn } @q (pl; \text{pc}_1[pc_1]; \tau_1, ch_2[pc_2]; \tau_2) \). \( e_1 \) then \( e_2 ; \tau \). From the premises, we have
\[
\Pi; \Gamma; \Theta[ch_1 \mapsto \text{chan}_{p \rightarrow q} \text{pc}_1 \tau_1, ch_2 \mapsto \text{chan}_{p \rightarrow q} \text{pc}_2 \tau_2]; p; \text{pc} \vdash e_2 : \tau \\
\Pi; \emptyset[ch_1 \mapsto \text{chan}_{p \rightarrow q} \text{pc}_1 \tau_1, ch_2 \mapsto \text{chan}_{p \rightarrow q} \text{pc}_2 \tau_2]; q; \text{pc} \vdash e_1; \text{unit} \Pi \vdash \text{pc} \subseteq \text{pc} \\
\Pi \vdash p \succ \text{pc} \\
\Pi \vdash q \succ \text{pc}
\]

Straightforward application of induction hypothesis to the premises.

**Case DT-BRACKET:** The premise \( \Pi \vdash H^t \cup \text{pc} \subseteq \text{pc}'' \) implies \( \Pi \vdash H^t \cup \text{pc} \subseteq \text{pc}'' \).

**Case DT-BRACKET-VALUES:** Applying induction to the premises gives the required conclusion.

**Case DT-BRACKET-WHERE:** Similar to above case.

\[ \square \]

**Lemma 12** (Weakening Channel Environment for Values). If \( \Pi; \Gamma; \Theta; p; \text{pc} \vdash \bar{v} : \tau \) then \( \Pi; \Gamma; \Theta' ; p; \text{pc} \vdash \bar{v} : \tau \) for any \( \Theta' \).

**Proof.** Proof is by induction on the structure of the values.
**Case Var:** Trivial
**Case Unit:** Trivial
**Case Delegation:** Trivial
**Case \( \eta \), \( v \):** Apply induction to the premise of DT-UNITMSEALED.
**Case \( \mathtt{inj}, v \):** Apply induction to the premise of DT-INJ.
**Case Lambda:** Trivial since functions carry their own channel environment.

**Case TLambda:** Same as above.

**Case Where:** Apply induction to the premise of DT-INJ.

**Case \( v; \pi \):** Apply induction to the premise of DT-HALT and DT-HALT2.

**Case \((\lambda v_1 \text{ where } v_1' \mid \lambda v_2 \text{ where } v_2')\):** From DT-BRACKET-WHERE, we have that

\[
\Pi \vdash H^\pi \leq \tau
\]

\[
\Pi; \Gamma; \Theta; p; \text{pc} \vdash \lambda v_1 \; \vdash v_1' : \tau
\]

\[
\Pi; \Gamma; \Theta; p; \text{pc} \vdash \lambda v_2 \; \vdash v_2' : \tau
\]

Applying induction to the premises, we have that

\[
\Pi \vdash H^\pi \leq \tau
\]

\[
\Pi; \Gamma; \Theta'; p; \text{pc} \vdash \lambda v_1 \; \vdash v_1' : \tau
\]

\[
\Pi; \Gamma; \Theta'; p; \text{pc} \vdash \lambda v_2 \; \vdash v_2' : \tau
\]

Thus, from DT-BRACKET-WHERE, we have \( \Pi; \Gamma; \Theta; p; \text{pc} \vdash (\lambda v_1 \mid \lambda v_2) : \tau \)

**Case \((\lambda v_1 \mid \lambda v_2)\):** Similar to above case.

**Case \((\lambda v_1 \mid \lambda v_2)\):** Similar to above case.

**Case \((\lambda v_1 \mid \lambda v_2)\):** From DT-BRACKET-VALUES, we have that

\[
\Pi \vdash H^\pi \leq \tau
\]

\[
\Pi; \Gamma; \Theta; p; \text{pc} \vdash \lambda v_1 : \tau
\]

\[
\Pi; \Gamma; \Theta; p; \text{pc} \vdash \lambda v_1 : \tau
\]

Applying induction to the premises, we have that

\[
\Pi \vdash H^\pi \leq \tau
\]

\[
\Pi; \Gamma; \Theta'; p; \text{pc} \vdash \lambda v_1 : \tau
\]

\[
\Pi; \Gamma; \Theta'; p; \text{pc} \vdash \lambda v_1 : \tau
\]

Thus \( \Pi; \Gamma; \Theta'; p; \text{pc} \vdash (\lambda v_1 \mid \lambda v_2) : \tau \).

\[\square\]

**Lemma 13 (Non-Bracket Values PC).** Let \( \Pi_i; \Gamma_i; \Theta_i; p_i; \text{pc}_i \vdash e_i : \tau_i \mid \cdots \mid \Pi_m; \Gamma_m; \Theta_m; p_m; \text{pc}_m \vdash e_m : \tau_m \). If \( \Pi_i; \Gamma_i; \Theta_i; p_i; \text{pc}_i \vdash \hat{v} : \tau \) for some \( i = \{1 \ldots m\} \) such that \( \hat{v} \) is not a bracket then \( \Pi'; \Gamma'; \Theta'; p'; \text{pc}' \vdash \hat{v} : \tau \) for any \( \text{pc}' \) such that \( \Pi_i \vdash p_i' \supseteq \text{pc}' \).

**Proof.** Recall that \( \text{pc} = \bigsqcap_i T_i \cap \bigsqcap_i \text{pc}_i \). Proof is by induction on the values. Also, the condition \( \Pi_i \vdash p_i' \supseteq \text{pc}' \) ensures that the proof is straightforward for all values except functions and where terms. We prove important cases.

**Case Function:** Given \( \Pi_i; \Gamma_i; \Theta_i; p_i; \text{pc}_i \vdash \lambda(x: \hat{\pi})[\text{pc}'', \Theta''', \text{pc}', \Pi_\pi] \vdash e : \vdash \vdash \text{pc}''' ; \Theta'''' ; \Pi_\pi \vdash \tau \). We have to prove that:

\[
\Pi_i; \Gamma_i; \Theta_i; p_i'; \text{pc}' ; \lambda(x: \hat{\pi})[\text{pc}'', \Theta''', \text{pc}', \Pi_\pi] \vdash e \vdash \vdash \text{pc}''' ; \Theta'''' ; \Pi_\pi \vdash \tau
\]

This is straightforward as there is no dependency on \( \text{pc}' \) to type check the function body \( e \).

**Case Where:** Given \( \Pi_i; \Gamma_i; \Theta_i; p_i; \text{pc}_i \vdash \hat{v} \text{ where } (p \supseteq q) : \tau_i \). We have to prove that:

\[
\Pi_i; \Gamma_i; \Theta_i; p_i'; \text{pc} ; \hat{v} \text{ where } (p \supseteq q) : \tau_i
\]

From DT-WHERE, we have that \( \Pi_i \vdash \text{pc} \supseteq \nabla(q) \). Note that \( \text{pc} \) is constant for a given distributed configuration and does not change with the \( \text{pc}' \). We are already given that \( \Pi_i \vdash p_i' \supseteq \text{pc}' \). Applying induction to the remaining premises, we have all premises for DT-WHERE.

\[\square\]

**Lemma 14 (Variable Substitution).** If \( \Pi; \Gamma; x : \tau'; \Theta; p; \text{pc} \vdash e : \tau \) and \( \Pi; \Gamma; \Theta; p; \text{pc} \vdash \hat{v} : \tau' \), then \( \Pi; \Gamma; \Theta; p; \text{pc} \vdash e[x \mapsto \hat{v}] : \tau \).

**Proof.** Proof is by the induction on the structure of the expression \( e \). Interesting case is bracket. Given \( \Pi; \Gamma; x : \tau'; \Theta; p; \text{pc} \vdash (e_1 \mid e_2) : \tau \). We have to prove that

\[
\Pi; \Gamma; \Theta; p; \text{pc} \vdash (e_1[x \mapsto \hat{v}]_1) \mid e_2[x \mapsto \hat{v}]_2 : \tau
\]
We first describe the case DT-Bracket. The proof for the cases DT-Bracket-Values and DT-Bracket-Where are similar. From DT-Bracket, we have that

\[
\Pi; \Gamma, x : \tau'; \Theta; \rho; \rho' \vdash e_i : \tau
\]

(43)

\[
\Pi; \Gamma, x : \tau'; \Theta; \rho; \rho' \vdash e_i : \tau
\]

(44)

\[
\Pi \vdash (H^\pi \sqcup \rho) \sqsubseteq \rho'
\]

(45)

\[
\Pi \vdash H^\pi \leq \tau
\]

(46)

Applying clearance (Lemma 7), we have that \( \Pi \vdash p \not> \rho' \). Depending on whether \( \hat{e} \) is a bracket value, we have two cases

**Case** \( \hat{e} = (\hat{e}_1 | \hat{e}_2) \): From DT-Bracket-Values (or from DT-Bracket-Where), we have that

\[
\Pi; \Gamma; \Theta; \rho; \rho' \vdash \hat{e}_1 : \tau'
\]

(47)

\[
\Pi; \Gamma; \Theta; \rho; \rho' \vdash \hat{e}_2 : \tau'
\]

(48)

Since non-bracketed values can be typed under any \( \rho \) which acts for the place under which value is typed (Lemma 13), we have that \( \Pi; \Gamma; \Theta; \rho; \rho' \vdash \hat{e}_i : \tau' \) for all \( i \in \{1, 2\} \). Applying induction to the premises (43) and (44), we get

\[
\Pi; \Gamma; \Theta; \rho; \rho' \vdash \rho \vdash (e_1[x \mapsto \hat{e}_1] | e_2[x \mapsto \hat{e}_2]) : \tau
\]

(49)

**Case** \( \hat{e} \neq (\hat{e}_1 | \hat{e}_2) \): Since non-bracketed values can be typed under any \( \rho \) which acts for the place under which value is typed (Lemma 13), we have that \( \Pi; \Gamma; \Theta; \rho; \rho' \vdash \hat{e} : \tau' \). Applying induction to the premises (43) and (44), we get

\[
\Pi; \Gamma; \Theta; \rho; \rho' \vdash \rho \vdash e_1[x \mapsto \hat{e}] : \tau
\]

(50)

\[
\Pi; \Gamma; \Theta; \rho; \rho' \vdash \rho \vdash e_2[x \mapsto \hat{e}] : \tau
\]

(51)

and thus

\[
\Pi; \Gamma; \Theta; \rho; \rho' \vdash \rho \vdash (e_1[x \mapsto \hat{e}] | e_2[x \mapsto \hat{e}]) : \tau
\]

(52)

(53)

**Lemma 15 (Projection Preserves Types).** If \( \Pi; \Gamma; \Theta; \rho; \rho' \vdash e : \tau \), then \( \Pi; \Gamma; \Theta; \rho; \rho' \vdash [e]_i : \tau \) for \( i \in \{1, 2\} \).

**Proof.** Proof is by induction on the typing derivation. Interesting case is DT-Bracket. Applying Lemma 11 to the expression typing judgments, we have the proof.

**Lemma 16 (Type Substitution Preserves Well-Typedness).** Let \( \tau' \) be well-formed in \( \Gamma, X, \Gamma' \). If \( \Pi; \Gamma, X, \Gamma'; \Theta; \rho; \rho' \vdash e : \tau \) then \( \Pi; \Gamma, \Gamma'[X \mapsto \tau'] ; \Theta; \rho; \rho' \vdash \rho \vdash e[X \mapsto \tau'] : \tau[X \mapsto \tau'] \).

**Proof.** Proof is by induction on the typing derivation \( \Pi; \Gamma; \Theta; \rho; \rho' \vdash e : \tau \).

**Case DT-Var:** Depending on whether \( \tau \) uses \( X \) two cases arise. Either \( \Pi; \Gamma, x : \tau, X, \Gamma'; \Theta; \rho; \rho' \vdash e : \tau \) or \( \Pi; \Gamma, X, x : \tau, \Gamma'; \Theta; \rho; \rho' \vdash x : \tau \). The former case, since \( \Gamma, X, x : \tau \) does not use \( X \), we have that \( \tau[X \mapsto \tau'] \) is same as \( \tau \).

In the latter case, we have that \( \Pi; \Gamma, X, x : \tau[X \mapsto \tau'] ; \Theta; \rho; \rho' \vdash x : \tau[X \mapsto \tau'] \).

**Case DT-Unit:** Straightforward from the corresponding typing judgment.

**Case DT-Del:** Straightforward from the corresponding typing judgment.

**Case DT-Lam:** Given \( \Pi; \Gamma, \Gamma', \Theta; \rho; \rho' \vdash \lambda(x : \tau_1)[\rho \vdash e \vdash \tau_2] \). From DT-Lam \( \Pi; \Gamma, \Gamma', \Theta; \rho; \rho' \vdash \lambda(x : \tau_1)[\rho \vdash e \vdash \tau_2] \). Applying induction hypothesis to the premise, we have \( \Pi; \Gamma, \Gamma'[X \mapsto \tau'] ; \Theta; \rho; \rho' \vdash e[X \mapsto \tau'] ; \tau_2[X \mapsto \tau'] \). From DT-Lam, we thus have \( \Pi; \Gamma, \Gamma'[X \mapsto \tau'] ; \Theta; \rho; \rho' \vdash \lambda(x : \tau_1)[\rho \vdash e[X \mapsto \tau'] ; \tau_2[X \mapsto \tau'] \)

(54)

\[
\Pi; \Gamma, \Gamma'[X \mapsto \tau'] ; \Theta; \rho; \rho' \vdash e[X \mapsto \tau'] : \tau_2[X \mapsto \tau'] \]

(55)

From DT-App, we thus have \( \Pi; \Gamma, \Gamma'[X \mapsto \tau'] ; \Theta; \rho; \rho' \vdash e[X \mapsto \tau'] ; e'[X \mapsto \tau'] : \tau_2[X \mapsto \tau'] \)

29
Case DT-TLam: Given $\Pi; \Gamma, X, \Gamma'; \Theta; p; pc \vdash \Lambda Y[pc', \Theta', \varphi, \Pi']. e : \forall Y[pc', \Theta', \varphi, \Pi']. \tau$. Applying induction hypothesis to the premise of DT-TLAM we have

$$\Pi; \Gamma, (\Gamma', Y)[X \mapsto \tau'] ; \Theta; p; pc \vdash e[X \mapsto \tau'] : \tau[X \mapsto \tau']$$

So from DT-TLAM, we have

$$\Pi; \Gamma, \Gamma'[X \mapsto \tau'] ; \Theta; p; pc \vdash \Lambda Y[pc', \Theta', \varphi, \Pi']. e[X \mapsto \tau'] : \forall Y[pc', \Theta', \varphi, \Pi']. \tau[X \mapsto \tau']$$

Case DT-TApp: Given $\Pi; \Gamma, X, \Gamma'; \Theta; p; pc \vdash e \tau' : \tau[Y \mapsto \tau'']$. Applying induction hypothesis to the premises of T-TAPP, we have $\Pi; \Gamma, X, \Gamma'[X \mapsto \tau'] ; \Theta; p; pc \vdash e[X \mapsto \tau'] : \forall Y[pc', \Theta', \varphi, \Pi']. \tau[X \mapsto \tau']$. From DT-TAPP, we thus have $\Pi; \Gamma, \Gamma'[X \mapsto \tau'] ; \Theta; p; pc \vdash (e[X \mapsto \tau']) \tau''[X \mapsto \tau'''] : \tau[X \mapsto \tau''']$. (57)

Case DT-Pair: Straightforward application of induction hypothesis to the premises.

Case DT-UnPair: Straightforward application of induction hypothesis to the premises.

Case DT-Unit: Straightforward application of induction hypothesis to the premises.

Case DT-Case: Straightforward application of induction hypothesis to the premises.

Case DT-UnitM: Straightforward application of induction hypothesis to the premises.

Case DT-BindM: Straightforward application of induction hypothesis to the premises.

Case DT-Where: Straightforward application of induction hypothesis to the premises.

Case DT-TEEG: Straightforward application of induction hypothesis to the premises.

Case DT-Bracket-Where: Straight forward application of induction hypothesis to the premises.

Case DT-Bracket-VALUES: Straight forward application of induction hypothesis to the premises.

Lemma 17 (Non-Bracket values sent over a channel). Let $v$ be the well-typed non-bracket value sent over a channel. That is, for some $\Pi, p, pc$. $\Pi; \emptyset; \emptyset; p; pc \vdash v : \tau$. Then $\forall \Pi', p', pc'$. $\Pi' \vdash p' \triangleright pc'$, $\Pi'; \emptyset; \emptyset; p'; pc' \vdash v : \tau$.

Proof. Induction on the structure of values.

Case Unit: Given that $\Pi' \vdash q \triangleright pc'$. From DT-UNIT, we thus have $\Pi'; \emptyset; \emptyset; q; pc' \vdash \{\} : unit$.

Case Pair: Given $\Pi; \emptyset; \emptyset; p; pc \vdash \langle v_1, v_2 \rangle : \tau_1 \times \tau_2$ for all $\Pi$ such that $\Pi \vdash p \triangleright pc$. Inverting DT-PAIR, we have $\Pi; \emptyset; \emptyset; p; pc \vdash v_1 : \tau_1$. Also given that $\Pi' \vdash p' \triangleright pc'$, Applying induction hypothesis, we have $\Pi'; \emptyset; \emptyset; p'; pc' \vdash v_1 : \tau_1$. From DT-PAIR, we thus have all premises to prove $\Pi'; \emptyset; \emptyset; q; pc' \vdash \langle v_1, v_2 \rangle : \tau_1 \times \tau_2$.

Case Del: Similar to the above case.

Case Inj: Similar to the above case.

Case Seal: Similar to the above case.

Case Where: Given $\Pi; \emptyset; \emptyset; pl; pc \vdash v$ where $v' : \tau$. Inverting DT-WHERE, we have:

$$\Pi; \Gamma; \Theta; pl; pc \vdash v' : (p \triangleright q)$$

(56)

(56) is the premise of DT-TL.

So from DT-TL, we have:

$$\Pi; \Gamma, (\Gamma', Y)[X \mapsto \tau'] ; \Theta; p; pc \vdash e[X \mapsto \tau'] : \tau[X \mapsto \tau']$$

(57)

(57) is the premise of DT-TAPP.

Applying induction hypothesis to the first 2 premises, we have:

$$\Pi; \Gamma; \Theta; p'; pc' \vdash v' : (p \triangleright q)$$

(61)

Applying induction hypothesis to the first 2 premises, we have:

$$\Pi' \vdash (p \triangleright q) \vdash v : \tau$$

(62)

(62) is the premise of DT-PAIR.

Applying induction hypothesis to the first 2 premises, we have:

$$\Pi' \vdash (p \triangleright q) \vdash v : \tau$$

(63)

(63) is the premise of DT-PAIR.
We now argue that the following holds.

\[ \Pi' \vdash \nabla (p^-) \Rightarrow \nabla (q^-) \]

Recall that the value \( v \) sent over a channel is closed over required delegations and so \( \emptyset \vdash \nabla (p^-) \Rightarrow \nabla (q^-) \) holds. Extending delegation context, we have the above premise. Hence the proof.

**Case Lam:** Given \( \Pi; \emptyset; \emptyset; p; pc \vdash x: \tau | [pc''', \Theta'', \Gamma, \Pi, \lambda], e: \vdash pc''', \Theta'', \Gamma, \Pi, \lambda \Rightarrow \tau \) for all \( \Pi \) such that \( \Pi \vdash p \gg pc \). Inverting DT-LAM, we have

\[ \forall p' \in \mathcal{P}, \Pi, \lambda; x: \hat{\tau}; \Theta', p'; pc'' \vdash e: \tau \]

We are also given that \( \Pi' \vdash q \gg pc' \). Combining this with above, from DT-LAM, we thus have all premises to prove

\[ \Pi'; \emptyset; \emptyset; q; pc' \vdash x: \tau | [pc''', \Theta'', \Gamma, \Pi, \lambda], e: \vdash pc''', \Theta'', \Gamma, \Pi, \lambda \Rightarrow \tau. \]

**Case TLam:** Similar to above.

\[ \square \]

Using the above lemmas, we are now ready to prove type preservation for a process.

**Lemma 18** (Type Preservation for a Process). Let \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j: \tau_j \), for every \( j \in \{1 \ldots m\} \). If \( p_j, D_j \vdash e_j \rightarrow e_j' \) such that for every \( (p \gg q) \in \Pi_j \), \( (p \gg q) \in D_j \) then \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j': \tau_j \)

**Proof.** By proving inductively the on the step relation \( p_j, D_j \vdash e_j \rightarrow e_j' \). We only prove interesting cases. Remaining cases (DE-APP', DE-TAPP', DE-CASE', DE-UNITM', DE-BINDM', DE-ASSUME', DE-SEND') follow from straightforward application of induction hypothesis to the premises.

**Case DE-APP:** Given \( e_j = (\lambda (x: \tau)[pc', \Theta, \Pi, \lambda], e) \) \( v \) and \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash (\lambda (x: \tau)[pc', \Theta, \Pi, \lambda], e) v: \tau_2 \). From the premises we have,

\( \Pi_j; \Gamma_j; x: \tau'; \Theta_j; p_j; pc' \vdash e: \tau_j \) and \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash v: \tau' \)

Since \( \Pi_j \vdash p_j \gg pc \), invoking PC reduction (Lemma 11, we have that \( \Pi_j; \Gamma_j; x: \tau'; \Theta_j; p_j; pc_j \vdash e: \tau_j \).

We have \( e_j' = e(x/v) \). Invoking Lemma 14, we have \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e(x/v): \tau_j \).

**Case DE-TAPP:** Similar to above case.

**Case DE-CASE1:** Given \( e_j = \text{case } (\text{inj}_1 v) \) \( of \) \( \text{inj}_j(x). e_j1 | \text{inj}_j(x). e_j2 \)

and \( e_j' = e_j1[x/v] \). Also,

\( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash \text{case } (\text{inj}_1 v) \) \( of \) \( \text{inj}_j(x). e_j1 | \text{inj}_j(x). e_j2: \tau \). From the premises we have, \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash \text{inj}_1 v: \tau_j + \tau_j'' \) and \( \Pi_j; \Gamma_j; x: \tau_j; \Theta_j; p_j; pc_j \vdash e_j: \tau_j \). From DT-INJ, we have \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash v: \tau_j' \).

Invoking Lemma 14, we have \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j(x/v): \tau_j \).

**Case DE-CASE2:** Similar to above.

**Case DE-UNITM:** Given \( e_j = \eta_\ell v \) \( and \) \( e_j' = \eta_\ell v \). Also, \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash \eta_\ell v: \ell \) says \( \tau \). From the premises it follows that \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc \vdash \eta_\ell v: \ell \) says \( \tau \).

**Case DE-BINDM:** Given \( e_j = \text{bind } x = v \) \( in \) \( e' \) \( and \) \( e_j' = e'[x/v] \) \( Also, \) \( \Pi_j; \Gamma; \Theta; p; pc \vdash \text{bind } x = v \) \( in \) \( e': \tau \). From the premises, we have the following:

\[ \Pi; \Gamma; \Theta; p; pc \vdash v: \tau' \]
\[ \Pi; \Gamma, x: \tau'; \Theta; p; pc \cup \ell \vdash e': \tau \]
\[ \Pi \vdash pc \cup \ell \leq \tau \]
\[ \Pi \vdash p \gg pc \]

We have to prove that \( \Pi; \Gamma; \Theta; p; pc \vdash e'[x/v]: \tau \). Since we have that \( \Pi \vdash p \gg pc \), applying PC reduction (Lemma 11) to the premise (65), we have \( \Pi; \Gamma, x: \tau'; \Theta; p; pc \vdash e': \tau \).

Invoking Lemma 14, we thus have \( \Pi; \Gamma; \Theta; p; pc \vdash e'[x/v]: \tau \).

**Case DE-ASSUME:** Given \( e = \text{assume } v \) \( in \) \( e' \) \( and \) \( e' = e' \) \( where \) \( v \). Also, \( \Pi; \Gamma; \Theta; p; pc \vdash \text{assume } v \) \( in \) \( e': \tau \). Let D be such that for every \( (p \gg q) \in \Pi \), \( (p \gg q) \in D \). From DT-ASSUME, we have

\[ \Pi; \Gamma; \Theta; pl; pc \vdash v: (p \gg q) \]
\[ \Pi; (p \gg q); \Gamma; \Theta; pl; pc \vdash e': \tau \]
\[ \Pi \vdash pc \gg \nabla (q) \]
\[ \Pi \vdash \nabla (pl^-) \gg \nabla (q^-) \]
\[ \Pi \vdash pl \gg pc \]
We need to prove:

$$\Pi; \Gamma; \Theta; p; pc \vdash e' \text{ where } v: \tau$$

Comparing with the given premises, we have all except (80).

$$\Pi; \Gamma; \Theta; pl; pc \vdash v: (p \gtrsim q)$$  \hspace{1cm} (73)
$$\Pi \cdot (p \gtrsim q); \Gamma; \Theta; pl; pc \vdash e: \tau$$  \hspace{1cm} (74)
$$\Pi_{inst} \vdash \text{pc} \gtrsim \nabla(q)$$  \hspace{1cm} (75)
$$\Pi \vdash \nabla(p^{-}) \gtrsim \nabla(q^{-})$$  \hspace{1cm} (76)
$$\Pi \vdash pl \gtrsim pc$$  \hspace{1cm} (77)

We need to prove:

$$\Pi; \Gamma; \Theta; p; pc \vdash e' \text{ where } v: \tau$$

Comparing with the given premises, we have all except (80).

$$\Pi; \Gamma; \Theta; pl; pc \vdash v: (p \gtrsim q)$$  \hspace{1cm} (78)
$$\Pi \cdot (p \gtrsim q); \Gamma; \Theta; pl; pc \vdash e: \tau$$  \hspace{1cm} (79)
$$\Pi_{inst} \vdash \text{pc} \gtrsim \nabla(q)$$  \hspace{1cm} (80)
$$\Pi \vdash \nabla(p^{-}) \gtrsim \nabla(q^{-})$$  \hspace{1cm} (81)
$$\Pi \vdash pl \gtrsim pc$$  \hspace{1cm} (82)

Since $pc$ grows monotonically both inside and outside TEEs, we have that $\overline{pc}$ has more integrity than $pc$. And so, if $\Pi \vdash pc \gtrsim \nabla(q)$ then $\Pi \vdash \overline{pc} \gtrsim \nabla(q)$. We now argue that if $\Pi \vdash \overline{pc} \gtrsim \nabla(q)$ then $\Pi_{inst} \vdash \overline{pc} \gtrsim \nabla(q)$. The argument is similar to proving delegation invariance in FLAC. We sketch the high-level details here: every delegation added to $\Pi_{inst}$ requires that $\overline{pc}$ is the voice of the delegator. That is, if $\Pi = \Pi_{inst} \cdot (r \gtrsim s)$, then it must be the case that the assumption added the delegation after checking $\Pi_{inst} \vdash pc \gtrsim \nabla(s)$ (for some $pc$) which implies $\Pi_{inst} \vdash \overline{pc} \gtrsim \nabla(s)$. Now let $\Pi' = \Pi \cdot (u \gtrsim v)$. Following similar argument, we have that $\Pi \vdash \overline{pc} \gtrsim \nabla(v)$. The derivation has two cases: $\Pi_{inst} \vdash \overline{pc} \gtrsim \nabla(v)$ or $\Pi_{inst} \cdot (r \gtrsim s) \vdash \overline{pc} \gtrsim \nabla(v)$. For the latter case, notice that $\Pi_{inst} \vdash \overline{pc} \gtrsim \nabla(v)$ and $\Pi_{inst} \cdot (r \gtrsim s) \vdash \overline{pc} \gtrsim \nabla(v)$, hence it must be the case that $\Pi_{inst} \vdash s \gtrsim \nabla(v)$. Using transitivity, we now have that $\Pi_{inst} \vdash \overline{pc} \gtrsim \nabla(v)$. Thus, using induction on the delegation context it can be proved that if $\Pi \vdash pc \gtrsim \nabla(q)$ then $\Pi \vdash \overline{pc} \gtrsim \nabla(q)$. This gives us the premise (80). Hence proved.

**Case DE-WHERE:** Given $e = e \ where \ v$ and $e' = e' \ where \ v$. Also, $\Pi; \Gamma; \Theta; p; pc \vdash e \ where \ v: \tau$. Let $D$ be such that for every $(p \gtrsim q) \in \Pi$, $(p \gtrsim q) \in D$. From DT-WHERE, we have that

$$\Pi \cdot (a \gtrsim b); \Gamma; \Theta; p; pc \vdash e: \tau$$  \hspace{1cm} (83)
$$\Pi; \Gamma; \Theta; p; pc \vdash v: (a \gtrsim b)$$  \hspace{1cm} (84)

From DT-WHERE, we have $p, D, v \vdash e \longrightarrow e'$. So, we have that $v \in D_i \cdot v$ and $v \in \Pi \cdot (a \gtrsim b)$. Applying inductive to the premise (83), we have that $\Pi \cdot (a \gtrsim b); \Gamma; \Theta; p; pc \vdash e: \tau$ and so $\Pi; \Gamma; \Theta; p; pc \vdash e' \ where \ v: \tau$.

**Case DE-TEE:** Given $e = \text{TEE}^t e$ and $e' = \text{runTEE}^t e$. Also given $\Pi; \Gamma; \Theta; p; pc \vdash \text{TEE}^t e: \text{unit;} \Box$. From DT-TEE, we trivially have that $\Pi; \Gamma; \Theta; p; pc \vdash \text{runTEE}^t e: \text{unit;} \Box$.

**Case DE-TEE^t:** Given $e = \text{runTEE}^t e$ and $e' = \text{runTEE}^t e'$. Also given $\Pi; \Gamma; \Theta; p; pc \vdash \text{runTEE}^t e: \text{unit;} \Box$. From the premises of DT-TEE, we have

$$\Pi; \emptyset; \Theta; t; t^\frown \land \text{pc}^\frown \vdash e: \tau$$  \hspace{1cm} (85)

From the premises of DE-TEE, we have

$$t, D \vdash e \longrightarrow e'$$

Applying induction hypothesis to the premise, we have

$$\Pi; \emptyset; \Theta; t; t^\frown \land \text{pc}^\frown \vdash e': \tau$$

Hence $\Pi; \Gamma; \Theta; p; pc \vdash \text{runTEE}^t e': \tau$.

**Case DE-TEE^t:** Given $e = \text{TEE}^t v$ and $e' = (\Box); \Box$. Also given $\Pi; \Gamma; \Theta; p; pc \vdash \text{runTEE}^t v: \text{unit;} \Box$. From DT-UNIT and DT-HALT, we have that $\Pi; \Gamma; \Theta; p; pc \vdash (\Box); \Box: \text{unit;} \Box$. Thus $\Pi; \Gamma; \Theta; p; pc \vdash e': \text{unit;} \Box$.

**Case DE-SEND:** Given $p, D \vdash (\text{send } v \ v' \ \text{then } e_{s_{\Box}}) \longrightarrow (p, \text{send } v \ v' \ \text{then } e_{s_{\Box}}; \Box)$ where $v' = \text{export}_{\text{del}}(D, v)$.

Also, $\Pi; \Gamma; \Theta; p; pc \vdash \text{send } v \ v' \ \text{then } e_{s_{\Box}}: \text{unit}$. We need to prove that

$$\Pi; \Gamma; \Theta; p; pc \vdash \text{send } v \ v' \ \text{then } e_{s_{\Box}}; \Box: \hat{\tau}; \Box$$
Inverting the premises of DT-SEND, we have that
\[
\begin{align*}
\Pi; \Gamma; p; pc &\vdash \text{chan}_{p \rightarrow q} \quad pc_{ch} \quad \xi \\
\Pi; \Gamma; \emptyset; p; pc &\vdash v: \tau \\
\Pi; \Gamma; \Theta; p; pc &\vdash e_{\text{rec}}: \tau' \\
\tau' &\in \{\xi', \xi''\} \\
\Pi \vdash pc \subseteq pc_{ch} \\
\Pi \vdash pc_{ch} \subseteq pc' \\
\Pi \vdash pc' \leq \tau' \\
\Pi \vdash p \succ pc & \\
\Pi \vdash p \succ pc_{ch} &
\end{align*}
\]

To prove what we want, we have all the required premises except
\[
\Pi; \emptyset; p; pc \vdash v': \tau
\]

Since export,del(D,v) closes over required delegations, v' requires no further assumptions on delegations. We still need to prove that the variable typing context can be empty. Because of substitution semantics, if we start with a closed program then an expression that gets evaluated to a value is closed as well (Lemma 6). Hence proved.

**Case DE-HALT**: Applying induction hypothesis to the premise, we have the conclusion.

**Case DE-HALT**: Given e = v;\Box and e' = v;\Box. From DT-HALT, the type of v;\Box is \tau;\Box. From DT-HALT2, the type of e is thus \tau;\Box. We already have that the type of e' is also \tau;\Box. Hence proved.

**Case DW-APP**: Given e = (v where \langle p \succ q \rangle) v' and e' = (v v') where \langle p \succ q \rangle. We have to prove that
\[
\Pi; \Gamma; p; pc \vdash (v v') where \langle p \succ q \rangle: \tau
\]

From DT-APP we have:
\[
\begin{align*}
\Pi; \Gamma; pl; pc &\vdash v where \langle p \succ q \rangle : \tau_1 \\
\Pi; \Gamma; pl; pc &\vdash v': \tau_1 \\
\Pi \vdash pc \subseteq pc' \\
pl \in P \\
\Theta |_{\text{dom}(\Theta')} &= \Theta' \\
\forall(p \succ q) \in \Pi'. \Pi \vdash p \succ q \\
\Pi \vdash pl \succ pc &
\end{align*}
\]

Rule DT-WHERE gives us the following:
\[
\begin{align*}
\Pi; \Gamma; \Theta; p; pc &\vdash \langle p \succ q \rangle : \tau_1 \\
\Pi \vdash pc \succ \nabla(q) \\
\Pi \vdash \nabla(p^-) \succ \nabla(q^-) \\
\Pi \cdot \langle p \succ q \rangle; \Gamma; \Theta; p; pc &\vdash v: \tau_1 \\
\Pi \cdot \langle p \succ q \rangle; \Gamma; \Theta; p; pc &\vdash v': \tau
\end{align*}
\]

We now want to show that e' is well typed via DT-WHERE. The key premise is to show that the subexpression (v v') is well-typed via DT-APP. That is,
\[
\Pi \cdot \langle p \succ q \rangle; \Gamma; \Theta; p; pc \vdash v \cdot v': \tau
\]

Applying Lemma 10 (extending assumptions for terms) to (96) and applying Lemma 8 to (97), as well as using premises from (106) to (101), we have
\[
\begin{align*}
\Pi \cdot \langle p \succ q \rangle; \Gamma; \Theta; p; pc &\vdash v: \tau_1 \\
\Pi \cdot \langle p \succ q \rangle &\vdash pc \subseteq pc'pl \in P \\
\Theta |_{\text{dom}(\Theta')} &= \Theta' \\
\forall(a \succ b) \in \Pi'. \Pi \cdot \langle p \succ q \rangle &\vdash a \succ b \\
\Pi \cdot \langle p \succ q \rangle &\vdash pl \succ pc &
\end{align*}
\]
Combining with (105), we have (106). Remaining clauses, that is, (102), (103), and (104), give:

$$
\Pi; \Gamma; p; \text{pc} \vdash (v \ e) \text{ where } \langle p \succcurlyeq q \rangle : \tau
$$

**Case DW-TAPP:** Given \( e = (v \text{ where } \langle p \succcurlyeq q \rangle ) \) and 
\( e' = (v \ \tau') \text{ where } \langle p \succcurlyeq q \rangle \). We have to prove that

$$
\Pi; \Gamma; p; \text{pc} \vdash (v \ e') \text{ where } \langle p \succcurlyeq q \rangle : \tau[X \mapsto \tau']
$$

From DT-TAPP we have:

$$
\Pi; \Gamma; p; \text{pc} \vdash v \text{ where } \langle p \succcurlyeq q \rangle : \forall X[\text{pc}', \Theta', \mathcal{P}, \Pi']. \tau
$$

(112)

$$
\Pi \models \text{pc} \sqsubseteq \text{pc}'
$$

(113)

Rule DT-WHERE gives us the following:

$$
\Pi; \Gamma; p; \text{pc} \vdash (p \succcurlyeq q) : (p \succcurlyeq q)
$$

(114)

$$
\Pi \models \nabla(q)
$$

(115)

$$
\Pi \models \nabla(p^{-}) \succcurlyeq \nabla(q^{-})
$$

(116)

$$
\Pi \cdot (p \succcurlyeq q) ; \Gamma; p; \text{pc} \vdash v : \forall X[\text{pc}', \Theta', \mathcal{P}, \Pi']. \tau
$$

(117)

We now want to show that \( e' \) is well typed via DT-WHERE. The key premise is to show that the subexpression \((v \ \tau')\) is well-typed via DT-TAPP. That is,

$$
\Pi \cdot (p \succcurlyeq q); \Gamma; p; \text{pc} \vdash v \ e' : \tau[X \mapsto \tau']
$$

(118)

Applying Lemma 10 (extending assumptions for terms) to (113), we have:

$$
\Pi \cdot (p \succcurlyeq q) \models \text{pc} \sqsubseteq \text{pc}'
$$

(119)

Combining with (117), we have (118). Remaining clauses, that is, (114), (115), and (116), give

$$
\Pi; \Gamma; p; \text{pc} \vdash (v \ e') \text{ where } \langle p \succcurlyeq q \rangle : \tau[X \mapsto \tau']
$$

**Case DW-UNPAIR:** Given \( e = \text{proj}_i((v_1, v_2) \text{ where } \langle p \succcurlyeq q \rangle ) \) and \( e' = \text{proj}_i((v_1, v_2) \text{ where } \langle p \succcurlyeq q \rangle ) \). We have to prove that

$$
\Pi; \Gamma; p; \text{pc} \vdash \text{proj}_i((v_1, v_2)) \text{ where } \langle p \succcurlyeq q \rangle : \tau_i
$$

From DT-UNPAIR, we have:

$$
\Pi; \Gamma; p; \text{pc} \vdash \langle v_1, v_2 \rangle \text{ where } \langle p \succcurlyeq q \rangle : \tau_1 \times \tau_2
$$

(120)

From (120) and DT-WHERE, we have:

$$
\Pi; \Gamma; p; \text{pc} \vdash (p \succcurlyeq q) : (p \succcurlyeq q)
$$

(121)

$$
\Pi \models \nabla(q)
$$

(122)

$$
\Pi \models \nabla(p^{-}) \succcurlyeq \nabla(q^{-})
$$

(123)

$$
\Pi \cdot (p \succcurlyeq q) ; \Gamma; p; \text{pc} \vdash \langle v_1, v_2 \rangle : \tau_1 \times \tau_2
$$

(124)

From (124) and DT-UNPAIR, we have: \( \Pi \cdot (p \succcurlyeq q); \Gamma; p; \text{pc} \vdash \text{proj}_i((v_1, v_2) : \tau_i \) Combining with remaining premises ((121) to (124)) we have \( \Pi; \Gamma; p; \text{pc} \vdash \text{proj}_i((v_1, v_2) : \tau_i \)

**Case DW-CASE:** Given \( e = \text{case } v \text{ of } (p \succcurlyeq q) \text{ of } \text{inj}_1(x).e_1 | \text{inj}_2(x).e_2 \) and \( e' = \text{case } v \text{ of } \text{inj}_1(x).e_1 | \text{inj}_2(x).e_2 \) where \( p \succcurlyeq q \). We have to prove that

$$
\Pi; \Gamma; p; \text{pc} \vdash (\text{case } v \text{ of } \text{inj}_1(x).e_1 | \text{inj}_2(x).e_2) \text{ where } \langle p \succcurlyeq q \rangle : \tau
$$

From DT-CASE we have:

$$
\Pi; \Gamma; p; \text{pc} \vdash v \text{ where } \langle p \succcurlyeq q \rangle : \tau_1 \times \tau_2
$$

(125)

$$
\Pi \vdash \text{pc} \sqsubseteq \ell \leq \tau
$$

(126)

$$
\Pi \models \text{pc} \sqsubseteq \ell
$$

(127)

$$
\Pi; \Gamma; x : \tau_i; p; \text{pc} \vdash e_i : \tau
$$

(128)

$$
\Pi; \Gamma; x : \tau_2; p; \text{pc} \vdash e_2 : \tau
$$

(129)
From (125) and rule DT-WHERE, we get the following:

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; \PC &\vdash (p \triangleright q): (p \triangleright q) \\
\Pi &\vdash \PC \triangleright \nabla(q) \\
\Pi &\vdash \nabla(p^{-}) \triangleright \nabla(q^{-}) \\
\Pi; \Gamma; \Theta; p; \PC &\vdash v: \tau_{1} + \tau_{2}
\end{align*}
\]

(130)  
(131)  
(132)  
(133)

The key premise to prove is that:

\[
\Pi \cdot (p \triangleright q); \Gamma; \Theta; p; \PC \vdash (\text{case } v \text{ of } \text{inj}_{1}(x). e_{1} \mid \text{inj}_{2}(x). e_{2}) : \tau
\]

which follows from (133) and extending delegations in equations (126) to (129) (Lemma 10). Combining with remaining premises, we have

\[
\Pi; \Gamma; \Theta; p; \PC \vdash (\text{case } v \text{ of } \text{inj}_{1}(x). e_{1} \mid \text{inj}_{2}(x). e_{2}) \text{ where } (p \triangleright q) : \tau
\]

Case DW-UNITM: Given \( e = \eta_{\ell} (v \text{ where } (p \triangleright q)) \) and \( e' = (\eta_{\ell} v) \text{ where } (p \triangleright q) \). We have to prove that

\[
\Pi; \Gamma; \Theta; p; \PC \vdash \eta_{\ell} v \text{ where } (p \triangleright q): \ell \text{ says } \tau
\]

From DT-UNITM we have:

\[
\Pi; \Gamma; \Theta; p k; \PC \vdash v \text{ where } (p \triangleright q): \tau
\]

(134)

From DT-WHERE, we have:

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; \PC &\vdash (p \triangleright q): (p \triangleright q) \\
\Pi &\vdash \PC \triangleright \nabla(q) \\
\Pi &\vdash \nabla(p^{-}) \triangleright \nabla(q^{-}) \\
\Pi \cdot (p \triangleright q); \Gamma; \Theta; p; \PC &\vdash v: \tau
\end{align*}
\]

(135)  
(136)  
(137)  
(138)

Combining with other premises ((135) to (138)), we have \( \Pi; \Gamma; \Theta; p; \PC \vdash \eta_{\ell} v \text{ where } (p \triangleright q): \ell \text{ says } \tau \).

Case DW-BINDM: Given \( e = \text{bind } x = (v \text{ where } (p \triangleright q)) \text{ in } e \) and \( e' = (\text{bind } x = v \text{ in } e) \text{ where } (p \triangleright q) \). We have to prove that

\[
\Pi; \Gamma; \Theta; p; \PC \vdash (\text{bind } x = v \text{ in } e) \text{ where } (p \triangleright q): \tau
\]

From DT-BINDM we have:

\[
\begin{align*}
\Pi; \Gamma; \Theta; p k; \PC &\vdash (v \text{ where } (p \triangleright q)) : \ell \text{ says } \tau' \\
\Pi; \Gamma; x : \tau'; \Theta; p; \PC \cup \ell &\vdash e: \tau \\
\Pi &\vdash \PC \cup \ell \leq \tau
\end{align*}
\]

(139)  
(140)  
(141)

From (139) and rule DT-WHERE, we get the following:

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; \PC &\vdash (p \triangleright q): (p \triangleright q) \\
\Pi &\vdash \PC \triangleright \nabla(q) \\
\Pi &\vdash \nabla(p^{-}) \triangleright \nabla(q^{-}) \\
\Pi \cdot (p \triangleright q); \Gamma; \Theta; p; \PC &\vdash v: \ell \text{ says } \tau'
\end{align*}
\]

(142)  
(143)  
(144)  
(145)

We now want to show that \( e' \) is well typed via DT-WHERE. That is, we need the following premises,

\[
\begin{align*}
\Pi \cdot (p \triangleright q); \Gamma; \Theta; p; \PC &\vdash \text{bind } x = v \text{ in } e: \tau \\
\Pi; \Gamma; \Theta; p; \PC &\vdash (p \triangleright q): (p \triangleright q) \\
\Pi &\vdash \PC \triangleright \nabla(q) \\
\Pi &\vdash \nabla(p^{-}) \triangleright \nabla(q^{-})
\end{align*}
\]

(146)  
(147)  
(148)  
(149)

Extending the delegation context (Lemma 10) in the premises (140), (141) and from (145) we have (146).
We already have (147) from (142); (148) from (143); (149) from (144). Combining, we have
\[ \Pi; \Gamma; \Theta; p; pc \vdash (\text{bind } x = v \text{ in } e) \text{ where } \langle p \succ q \rangle : \tau \]

Case DW-Assume: Given \( e = \text{assume } v \text{ where } (a \succ b) \) in \( e \) and \( e' = \text{assume } v \text{ in } e \) where \( (a \succ b) \). From DT-Assume, we have
\[ \Pi; \Gamma; \Theta; p; pc \vdash \text{(147)} \quad \Pi; \Gamma; \Theta; p; pc \vdash \text{(148)} \quad \Pi; \Gamma; \Theta; p; pc \vdash \text{(149)} \]
\[ \Pi; \Gamma; \Theta; p; pc \vdash (a \succ b) : \langle r \succ s \rangle \]
\[ \Pi; \Gamma; \Theta; p; pc \vdash e : \tau \]
\[ \Pi \vdash pc \succ \nabla(s) \]
\[ \Pi \vdash \nabla(r^-) \succ \nabla(s^-) \]

Expanding the first premise using DT-Where, we have
\[ \Pi; \Gamma; \Theta; p; pc \vdash (a \succ b) : \langle a \succ b \rangle \]
\[ \Pi; \Gamma; \Theta; p; pc \vdash v : \langle r \succ s \rangle \]
\[ \Pi \vdash pc \succ \nabla(b) \]
\[ \Pi \vdash \nabla(a^-) \succ \nabla(b^-) \]

We want to show
\[ \Pi; \Gamma; \Theta; p; pc \vdash (a \succ b) : \langle a \succ b \rangle \]
\[ \Pi; \Gamma; \Theta; p; pc \vdash \text{assume } v \text{ in } e : \tau \]
\[ \Pi \vdash pc \succ \nabla(b) \]
\[ \Pi \vdash \nabla(a^-) \succ \nabla(b^-) \]

Extending delegation context (Lemma 10) in the premises (151), (152), (157) and combining with topmost premise we have the (159). Remaining premises follow from (154), (156) and (157).

Case DW-TEEG: Given \( e = \text{runTEE}^t (\hat{v} \text{ where } (a \succ b)) \) and \( e' = \text{runTEE}_v^t (\hat{v}) \text{ where } (a \succ b) \). Also given \( \Pi; \Gamma; \Theta; p; pc \vdash e : \text{unit} \square \). From DT-TEEG, we have
\[ \Pi; \emptyset; \Theta' ; t; t^- \land pc^- \vdash \hat{v} \text{ where } (a \succ b) : \tau \]
\[ \tau \in \{ \text{unit}, \text{unit} \square \} \]
\[ C = \{ ch | \Theta(ch) = \text{chan}_{\text{mp}} pc' \succ \land \Pi \vdash pc \subseteq pc' \} \]
\[ \Theta |c = \Theta' \]
\[ \Pi \vdash p \succ pc \]

Expanding the first premise using DT-Where, we have
\[ \Pi; \emptyset; \Theta' ; t ; t^- \land pc^- \vdash (a \succ b) : \langle a \succ b \rangle \]
\[ \Pi ; (a \succ b) ; \emptyset ; \Theta' ; t ; pc^- \land t^- \vdash \hat{v} : \tau \]
\[ \Pi \vdash pc \succ \nabla(b) \]
\[ \Pi \vdash \nabla(a^-) \succ \nabla(b^-) \]
\[ \Pi \vdash t \succ pc^- \land t^- \]

To prove \( \Pi ; \Gamma ; \Theta ; p ; pc \vdash e' : \text{unit} \square \), we need the following premises:
\[ \Pi ; \Gamma ; \Theta ; p ; pc \vdash (a \succ b) : \langle a \succ b \rangle \]
\[ \Pi ; (a \succ b) ; \Gamma ; \Theta ; p ; pc \vdash \text{runTEE}^t (\hat{v}) : \text{unit} \square \]
\[ \Pi \vdash pc \succ \nabla(b) \]
\[ \Pi \vdash \nabla(a^-) \succ \nabla(b^-) \]
\[ \Pi \vdash p \succ pc \]

(172) follows from (166) using DT-UNIT. To prove (173), we need the following premises
\[ \Pi; \emptyset; \Theta'' ; t ; t^- \land p \succ \vdash \hat{v} : \tau \]
\[ C' = \{ ch | \Theta(ch) = \text{chan}_{\text{mp}} pc' \succ \land \Pi \vdash pc \subseteq pc' \} \]
\[ \Theta |c' = \Theta'' \]
\[ \Pi \vdash p \succ pc \]
Invoking lemma that values do not depend on the channel environment (Lemma 12) on premise (168), we have (177). From premises (178) to (180) we thus have the premise (173). Weakening the delegation context in (165), we have (180). Premises (174) and (175) follow from (169) and (170). Hence proved.

**Case DW-HALT:** Given \( e = p, D \vdash (\tilde{v} \text{ where } \langle a \not\approx b \rangle); \square \) and \( e' = p, D \vdash (\tilde{v}; \square \text{ where } \langle a \not\approx b \rangle) \). Straight forward proof.

**Case BD-STEP:** Given \( e = (e_1 | e_2) \) and \( e' = (e'_1 | e'_2) \). Also \( \Pi; \Gamma; \Theta; p; pc \vdash (e_1 | e_2) : \tau \). We have to prove

\[
\Pi; \Gamma; \Theta; p; pc \vdash (e'_1 | e'_2) : \tau
\]

Without loss of generality, let \( i = 1 \). Thus from the premises of BD-STEP, we have \( e_1 \rightarrow e'_1 \) and \( e'_2 = e_2 \). Since, values cannot take a step, inverting the well-typedness of bracket is only possible through DT-BRACKET and not through DT-BRACKET-VALUES or DT-BRACKET-WHERE. From DT-BRACKET, we have

\[
\Pi; \Gamma; \Theta; p; pc' \vdash e_1 : \tau
\]

\[
\Pi; \Gamma; \Theta; p; pc' \vdash e_2 : \tau
\]

\[
\Pi \vdash (H^\sigma \sqsubseteq pc) \rightarrow pc'
\]

\[
\Pi \vdash H^\sigma \leq \tau
\]

Since (181) holds, applying induction to the premise \( e_1 \rightarrow e'_1 \), we have that \( \Pi; \Gamma; \Theta; p; pc' \vdash e'_1 : \tau \). Combining with remaining premises ((182) to (184)) we thus have that \( \Pi; \Gamma; \Theta; p; pc \vdash (e'_1 | e'_2) : \tau \).

**Case BD-APP:** Invalid case as DP-FUN is removed and so a bracket of function values is no longer well-typed.

**Case BD-TAPP:** Invalid case as DP-TFUN is removed and so a bracket of type abstraction values is no longer well-typed.

**Case BD-UNPAIR:** Given \( e = \text{proj}_j, (\langle v_{11}, v_{12} \rangle \mid \langle v_{21}, v_{22} \rangle) \) and \( e' = (v_{1i} \mid v_{2i}) \) Also \( \Pi; \Gamma; \Theta; p; pc \vdash \text{proj}_j, (\langle v_{11}, v_{12} \rangle \mid \langle v_{21}, v_{22} \rangle) : \tau_i \) We have to prove

\[
\Pi; \Gamma; \Theta; p; pc \vdash (v_{1i} \mid v_{2i}) : \tau_i
\]

From DT-UNPAIR, we have:

\[
\Pi; \Gamma; \Theta; p; pc \vdash (v_{1i1} \mid v_{1i2}) \mid (v_{2i1} \mid v_{2i2}) : \tau_1 \times \tau_2
\]

Since they are already values, they can be inverted using either DT-BRACKET-VALUES or DT-BRACKET-WHERE. We first use the former. Proof for the latter is similar.

\[
\Pi; \Gamma; \Theta; p; pc \vdash (v_{11}, v_{12}) ; \tau_1 \times \tau_2
\]

\[
\Pi; \Gamma; \Theta; p; pc \vdash (v_{21}, v_{22}) ; \tau_1 \times \tau_2
\]

\[
\Pi \vdash H^\sigma \leq \tau_1 \times \tau_2
\]

From (186), (187) and DT-UNPAIR, we have \( \Pi; \Gamma; \Theta; p; pc \vdash v_{1i} : \tau_i \) and \( \Pi; \Gamma; \Theta; p; pc \vdash v_{2i} : \tau_i \) for \( i = \{1, 2\} \).

From (188) and DP-PAIR, we have \( \Pi \vdash H^\sigma \leq \tau_i \). Combining with other premises, from DT-BRACKET-VALUES, we have \( \Pi; \Gamma; \Theta; p; pc \vdash (v_{1i} \mid v_{2i}) : \tau_i \).

**Case BD-BINDM1:** Invalid case as the given bracket expression isn’t well-typed.

**Case BD-BINDM3:** Given \( e = \text{bind } x = (\tilde{\ell}_i, v_1 \mid \tilde{\ell}_i, v_2) \) in \( e \). Here \( e' = ([e]_1[x \mapsto v_1] \mid [e]_2[x \mapsto v_2]) \). Also \( \Pi; \Gamma; \Theta; p; pc \vdash \text{bind } x = (\tilde{\ell}_i, v_1 \mid \tilde{\ell}_i, v_2) \) in \( e \) : \( \tau \). From DT-BINDM, we have

\[
\Pi; \Gamma; \Theta; p; pl; pc \vdash (\tilde{\ell}_i, v_1 \mid \tilde{\ell}_i, v_2) : \ell \text{ says } \tau'
\]

\[
\Pi; \Gamma, x : \tau' \vdash \Theta; p; pc \sqsubseteq \ell \vdash e : \tau
\]

\[
\Pi \vdash pc \sqsubseteq \ell \leq \tau
\]

\[
\Pi \vdash p \not\rightarrow pc
\]

From (189) and DT-BRACKET-VALUES, we have

\[
\Pi; \Gamma; \Theta; p; pc \vdash (\tilde{\ell}_i, v_1) : \ell \text{ says } \tau'
\]

\[
\Pi; \Gamma; \Theta; p; pc \vdash (\tilde{\ell}_i, v_2) : \ell \text{ says } \tau'
\]

\[
\Pi \vdash H^\sigma \sqsubseteq \ell
\]

We have to prove that

\[
\Pi; \Gamma; \Theta; p; pc \vdash ([e]_1[x \mapsto v_1] \mid [e]_2[x \mapsto v_2]) : \tau
\]
For some $\widehat{pc}$ we need the following premises to satisfy DT-Bracket:

$$
\Pi; \Gamma; \Theta; p; \widehat{pc} \vdash e[x \mapsto v_1] : \tau \tag{196}
$$

$$
\Pi; \Gamma; \Theta; p; \widehat{pc} \vdash e[x \mapsto v_2] : \tau \tag{197}
$$

$$
\Pi \vdash (H^e \sqcup pc) \subseteq \widehat{pc} \tag{198}
$$

$$
\Pi \vdash H^e \subseteq \tau \tag{199}
$$

A natural choice for $\widehat{pc}$ is $pc \sqcup \ell$. From (190)

$$
\Pi; \Gamma; x : \tau'; \Theta; p; \widehat{pc} \vdash e : \tau
$$

Invoking clearance lemma (Lemma 7) on the premise (190) we have that

$$
\Pi \vdash p \gg pc \sqcup \ell
$$

From the lemma that non-bracketed values can be typed under any $pc$ such that they are bound by the place’s authority (Lemma 13), we have

$$
\Pi; \Gamma; \Theta; p; \widehat{pc} \vdash v_1 : \tau'
$$

Lemma 15 (bracket projection) and Lemma 14 (substitution), we have (196) and (197). From (195) and (191) we have (199).

Thus we have all premises necessary to prove $\Pi; \Gamma; \Theta; p; pc \vdash (\exists \Theta', p'; pc'; \tau')$ and $\Pi' |_{dom(\Pi)} = \Pi$.

**Case BD-CASE:** Does not occur. Not well-typed.

**Case BD-ASSUME:** Does not occur. Not well-typed.

Before we prove type preservation for the distributed system, we show that holes in the evaluation contexts can be typed under a suitable $pc$. We express this using the relation.

$$
\Pi; \Gamma; \Theta; p; pc \vdash T[e] : \tau \triangleright \Pi'; \Gamma'; \Theta'; pc' \vdash e : \tau'
$$

Figure 21 defines the relation using inference rules. The following lemma proves that every hole is well-typed under some $pc$.

**Lemma 19 (Hole has a Suitable pc).** If $\Pi; \Gamma; \Theta; p; pc \vdash T[e] : \tau$ then $\exists \Pi', \Gamma', p', pc', \tau'$ such that $\Pi; \Gamma; \Theta; p; pc \vdash T[e] : \tau \triangleright \Pi'; \Gamma'; \Theta'; p'; pc' \vdash e : \tau'$ and $\Pi' |_{dom(\Pi)} = \Pi$.

**Proof.**

The following two lemmas prove that channel environment can be extended for a well-typed expression and context.

**Lemma 20 (Weakening Channel Environment for Expressions).** If $\Pi; \Gamma; \Theta; p; pc \vdash e : \tau$ then $\Pi; \Gamma; \Theta'; pc' \vdash e : \tau$ such that $\Theta' |_{dom(\Theta)} = \Theta$.

**Proof.** Straightforward induction on the typing judgement.

**Lemma 21 (Weakening Channel Env for Contexts).** If $\Pi; \Gamma; \Theta; p; pc \vdash T[e] : \tau$ then for all $\Theta'$ such that $\Theta' |_{dom(\Theta)} = \Theta$, $\Pi; \Gamma; \Theta'; pc \vdash T[e] : \tau$.

**Proof.** Straightforward invocation of Lemma 20.
Fig. 24: Extracting holes from well-typed contexts

**Case** \( e \): Given \( \Pi; \Gamma; p; pc \vdash T[\text{spawn} \_@ q \ (pl, ch1 \ [pc_1; \tau_1], \ ch2 \ [pc_2; \tau_2])], e_1 \) then \( e_2 \) \( e: \tau \). Inverting using DT-APP, we have that:

\[
\begin{align*}
\Pi; \Gamma; p; pc & \vdash T[\text{spawn} \_@ q \ (pl, ch1 \ [pc_1; \tau_1], \ ch2 \ [pc_2; \tau_2])], e_1 \text{ then } e_2 \vdash e: \tau_1 \\
\Pi; \Gamma; p; pc & \vdash e: \tau_1
\end{align*}
\]

Applying induction hypothesis to (201), we have

\[
\Pi; \Gamma; p; pc \vdash T[e_2]: \tau_1 \xrightarrow{\rho''', \Theta'', \rho', \Pi, \lambda} \tau
\]

Weakening channel environment in (202) (Lemma 20), we have

\[
\Pi; \Gamma; \Theta; p; pc \vdash e: \tau_1
\]
The condition $\Theta' |_{\text{dom}(\alpha''')} = \Theta'''$ still holds. Thus from DT-APP, we have
\[ \Pi; \Gamma; \Theta'; p; pc \vdash T[e_2] e : \tau \]

**Proof.**

Proof by induction on the relation $W$ the set of TEE principals in Lemma 24 (High Contexts without TEEs have High Holes).

**Case $v W$:** Straight forward application of induction hypothesis.

**Case $\langle W, e \rangle$:** Straight forward application of induction hypothesis.

**Case $\langle v, W \rangle$:** Straight forward application of induction hypothesis.

**Case $\text{proj}_i W$:** Straight forward application of induction hypothesis.

**Case $\text{inj}_i W$:** Straight forward application of induction hypothesis.

**Case $\eta W$:** Straight forward application of induction hypothesis.

**Case $\text{bind} x = W \text{ in } e$:** Straight forward application of induction hypothesis.

**Case $W \tau$:** Straight forward application of induction hypothesis.

**Case $\text{assume } W \text{ in } e$:** Straight forward application of induction hypothesis.

**Case $\text{send } v W \text{ then } e_{\text{sc}}$:** Straight forward application of induction hypothesis.

**Case $\text{case } W \text{ of } \text{inj}_1(x). e | \text{inj}_2(x). e$:** Straight forward application of induction hypothesis.

**Case $W \text{ where } v$:** Straight forward application of induction hypothesis.

**Case $\text{runTEE'} W$:** Syntactically not possible.

□

**Lemma 24** (High Contexts without TEEs have High Holes). Let $\Pi; \Gamma; \Theta; p; pc \vdash E[e]: \tau \triangleright \Pi'; \Gamma'; \Theta'; p'; pc' \vdash e: \tau'$ and $T$ be the set of TEE principals in $W$. If $\exists pc_H$.

1. $\Pi \triangleright H^\pi \cup pc \subseteq pc_H$
2. $\Pi; \Gamma; \Theta; p; pc_H \vdash T[e]: \tau$
3. $\Pi \triangleright H^\pi \leq \tau$

then $\exists pc'_H$ such that

1. $\Pi' \triangleright H^\pi \cup pc' \subseteq pc'_H$
2. $\Pi'; \Gamma'; \Theta'; p'; pc'_H \vdash e: \tau'$
3. $\Pi' \triangleright H^\pi \leq \tau'$

**Proof.**

Proof by induction on the relation $\Pi; \Gamma; \Theta; p; pc \vdash E[e]: \tau \triangleright \Pi'; \Gamma'; \Theta'; p'; pc' \vdash e: \tau'$.

**Case $T\text{-HOLE}$**: Straightforward as $pc' = pc$. Choose $pc'_H = pc_H$.

**Case $T\text{-LAM}$**: Straightforward application of induction hypothesis.

**Case $T\text{-APP}$**: Straightforward application of induction hypothesis.

**Case $T\text{-ARG}$**: Straightforward application of induction hypothesis.

**Case $T\text{-PAIR-LEFT}$**: Straightforward application of induction hypothesis.

**Case $T\text{-PAIR-RIGHT}$**: Straightforward application of induction hypothesis.

**Case $T\text{-PROJ}$**: Straightforward application of induction hypothesis.

**Case $T\text{-INJ}$**: Straightforward application of induction hypothesis.

**Case $T\text{-UNITM}$**: Straightforward application of induction hypothesis.

**Case $T\text{-RUNTEE}$**: Does not occur syntactically.

**Case $T\text{-BINDM}$**: Straightforward application of induction hypothesis.

**Case $T\text{-ASSUME}$**: Straightforward application of induction hypothesis.

**Case $T\text{-SEND}$**: Straightforward application of induction hypothesis.

**Case $T\text{-CASE}$**: Straightforward application of induction hypothesis.

**Case $T\text{-WHERE}$**: Applying induction to the premises, we have

\[ \Pi; (r \triangleright s) \triangleright H^\pi \cup pc \subseteq pc_H \land \\
\Pi; (r \triangleright s); \Gamma; \Theta ; p; pc_H \vdash E[e]: \tau \land \\
\Pi; (r \triangleright s) \triangleright H^\pi \leq \tau \\
\implies \\
\exists pc'_H. \Pi' \triangleright H^\pi \cup pc' \subseteq pc'_H \land \\
\Pi'; \Gamma'; \Theta'; p'; pc'_H \vdash e: \tau' \land \\
\Pi \triangleright H^\pi \leq \tau' \quad (203) \]

We are given that

\[ \Pi \triangleright H^\pi \cup pc \subseteq pc_H \text{ and } \\
\Pi \triangleright H^\pi \leq \tau \]
This means the delegation \( r \gtrdot s \) is not necessary to derive the required flows-to elation. Hence proved the case.

We are now ready to prove the type preservation of a step in the system.

**Lemma 25 (Type Preservation for the Distributed System).** Let \( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \Rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_i, e'_i \rangle \parallel \cdots \parallel \langle p_m, e'_m \rangle \) such that \( n \geq m \) and \( \forall k \in \{1, \ldots, m\} \), \( \Pi_k; \Gamma_k; \Theta_{k'; p_k}; pc_k \vdash e_k : \tau_k \). Also let,

- \( \forall \ell' \parallel \forall \{i, j\} \subseteq \{1, \ldots, m\} \parallel \Pi_i \parallel H^\pi \subseteq \ell' \Rightarrow \Pi_j \parallel H^\pi \subseteq \ell' \)
- \( \forall k \in \{1, \ldots, m\} \parallel \forall \ell'. \Pi_k \parallel H^\pi \subseteq \ell' \iff \Pi_k \parallel H^\pi \subseteq \ell' \)

Then the following hold.

1) \( \Pi_1; \ldots; \Pi_k; \Theta_{k}; \Theta_{k'; p_k}; pc_k \vdash e_k : \tau_k \) such that \( \Theta_k \subseteq \Theta_{k'} \)
2) If \( n = m + 1 \), then \( \Pi_1; \ldots; \Pi_{n'}; \Theta_{n'}; p_{n'}; pc_{n'} \vdash e_n : \tau_n \) for some \( \Pi_{n'}, \Theta_{n'}, pc_{n'} \) and \( \tau_n \)
3) If \( n = m + 1 \), then \( \forall \ell'. \Pi_n \parallel H^\pi \subseteq \ell' \iff \Pi_n \parallel H^\pi \subseteq \ell' \)
4) \( \forall \ell' \parallel \forall \{i, j\} \subseteq \{1, \ldots, n\} \parallel \Pi_i \parallel H^\pi \subseteq \ell' \iff \Pi_j \parallel H^\pi \subseteq \ell' \)

**Proof.** Proof is by induction on the system step relation (\( \Rightarrow \)).

**PAR-STEP:** Given 

\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1 : \tau_1 \parallel \cdots \parallel \Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m : \tau_m
\]

From the premises of DT-SYS, we have that \( \Pi_k; \Gamma_k; \Theta_{k}; p_k; pc_k \vdash e_k : \tau_k \) for every \( k \in \{1, \ldots, m\} \).

Also given, \( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_n \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \Rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_i, e'_i \rangle \parallel \cdots \parallel \langle p_m, e'_m \rangle \). From the premises we have that \( p_i, \emptyset \vdash e_i \Rightarrow e'_i \) for some \( i = \{1, \ldots, m\} \). Thus we have \( n = m \) and \( e'_k = e_k \) for every \( k \in \{1, \ldots, m\} \setminus \{i\} \).

For \( k = i \), invoking type preservation for single process (Lemma 18) gives us that \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e'_i : \tau_i \). Thus the new configuration is well-typed by DT-SYS.

a) **Proof for remaining results:** Since \( n = m \), we trivially have the results stated in 3 and 4.

**PAR-SPAWN:** Given

\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1 : \tau_1 \parallel \cdots \parallel \Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m : \tau_m
\]

From the premises of DT-SYS, we have that \( \Pi_k; \Gamma_k; \Theta_{k'; p_k}; pc_k \vdash e_k : \tau_k \) for every \( k \in \{1, \ldots, m\} \). Also given

\[
\langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_1, T[\text{spawn} \ \emptyset \ (pl, ch_1, pc_1; \tau_1), \ ch_2[pc_1; \tau_1], \ e \ \text{then} \ e'] \rangle \parallel \langle p_n, e_n \rangle \Rightarrow \\
\langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_1, T[e'[\nu_r]/ch_2[\nu_s/ch_2]](p_m, e_m) \parallel \langle q, e[\nu_r/ch_2[\nu_s/ch_2]] \rangle \parallel \langle p_m, e_m \rangle
\]

Here we have \( n \neq m \) and \( (e'_i, e'_n) = (T[e'], e) \). From DT-SPAWN, we have that \( \Pi_i; \emptyset; [ch_1 \mapsto \text{chan}_q-p, \ pc_1 \tau_1, \ ch_2 \mapsto \text{chan}_q-p \ pc_2 \tau_2]; q \vdash pc' \vdash e : \tau \) and thus \( pc_n = pc \). Let \( \Theta'_i = \Theta_i[ch_1 \mapsto \text{chan}_p-q \ pc_1 \tau_1, \ ch_2 \mapsto \text{chan}_p-q \ pc_2 \tau_2] \). It remains to show that

\[
\Pi_i; \Gamma_i; \Theta'_i; p_i; pc_i \vdash T[e'] : \tau_i
\]

Invoking Lemma 19, we have \( \Pi_i; \Gamma_i; \Theta'_i; p_i; pc_i \vdash T[\text{spawn} \ \emptyset \ (pl, ch_1', pc_1; \tau_1), \ ch_2[pc_1; \tau_1], \ e \ \text{then} \ e'] : \tau_i \vdash \Pi_i' ; \Gamma_i' ; \Theta'_i; p'_i; pc'_i \vdash \text{chan}_q-p \ pc_1 \tau_2; q \vdash pc' \vdash e : \tau \) and \( (e'_i, e'_n) = (T[e'], e) \). From DT-SPAWN, we have \( \Pi_i'; \Gamma_i'; \Theta'_i; p'_i; pc'_i \vdash T[e'] : \tau_i \). Invoking hole substitution (Lemma 23), we thus have \( \Pi_i; \Gamma_i; \Theta_{i'; p_i}; pc_i \vdash T[e'] : \tau_i \).

b) **Proof for remaining results:** Since \( n = m + 1 \), we have that \( \Pi_n = \Pi_i \) and so \( \Pi_n \subseteq \Pi_i \). Thus we have the results stated in condition 3 and 4.

**PAR-SEND-RECV:** Here \( n = m \). Without loss of generality, let \( (e_i, e_j) = (T[\text{send} \nu \ \emptyset \ \text{then} \ e_{s_{x_k}}], T[\text{recv} \nu \text{ as } x \text{ in } e]) \).

Then \( (e'_i, e'_j) = (T[e_{s_{x_k}}], T[e_{x \mapsto v}], T[e_{x \mapsto v}], T[e_{x \mapsto v}]) \).

We thus have \( \Pi_k; \Gamma_k; \Theta'_{k'; p_k}; pc_k \vdash e'_{k'; \tau_k} \) where \( \Theta'_{k'} = \Theta_k \) and \( e_{k'} = e_k \) for all \( k \in \{1, \ldots, m\} \setminus \{i, j\} \).

Given \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash T[\text{send} \nu \ \emptyset \ \text{then} \ e_{s_{x_k}}] : \tau_{i; p_i} \parallel \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash T[\text{recv} \nu \text{ as } x \text{ in } e] : \tau_{j; p'; c'} \parallel \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash \text{recv} \nu \text{ as } x \text{ in } e : \tau_{p'} \).

From DT-SENDDEL, we have that \( \Pi_i; \emptyset; [p'; p'_i; pc'_{i}; \vdash \nu \text{ as } x \text{ in } e \text{ for some } \Pi_i' \), such that \( \Pi_i' \subseteq \Pi_i \), and \( \Pi_j \parallel p'_i \neq pc'_i \).

Since non-bracket values sent over a channel can be typed on other places such that \( \Pi_j \parallel p'_j \neq pc'_j \) (Lemma 17), we have \( \Pi'_i; \emptyset; [p'; p'_i; pc'_{i}; \vdash \nu \text{ as } x \text{ in } e \text{ for some } \Pi'_i' \), such that \( \Pi'_i' \subseteq \Pi_i' \), and \( \Pi_j \parallel p'_j \neq pc'_j \).

If \( \nu = (v_1 \mid v_2) \), a bracket value, then there are 2 cases.

**Invert using DT-BRACKET-VALUES:** We have that \( \Pi_j \parallel H^\pi \leq \tau \). From the given conditions on the upward closure of \( H^\pi \), we have that \( \Pi_j \parallel H^\pi \leq \tau \). Thus from DT-BRACKET-VALUES, we have \( \Pi'_i; \emptyset; [p'; p'_i; pc'_{i}; \vdash (v_1 \mid v_2) : \tau \).
Invert using DT-BRACKET-WHERE: We already have that \((\hat{v}_1 \mid \hat{v}_2)\) is well-typed on node \(p_i\). That is, \(\Pi'_i; \emptyset; p'_i; pc'_i \vdash \hat{v}_i : \tau\). And so,

\[
\begin{align*}
\Pi'_i; \emptyset; p'_i; pc'_i \vdash \hat{v}_1 & \text{ where } v'_1 : \tau \\
\Pi'_i; \emptyset; p'_i; pc'_i \vdash \hat{v}_2 & \text{ where } v'_2 : \tau
\end{align*}
\]

(204) \hspace{1cm} (205)

We need to prove the following:

\[
\begin{align*}
\Pi'_j; \emptyset; p'_j; pc'_j \vdash \hat{v}_1 & \text{ where } v'_1 : \tau \\
\Pi'_j; \emptyset; p'_j; pc'_j \vdash \hat{v}_2 & \text{ where } v'_2 : \tau
\end{align*}
\]

(207) \hspace{1cm} (208)

(209)

From the given conditions on the upward closure of \(H^\pi\), we have that \(\Pi'_j \vdash H^\pi \leq \tau\). Thus from DT-BRACKET-VALUES, we have \(\Pi'_j; \emptyset; p'_j; pc'_j \vdash (v_1 \mid v_2) : \tau\) (weakening delegation and variable contexts, channel environment by invoking Lemma 12, Lemma 10).

From DT-RECV, we have \(\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc'_j \vdash e_n : \tau'_j\). Applying PC reduction (Lemma 11), we have that \(\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc'_j \vdash e_n : \tau'_j\). Invoking variable substitution (Lemma 14), we have that \(\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc'_j \vdash e_n[x \Rightarrow v] : \tau'_j\). Invoking hole substitution (Lemma 22), on \(\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash T[\text{recv } \nu \text{ as } x \text{ in } e; \Box] : \tau_j\), we have

\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e'_j : \tau_j
\]

From DT-SENDDEL, we also have that \(\Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_i \vdash e_n : \tau'_i\). Applying PC reduction (Lemma 11), we have that \(\Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_i \vdash e_n : \tau'_i\). Invoking hole substitution (Lemma 22), on \(\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash T[\text{send } \nu \text{ v then } e_{nk}] : \tau_i\), we have

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e'_i : \tau_i
\]

c) Proof for remaining results: Since \(n = m\), we trivially have the results stated in 3 and 4.

BD-PAR-STEP-L: Given

\[
\langle p_1, e_1 \rangle | \cdots | \langle p_i, (e_{i1} \mid e_{i2}) \rangle | \cdots | \langle p_m, e_m \rangle \Rightarrow \langle p_1, e'_1 \rangle | \cdots | \langle p_i, e'_i \rangle | \cdots | \langle p_m, e'_m \rangle
\]

Let \(e_i = (e_{i1} \mid e_{i2})\). From the premises of BD-PAR-STEP, we have

\[
\langle p_1, e_1 \rangle | \cdots | \langle p_i, e_{ik} \rangle | \cdots | \langle p_m, e_m \rangle \Rightarrow \\
\langle p_1, e_1 \rangle | \cdots | \langle p_i, e'_{ik} \rangle | \cdots | \langle p_m, e'_m \rangle
\]

Also from the remaining premises we have

\[
i \in \{1 \cdots m\}
\]

(210)

\[
e'_i = (e'_{i1} \mid e_{i2})
\]

(211)

\[
j = \begin{cases} 
n & \text{if } n \neq m \\
\in \{1 \cdots m\} & \text{otherwise}
\end{cases}
\]

(212)

\[
e'_n = \begin{cases} 
e'_i & \text{if } n \neq m \text{ and } j = i \\
e'_n & \text{if } n \neq m \text{ and } j \neq i
\end{cases}
\]

(213)

From DT-SYS, we have that

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i : \tau_i
\]

\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j : \tau_j
\]

We have four cases.

Case \(n = m\) and \(j = i\): Trivial case. Invoking type preservation for single process (Lemma 18), we get the conclusion.
d) Proof for remaining results: Since \( n = m \), we trivially have the results stated in 3 and 4.
Case \( n \neq m \) and \( j \neq i : e_i \) is a spawn expression. That is, we have

\[
e_i = (T_i[\text{spawn} \ @ q \ (pl, ch_r[pc_r]; \tau_r), \ ch_s[pc_s]; \tau_s]). \ e \ \text{then} \ e_n \ | \ e_{i2}
\]

\[
e'_i = (T_i[e_n] \ | \ e_{i2})
\]

\[
e'_j = e'_n = (e \ | \ \ast)
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i : \tau_i
\]

Note that TEE's do not have any spawn statement. Thus \( T_i \) is actually \( E_i \). That is,

\[
e_i = (E_i[\text{spawn} \ @ q \ (pl, ch_r[pc_r]; \tau_r), \ ch_s[pc_s]; \tau_s]). \ e \ \text{then} \ e_n \ | \ e_{i2}
\]

\[
e'_i = (E_i[e_n] \ | \ e_{i2})
\]

\[
e'_j = e'_n = (e \ | \ \ast)
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i : \tau_i
\]

From the DT-BRACKET (since it is an expression, we cannot invert using DT-BRACKET-VALUES or DT-BRACKET-WHERE), we have that \( e_i \) is protected for some \( pc'_i \) and so:

\[
\Pi_i \vdash (H^\pi \cup pc_i) \subseteq pc'_i
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc'_i \vdash T_i[\text{spawn} \ @ q \ (pl, ch_r[pc_r]; \tau_r), \ ch_s[pc_s]; \tau_s]). \ e \ \text{then} \ e_n \ : \tau
\]

Inverting the above expression using DT-SPAWN, we have:

\[
\Pi'_i; \emptyset; \emptyset[ch_r \rightarrow \text{chan}_q \rightarrow p'_i \ pc_r \ \tau_r, \ ch_s \rightarrow \text{chan}_q \rightarrow p'_i \ pc_s \ \tau_s]; q; pc'' \vdash e : \tau_n
\]

\[
\Pi'_i; \Gamma'_i; \Theta_i[ch_r \rightarrow \text{chan}_q \rightarrow p'_i \ pc_r \ \tau_r, \ ch_s \rightarrow \text{chan}_q \rightarrow p'_i \ pc_s \ \tau_s]; p'_i; pc' \vdash e_n : \tau
\]

\[
\Pi \vdash pc'' \subseteq pc''
\]

\[
\Pi \vdash p'_i \triangleright pc'
\]

\[
\Pi \vdash pc'' \leq \tau_n
\]

Invoking hole substitution (Lemma 23) with (223) we have

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash T_i[e_n] : \tau_i
\]

where \( \Theta'_i = \Theta_i[ch_r \rightarrow \text{chan}_q \rightarrow p'_i \ pc_r \ \tau_r, \ ch_s \rightarrow \text{chan}_q \rightarrow p'_i \ pc_s \ \tau_s] \). Weakening channel environment on (233) using Lemma 20, we have Thus, from DT-BRACKET, we have that

\[
\Pi_i; \Gamma_i; \Theta'_i; p_i; pc_i \vdash (T_i[e_n] \ | \ e_{i2}) : \tau_i
\]

We still need to show that for some \( \Pi_n \), \( \Gamma_n \), \( \Theta_n \), \( pc_n \) and \( \tau_n \), the following holds.

\[
\Pi_n; \Gamma_n; \Theta_n; q; pc_n \vdash (e \ | \ \ast) : \tau_n
\]

We need the following premises to prove that \( e'_j \) is well-typed.

\[
\Pi'_i \vdash (H^\pi \cup pc'' \subseteq pc''
\]

\[
\Pi'_i; \emptyset; \emptyset[q; pc'' \vdash e : \tau_n
\]

\[
\Pi'_i \vdash H^\pi \leq \tau_n
\]

Since high contexts (without TEE's) have high holes, applying Lemma 24 on (218), we have that

\[
\exists pc''_H. \ \Pi'_i \vdash H^\pi \cup pc'' \subseteq pc''_H
\]

\[
\Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc''_H \vdash \text{spawn} \ @ q \ (pl, ch_r[pc_r]; \tau_r), \ ch_s[pc_s]; \tau_s). \ e \ \text{then} \ e_n : \tau
\]

\[
\Pi'_i \vdash H^\pi \leq \tau
\]
Inverting (231) using DT-SPAWN we have that for some $pc'_H$:

$$\Pi'_1; \emptyset; \Theta'; q; pc'_1 \vdash e; \tau_n$$

$$\Pi \vdash pc'_H \subseteq pc''_H$$

Premise (227) follows from (230) and (234). Premise (229) follows from (226) Premise (228) follows from (233). We thus have that $(e | \bullet)$ is well-typed.

The new configuration is also well-formed as the channels inherit parent delegation contexts.

e) Proof for remaining results: Since $n = m + 1$, we have that $\Pi_n = \Pi_i$ and so $\Pi_n \subseteq \Pi_i$. Thus we have the results stated in condition 3 and 4.

Case $j \neq i$, $n = m$ and $e_j = (e_{j1} \mid e_{j2})$: If $e_j$ is a bracket value, then it must be the case that the left projections are senddel/recv expressions. Without loss of generality, assume the following:

$$e_i = (T_i[send \nu v \text{ then } e_{sx}] \mid e_{12})$$

$$e_j = (T_j[recv \nu \text{ as } x \text{ in } e_n] \mid e_{j2})$$

$$e'_i = (T_i[e_{sx}] \mid e_{12})$$

$$e'_j = (T_j[e_{en}[x \mapsto v]] \mid e_{j2})$$

$$\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i; \tau_i$$

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j; \tau_i$$

We have to show that:

$$\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1; \tau_1 \parallel \cdots \parallel$$

$$\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i; \tau_i \parallel \cdots \parallel$$

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j; \tau_j \parallel \cdots \parallel$$

$$\Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m; \tau_m$$

Inverting (239) and (240) using DT-BRACKET (since it is an expression, we cannot invert using DT-BRACKET-VALUES or DT-BRACKET-WHERE), we have that

$$\Pi_i \vdash (H^\pi \parallel pc_i) \subseteq pc'_i$$

(241)

$$\Pi_i; \Gamma_i; \Theta_i; p_i; pc'_i \vdash T_i[send \nu v \text{ then } e_{sx}]: \tau_i$$

(242)

$$\Pi_i \vdash H \leq \tau_i$$

(243)

and

$$\Pi_j \vdash (H^\pi \parallel pc_j) \subseteq pc'_j$$

(245)

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc'_j \vdash T_j[recv \nu \text{ as } x \text{ in } e_n]: \tau_j$$

(246)

$$\Pi_j \vdash H \leq \tau_j$$

(247)

Applying induction to the step relation in the premise:

$$\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1; \tau_1 \parallel \cdots \parallel$$

$$\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash T_i[e_{sx}; \Box]: \tau_i \parallel \cdots \parallel$$

(249)

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash T_j[e_n[x \mapsto v]; \Box]: \tau_j \parallel \cdots \parallel$$

(250)

Replacing (242) and (246) with (249) and (250) we have the proof.

$$\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1; \tau_1 \parallel \cdots \parallel$$

$$\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e'_i; \tau_i \parallel \cdots \parallel$$

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e'_j; \tau_j \parallel \cdots \parallel$$

$$\Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m; \tau_m$$
f) Proof for remaining results: Since \( n = m \), we trivially have the results stated in 3 and 4.

Case \( n = m \) and \( e_j = T[e] \): Applying induction hypothesis to the premise of BD-PAR-STEP-L, we have that \( \Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash e_{i_1} : \tau_i \). We already have \( \Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash e_{i_2} : \tau_i \) and so from DT-BRACKET (proving for a more restrictive case) we have

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash e'_{i_1} : \tau_i
\]

Since both \( e_i \) and \( e_j \) take a step, it must be the case that they are senddel and recv pairs. We then have two more cases.

Case \( e_j = \text{send} \nu v \) then \( e_{sk} \): Without loss of generality assume that \( e_j = \overline{\text{send}} \nu v \) then \( e_{sk} \). We then have the following:

\[
e_i = (T_i[\text{recv} \nu \text{ as } x \text{ in } e_r] \mid e_{i_2})
\]

\[
e'_{i} = (T_i[e_r[x \mapsto v]; \square] \mid e_{i_2})
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash (T_i[\text{recv} \nu \text{ as } x \text{ in } e_r] \mid e_{i_2}) : \tau_i
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash e_{i_2} : \tau_i
\]

We have to show that

\[
\Pi_j; \Gamma_j; \Theta_j; p_j; p_{c_j} \vdash T_j[(e_{sk} \mid \overline{\text{send}} \nu v \text{ then } e_{sk}; \square)] : \tau_j
\]

From (253) and DT-BRACKET (since it is an expression, we cannot invert using DT-BRACKET-VALUES or DT-BRACKET-WHERE), we have the following:

\[
\Pi_i \not\vdash (H^\Pi \cup p_{c_i}) \sqsubseteq p_{c_i'}
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash T_i[\text{recv} \nu \text{ as } x \text{ in } e_r] : \tau_i
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash e_{i_2} : \tau_i
\]

\[
\Pi_i \vdash H^\Pi \leq \tau_i
\]

Since holes can be typed under an appropriate \( p_{c_{ir}} \), invoking Lemma 19 on (258) we have

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_i} \vdash \text{recv} \nu \text{ as } x \text{ in } e_r : \tau_i \triangleright
\]

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_{c_{ir}} \vdash \text{recv} \nu \text{ as } x \text{ in } e_r : \tau_i \triangleright
\]

There are two cases depending on whether or not \( T_i \) includes runTEE. That is \( T_i = E_i \) or \( T_i \neq E_i \).

Case \( T_i = E_i \): Invoking Lemma 24 on (261) we have that

\[
\Pi'_i \not\vdash (H^\Pi \cup p_{c_{ir}}) \sqsubseteq p_{c_{ir}}
\]

\[
\Pi'_i; \Gamma'_i; \Theta'_i; p_i; p_{c_{ir}} \vdash \text{recv} \nu \text{ as } x \text{ in } e_r : \tau_i \triangleright
\]

\[
\Pi'_i \vdash H^\Pi \leq \tau_i \triangleright
\]

Inverting (263) using DT-RECV we have

\[
\Pi'_i; \Gamma'_i; \Theta'_i; p_i; p_{c_{ir}} \vdash \nu : \text{chan}_{p'_i \mapsto p''_i} p_{c_{ch}} \tau
\]

\[
\Pi; \Gamma, x : \hat{\top}; \Theta_i; p_i; p_{c} \vdash \nu : \tau'_i
\]

\[
\tau'_i \in \{\hat{\top}', \tau_i \}
\]

\[
\Pi'_i \vdash p_{c_{ir}} \sqsubseteq p_{c_{ch}}
\]

\[
\Pi'_i \vdash p_{c_{ir}} \sqsubseteq p_{c_{ir}}'
\]

\[
\Pi'_i \vdash p_{c_{ch}} \sqsubseteq p_{c_{ir}}'
\]

\[
\Pi'_i \vdash p_{c_{ir}}' \leq \tau_i'
\]

\[
\Pi'_i \vdash p'_i \geq p_{c_{ch}}
\]

\[
\Pi'_i \vdash p'_i \geq p_{c_{ir}}'
\]

Applying R-TRANS to (262) and (268), we have

\[
\Pi'_i \vdash H^\Pi \subseteq p_{c_{ch}}
\]
Case $T_i \neq E_i$: Consider the premises in (258) and (257). If $T_i$ includes $\text{runTEE}$ and $T_i[\text{recv } \nu \text{ as } x \text{ in } e_s]$ is well-typed under $pc_i'$, then $\exists pc''_i$ (since nested TEEs aren’t allowed and from Lemma 24 we have monotonic $pc$) such that

$$\Pi_i'' \vdash H^\pi \subseteq pc''_i \quad (275)$$

$$\Pi_i'' ; \Gamma_i'' ; \Theta_i'' ; p_i ; pc''_i \vdash \text{runTEE'}[E_i[\text{recv } \nu \text{ as } x \text{ in } e_s]] : \text{unit} \Box \quad (276)$$

Recall the premise from DT-TEEG

$$C = \{ch | ch \in \Theta(ch) = \text{chan}_{t=e} \quad pc' \tau \land \Pi_i'' \vdash pc''_i \subseteq pc'\}$$

for some $\Pi_i''$ such that $|_{\text{dom}(\Pi_i'')} = \Pi_i''$. Since $E_i$ cannot contain any $\text{runTEE}$ or $\text{spawn}$, we have $\Theta_i'' |_{C} = \Theta'_i$. This implies

$$\Pi_i'' \vdash H^\pi \subseteq pc_{ch} \quad (277)$$

Let us now focus on $j$th node. Since holes can be typed under appropriate $pc$, invoking Lemma 19 on (256), we have

$$\Pi_j ; \Gamma_j ; \Theta_j ; p_j ; pc_j \vdash T_j[\text{send } \nu \text{ v then } e_{sk}] : \tau_j \triangleright$$

$$\Pi_j' ; \Gamma_j' ; \Theta_j' ; p_j' ; pc_{js} \vdash \text{send } \nu \text{ v then } e_{sk} : \tau_j' \quad (278)$$

From (278) and DT-SENDDEL we have

$$\Pi_j' ; \Gamma_j' ; \Theta_j' ; p_j' ; pc_{js} \vdash \nu : \text{chan}_{p_j' \rightarrow p_j'} pc_{ch} \tau \quad (279)$$

$$\Pi_j' ; \emptyset ; \emptyset ; p_j' ; pc_{js} \vdash \nu : \tau \quad (280)$$

$$\Pi_j' \vdash pc_{js} \subseteq pc_{ch} \quad (281)$$

$$\Pi_j' ; \Gamma_j' ; \Theta_j' ; p_j' ; pc_{js} \vdash e_{sk} : \tau_j' \quad (282)$$

$$\tau_j' = \{\tau_j', \tau_j'\Box\} \quad (283)$$

$$\Pi_j' \vdash pc_{ch} \subseteq pc_{js}'' \quad (284)$$

$$\Pi_j' \vdash pc_{js} \subseteq \tau_j' \quad (285)$$

$$\Pi_j' \vdash p_j' \equiv pc_{js}'' \quad (286)$$

$$\Pi_j'' \subseteq \Pi_j' \quad (287)$$

$$\Pi_j'' \vdash pc_{js}'' \quad (288)$$

$$\Pi_j' \vdash p_j' \equiv pc_{ch} \quad (289)$$

To show that $e_j'$ is well-typed, we first need to find a $pc_{js}'$ such that DT-BRACKET holds for $(e_{sk} ; \Box | \text{send } \nu \text{ v then } e_{sk})$. That is, we need the following premises of the DT-BRACKET to type

$$\Pi_j' ; \Gamma_j' ; \Theta_j' ; p_j' ; pc_{js} \vdash (e_{sk} ; \Box | \text{send } \nu \text{ v then } e_{sk}) : \tau_j'\Box \quad (290)$$

$$\Pi_j' ; \Gamma_j' ; \Theta_j' ; p_j' ; pc_{js} \vdash (H^\pi \cup pc_{js}) \subseteq pc_{js}' \quad (291)$$

$$\Pi_j' ; \Gamma_j' ; \Theta_j' ; p_j' ; pc_{js}' \vdash \text{send } \nu \text{ v then } e_{sk} : \tau_j'\Box \quad (292)$$

$$\Pi_j' \vdash H^\pi \leq \tau_j'\Box \quad (293)$$

Let $pc_{js}' = pc_{ch}$. From premises (274), (277) and given conditions on the upward closure of $H^\pi$ we have

$$\Pi_j' \vdash H^\pi \subseteq pc_{ch} \quad (294)$$

Invoking hole substitution (Lemma 22) on (256) using the above premise and (278) we have the required proof.
Case $e_j = \text{recv } \nu \text{ as } x \text{ in } e$: Given $e_j = \text{recv } \nu \text{ as } x \in e$. We then have the following:

\[
\begin{align*}
e_i &= (T_i[\text{send } \nu \text{ then } e_{sx}] \mid e_{i2}) \\
e'_i &= (T_i[e_{sx}; \square] \mid e_{i2}) \\
\Pi; \Gamma; \Theta; p_i; pc_i \vdash e_i : \tau_i \quad (297) \\
\Pi; \Gamma; \Theta; p_i; pc_i \vdash e'_i : \tau_i \quad (298) \\
e'_j &= T_j[(e_{sx} \rightarrow \nu); \square \mid \text{recv } \nu \text{ as } x \in e] \quad (299) \\
\Pi; \Gamma; \Theta; p_j; pc_j \vdash e_j : \tau_j \quad (300) \\
\end{align*}
\]

We have to show that

\[
\Pi; \Gamma; \Theta; p_j; pc_j \vdash e'_j : \tau_j
\]

From (297) and DT-BRACKET (since it is an expression, we cannot invert using DT-BRACKET-VALUES or DT-BRACKET-WHERE), we have the following:

\[
\begin{align*}
\Pi; \Gamma; \Theta; p_i; pc_i \vdash T_i[\text{send } \nu \text{ then } e_{sx}] : \tau_i \\
\Pi; \Gamma; \Theta; p_i; pc_i \vdash e_{i2} : \tau_i \\
\Pi \vdash H^\pi \leq \tau_i
\end{align*}
\]

Since holes can be typed under an appropriate $pc_{is}$, invoking Lemma 19 on (302) we have

\[
\begin{align*}
\Pi; \Gamma; \Theta; p_i; pc_i \vdash T_i[\text{send } \nu \text{ then } e_{sx}] : \tau_i \\
\Pi; \Gamma; \Theta; p_i; pc_i \vdash \text{send } \nu \text{ then } e_{sx} : \tau'_i \\
\end{align*}
\]

From DT-SENDDEL we have

\[
\begin{align*}
\Pi''; \Gamma''; \Theta''; p''; pc_{is} \vdash v : \tau \\
\Pi''; \Theta; p''; pc_{is} \vdash v : \tau \\
\Pi'' \vdash pc_{is} \subseteq pc_{ch} \\
\Pi''; \Gamma; \Theta; p; pc_{is} \vdash e_{sx} : \tau'_i \\
\tau'_i = \{\tau'_i, \tau'_i \square\} \\
\Pi'' \vdash pc_{is} \subseteq pc_{is} \\
\Pi'' \vdash pc_{ch} \subseteq pc_{ch} \\
\Pi'' \vdash pc_{ch} \subseteq pc_{ch}' \\
\Pi'' \vdash pc_{ch} \subseteq pc_{ch}'' \\
\Pi'' \vdash pc_{ch}'' \leq \tau'_i \\
\Pi'' \subseteq \Pi'' \\
\Pi'' \vdash p'_i \succ \tau'' \\
\Pi'' \vdash p'_i \succ \tau'' \\
\Pi'' \vdash p'_i \succ pc_{ch} \\
\Pi'' \vdash p'_i \succ pc_{ch} \\
\end{align*}
\]

There are two cases depending on whether or not $T_i$ includes runTEE. That is $T_i = E_i$ or $T_i \neq E_i$.

**Case** $T_i = E_i$: Invoking Lemma 24 on (305) we have that

\[
\begin{align*}
\Pi'' \vdash (H^\pi \cup pc_{is}) \subseteq pc_{is} \\
\Pi''; \Gamma''; \Theta''; p''; pc_{is} \vdash \text{send } \nu \text{ then } e_{sx} : \tau''_i \\
\Pi'' \vdash H^\pi \leq \tau'_i \square \\
\end{align*}
\]

Applying R-TRANS to (319) and (318), we have

\[
\Pi'' \vdash H^\pi \subseteq pc_{ch} 
\]

**Case** $T_i \neq E_i$: Consider the premises in (302) and (301). If $T_i$ includes runTEE and $T_i[\text{send } \nu \text{ then } e_{sx}]$ is well-typed under $pc'_i$, then $\exists pc_{is}'$ (nested TEEs aren’t allowed and for non-TEEs we have monotonic $pc$ from Lemma 24) such that

\[
\begin{align*}
\Pi'' \vdash H^\pi \subseteq pc_{is}' \\
\Pi''; \Gamma''; \Theta''; p''; pc_{is}' \vdash \text{runTEE}(E_i[\text{send } \nu \text{ then } e_{sx}]) : \text{unit} \square \\
\Pi'' \vdash H^\pi \leq \text{unit} \square
\end{align*}
\]
Recall the premise from DT-TEEG
\[
C = \{ch \ | \ ch \in \Theta(ch) = \text{chan}_{return} \ pc \tau \land \Pi'' \vdash \ pc'' \subseteq pc\}
\]

Since \(E_i\) cannot contain any runTEE or spawn, we have \(\Theta''_i |_c = \Theta'_i\). This implies

\[
\Pi'' \vdash H^* \subseteq pc_{ch}
\] (325)

Let us now focus on \(j\th\) node. Since holes can be typed under an appropriate \(pc_{jr}\), invoking Lemma 19 on (300), we have

\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc \vdash T_j[recv \nu \ as \ x \ in \ e_{\kappa}] : \tau_j \triangleright
\]
\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{jr} \vdash recv \nu \ as \ x \ in \ e_{\kappa} : \tau'_j \boxdot
\] (326)

Inverting (326) using DT-RECEIVE we have

\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{jr} \vdash \nu : \text{chan}_{\tau'_j \rightarrow \tau'_j} pc_{ch} \tau
\]
\[
\Pi'_j \vdash pc_{jr} \subseteq pc_{ch}
\] (327) (328)

To show that \(e'_j\) is well-typed, we first need to find a \(pc'_{jr}\) such that DT-BRACKET holds for \((e_{\kappa}[x \mapsto v] | recv \nu as x in e_{\kappa})\). That is, we need the following premises to get
\(\Pi_j; \Gamma_j; \Theta_j; p_j; pc_{jr} \vdash (e_{\kappa}[x \mapsto v] | recv \nu as x in e_{\kappa}) : \tau_r\).

\[
\Pi'_j \vdash (H^* \cup pc_{jr}) \subseteq pc'_{jr}
\] (329)
\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{jr} \vdash recv \nu as x in e_{\kappa} : \tau'_i \boxdot
\] (330)
\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{jr} \vdash e_{\kappa}[x \mapsto v] : \tau'_i \boxdot
\] (331)
\[
\Pi'_j \vdash H^* \leq \tau'_i \boxdot
\] (332)

Let \(pc'_{jr} = pc_{ch}\). From premises (321), (325) and given input conditions on the upward closure of \(H^*\) we have

\[
\Pi'_j \vdash H^* \subseteq pc_{ch}
\]

Premise (329) follows from (328). We prove (330) as shown below: Inverting (300) using DT-RECV. Summarized as inference rule below.

\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{ch} \vdash ch : \text{chan}_{\tau'_i \rightarrow \tau'_i} pc_{ch} \tau \quad \Pi'_j; \Gamma'_j, x : \tau; \Theta'_j; p'_j; pc''_{jr} \vdash e_{\kappa} : \tau'_r
\]
\[
\tau'_r = \{\tau'_i, \tau'_i \boxdot\} \quad \Pi'_j \vdash pc_{ch} \subseteq pc''_{jr} \quad \Pi'_j \vdash pc'_{jr} \leq \tau'_r \quad \Pi'_j \vdash p'_j \triangleright pc_{ch} \quad \Pi'_j \vdash p'_j \triangleright pc_{jr}
\]
\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{ch} \vdash recv ch as x in e_{\kappa} : \tau'_i \boxdot
\]

To show (331), we first have to show that

\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{jr} \vdash \nu : \tau
\]

For this, we invoke the lemma that states that values sent are well-typed under places that satisfy the clearance requirement (Lemma 17) to (307). Premise (331) now follows from invoking substitution lemma on the premises of (330). We still need to show that \(\Pi'_j \vdash H^* \leq \tau'_i \boxdot\) holds. Consider the above premises: \(\Pi'_j \vdash pc_{ch} \subseteq pc''_{jr}\) and \(\Pi'_j \vdash pc'_{jr} \leq \tau'_r\). From these (329) and DP-HALT, the result follows. We now have all the premises to show

\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{jr} \vdash (e_{\kappa}[x \mapsto v] | recv \nu as x in e_{\kappa}) : \tau'_i \boxdot
\] (333)

Invoking hole substitution (Lemma 22) on (300) using the above premise we have the full proof.

\(h)\) Proof for remaining results: Since \(n = m\), we trivially have the results stated in 3 and 4.

**Case BD-PAR-SPAWN:** Similar to the spawn sub case in the proof of BD-PAR-STEP (i.e., Case \(n \neq m\) and \(j \neq i\)).

**Case BD-PAR-SEND-RECV-L:** Given

\[
e_i = T_i[[send \nu v \ then \ e_{sk} \ | \ e]]
\]
\[
e_j = T_j[[recv \nu as x in e_{\kappa} \ | \ e']]
\]
\[
e'_i = T_i[[e_{sk}; \boxdot \ | \ e]]
\]
\[
e'_j = T_j[[e_{\kappa}[x \mapsto v]; \boxdot \ | \ e']]
\] (334) (335) (336) (337)
Also given that \( e_i \) and \( e_j \) are well-typed.

\[
\Pi; \Gamma; \Theta; p_i; pc_i \vdash T_i[\text{send } \nu \text{ then } e_{\alpha k} | e] : \tau_i
\]

Invoking Lemma 19 we have that \((\text{send } \nu \text{ then } e_{\alpha k}; \square | e)\) is well typed for some \( pc_s \). That is,

\[
\Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_s \vdash \text{send } \nu \text{ then } e_{\alpha k}; \tau'_s \square \quad \Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_s \vdash e; \tau'_s \square \quad \Pi'_i \vdash H^\tau \leq \tau'_s \square
\]

So, from the second premise (following DT-SENDDEL) we have:

\[
\Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_s \vdash v : \tau
\]

\[
\Pi'_i; \Gamma; \Theta; p; pc_{is}'' \vdash e_{\alpha k} : \tau'_s
\]

\[
\tau'_i = \{ \tau'_s, \tau'_s \square \}
\]

\[
\Pi'_i \vdash pc_{is} \sqsubseteq pc_{is}''
\]

\[
\Pi'_i \vdash pc_{is}'' \leq \tau'_s
\]

\[
\Pi''_i \subseteq \Pi'_i
\]

\[
\Pi''_i \vdash p'_i \gg pc_{is}
\]

\[
\Pi'_i \vdash p'_i \gg pc_{is}
\]

\[
\Pi'_i \vdash pc_{ch}'' \gg pc_{ch}
\]

We already have \( H^\tau \leq \tau'_s \square \). Applying PC reduction (Lemma 11 to the fourth premise, we have \( \Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_s \vdash e_{\alpha k}; \square | e) \). So

\[
\Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_s \vdash (e_{\alpha k}; \square | e) : \tau'_s \square
\]

Depending on whether or not \( e_j \) is bracketed, we have two more cases.

Case \( e_j = (T_j[\text{recv } \nu \text{ as } x \text{ in } e_{\alpha k}] | e') \):

We are given that:

\[
e_j = T_j[(\text{recv } \nu \text{ as } x \text{ in } e_{\alpha k} | e')]
\]

\[
e'_j = T_j[(e_{\alpha k}[x \mapsto v] | e')]
\]

Also given

\[
\Pi; \Gamma; \Theta; p; pc_j \vdash T_j[(\text{recv } \nu \text{ as } x \text{ in } e_{\alpha k} | e')]: \tau_j
\]

Invoking Lemma 19 we have that \((\text{recv } \nu \text{ as } x \text{ in } e_{\alpha k} | e')\) is well typed for some \( pc_r \). That is,

\[
\Pi'_i; \Gamma'_j; \Theta'_j; p'_j; pc'_r \vdash \text{recv } \nu \text{ as } x \text{ in } e_{\alpha k}; \tau'_r \square \quad \Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc'_r \vdash e' : \tau'_r \square \quad \Pi'_j \vdash H^\tau \leq \tau'_r \square
\]

So, from the second premise (following DT-RECEIVE) we have:

\[
\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc'_r \vdash ch : \text{chan}_{p'_j} \rightarrow p'_i \ pc_{ch} \tau
\]

\[
\Pi'_j; \Gamma'_j, x : \tau; \Theta'_j; p'_j; pc'_r \vdash e_{\alpha k} : \tau'_r
\]

\[
\tau'_r = \{ \tau'_r, \tau'_r \square \}
\]

\[
\Pi'_j \vdash pc'_r \sqsubseteq pc_{ch}
\]

\[
\Pi'_j \vdash pc_{ch} \sqsubseteq pc'_r
\]

\[
\Pi'_j \vdash pc''_r \leq \tau'_r
\]

\[
\Pi'_j \vdash p'_j \gg pc'_r
\]

\[
\Pi'_j \vdash p'_j \gg pc_{ch}
\]

We now prove the \( \text{recv} \) part. First we have to prove that the value \( v \) is well-typed under the new context. From premise (338), we have that \( v \) can be typed under empty variable and channel environment, and a delegation context that enables a place to act for the \( pc \).
Applying Lemma 17 to (338) using (356), it then follows that

\[ \Pi_j'; \emptyset; \emptyset; p \varepsilon \pi c \vdash v : \tau \]

Weakening channel environment for values (Lemma 12) and variable context in the above judgment, we have:

\[ \Pi_j'; \Gamma_j'; \Theta_j'; p \varepsilon \pi c \vdash v : \tau \]

From variable substitution lemma (Lemma 14) we have

\[ \Pi_j'; \Gamma_j'; \Theta_j'; p \varepsilon \pi c \vdash \varepsilon_k[x \mapsto v] : \tau_i' \]

Thus we have

\[ \Pi_j; \Gamma_j; \Theta_j; p \varepsilon \pi c \vdash (\varepsilon_k[x \mapsto v] ; \Box | e') : \tau_i'^\Box \]

Invoking hole substitution (Lemma 22), we thus have

\[ \Pi_i; \Gamma_i; \Theta_i; p_i; \pi c_i \vdash T_i[(\varepsilon_k ; \Box | e)] : \tau_i \]

and

\[ \Pi_j; \Gamma_j; \Theta_j; p_j; \pi c_j \vdash T_j[(\varepsilon_k[x \mapsto v] ; \Box | e') : \tau_j] \]

Case \( e_j = T_j[\text{recv} \nu \text{ as } x \text{ in } \varepsilon_k] \):

\[ e_j = T_j[\text{recv} \nu \text{ as } x \text{ in } \varepsilon_k] \]

(358)

\[ e'_j = T_j[(\varepsilon_k[x \mapsto v] ; \Box | \text{recv} \nu \text{ as } x \text{ in } \varepsilon_k)] \]

(359)

The proof is similar to the case \( e_j = \text{recv} \nu \text{ as } v \text{ in } \varepsilon_k \) in the proof of BD-PAR-STEP-L.

i) Proof for remaining results: Since \( n = m \), we trivially have the results stated in 3 and 4.

Case BD-PAR-SEND-RECV-R: Similar to above case except that we prove when right projection takes a step.

Case BD-PAR-RECV-SEND-L: Similar to the proof of BD-PAR-SEND-RECV-L except that we now prove

\[ T_j[(\Box | \text{send} \nu \text{ then } \varepsilon_k)] \]

is well-typed.

Case BD-PAR-RECV-SEND-R: Similar to the proof of BD-PAR-SEND-RECV-R.

This completes the type preservation proof for the distributed system.

Using the Lemma 25, we will prove Theorem 1 restated as below. The key insight is that a well-typed DFLATE configuration cannot evaluate to bracketed final values on the attacker node \( p_j \).

**Theorem 3** (DFLATE noninterference with clearance). Let \( e_k \) for \( k \in \{1 \ldots m\} \) be DFLATE programs such that

\[ \Pi_{init}; \Gamma_k; \Theta_k; p_k; \pi c_k \vdash e_k : \tau_k, \text{ where } \tau_j = \ell \text{ says bool} \] and \( x : H \) says \( \tau \in \Gamma_i \) for some \( H \), and for all \( k \)

Processes do not downgrade \( H \):

\[ \forall k \in \{1 \ldots m\}. \forall \ell'. \Pi_{init} \triangleright H \equiv \ell' \iff \Pi_k^D \triangleright H \equiv \ell' \]

The attacker has limited authority:

\[ \Pi_{init} \not\triangleright H \not\equiv \ell \]

Then for all \( v_z, z \in \{1, 2\} \) such that \( \Pi; \Gamma_i; \Theta_i; p_i; \pi c_i \vdash v_z : H \) says \( \tau \), if \( \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, e_i[x \mapsto v_z] \rangle \| \cdots \| \langle p_m, e_m \rangle \)

steps to \( \langle p_1, e'_1 \rangle \| \cdots \| \langle p_i, e'_i \rangle \| \cdots \| \langle p_j, \hat{v}_j \rangle \| \cdots \| \langle p_m, e'_m \rangle \rangle \) we have \( \hat{v}_j = \hat{v}_j \).  

Proof. Given that

\[ \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, e_i[x \mapsto v_z] \rangle \| \cdots \| \langle p_m, e_m \rangle \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \| \cdots \| \langle p_j, \hat{v}_j \rangle \| \cdots \| \langle p_m, e'_m \rangle \rangle \]

Also given that

\[ \Pi_i; \Gamma_i, x : H \text{ says } \tau, \Theta_i; p_i; \pi c_i \vdash e_i : \tau_i \]

From DT-BRACKET-VALUES (note that since they are user-provided inputs, they cannot contain where terms), we have that

\[ \Pi_i; \Gamma_i, x : H \text{ says } \tau. \text{ Invoking substitution lemma (Lemma 14) we have that } \Pi_i; \Gamma_i, x : H \vdash e_i[x \mapsto (v_1 \mid v_2)] : \tau_i. \] From the type preservation (Lemma 25) we have that for all \( k \in \{1 \ldots n\} \) \( \Pi_k; \Gamma_k; \Theta_k; p_k; \pi c_k \vdash e_k : \tau_k \) such that \( \Theta_k \supseteq \Theta_k \). We prove for each case of \( \tau \) separately.

From the completeness property (Lemma 5), we have that

\[ \langle p_1, e_1 \rangle \| \cdots \| \langle p_i, e_i[x \mapsto (v_1 \mid v_2)] \rangle \| \cdots \| \langle p_m, e_m \rangle \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \| \cdots \| \langle p_j, \hat{v}_j \rangle \| \cdots \| \langle p_m, e'_m \rangle \rangle \]
and from the soundness property (Lemma 2), we have that \( |v_j'|_z = v_j' \) for \( z = \{1, 2\} \).

From the type preservation lemma, we have that \( \Pi_j; \Gamma_j; \Theta_j'; p_j; pc_j \vdash v_j': \ell \) says bool. We have to prove that

\[
|v_j'|_1 = |v_j'|_2
\]

Let us assume that \( v_j' \) is a bracket value. Then by DT-BRACKET-VALUES (or DT-BRACKET-WHERE), we have the following:

\[
\begin{align*}
\Pi_j; \Gamma_j; \Theta_j'; p_j; pc_j & \vdash [v_j']_1 : \tau_j \quad \text{(362)} \\
\Pi_j; \Gamma_j; \Theta_j'; p_j; pc_j & \vdash [v_j']_2 : \tau_j \quad \text{(363)} \\
\Pi_j & \vdash H^\tau \preceq \tau_j \quad \text{(364)}
\end{align*}
\]

From (364), we require that \( \Pi_j \vdash H^\tau \subseteq \ell \) (rule DP-LBL). But from condition (361) we are already given that \( \Pi_j \not\vdash H^\tau \wedge H^\tau \subseteq \ell \). Thus \( \Pi_j; \Gamma_j; \Theta_j'; p_j; pc_j \vdash v_j': \tau_j \) cannot be well-typed by DT-BRACKET-VALUES and so \( v_j' \) itself isn’t a bracket term.

Note that \( v_j' \) can only be a where term. We can prove this by induction on the structure of the value. The only interesting case is \( \eta_v \, v'' \). In this case, we can easily prove that \( v'' \) cannot be a bracket term because subtypes (bool = unit + unit) cannot protect any principal.

Without loss of generality, let \( v_j' = w \) where \( \langle p \iddots q \rangle \). We now need to prove that \( w \) is not a bracket term. We prove this by induction on the number of where (either bracket or non-bracket) terms. For base case, where there are zero where terms, we already proved that \( v_j' \) is not a bracket term.

j) **Induction Hypothesis:** Let \( v_j' = w \) where \( ^{n-1}p \iddots q \iddots q_n \) where \( \langle p \iddots q \rangle \). For \( k = \{0 \ldots n - 1\} \), \( w \) where \( \langle p_k \iddots q_k \rangle \) is not a bracket term.

k) **Induction Step:** For the induction step, we need to prove that \( v_j' = w \) where \( \langle p \iddots q \rangle \) where \( ^{n-1}p \iddots q \iddots q_n \) where \( \langle p \iddots q \rangle \) is not a bracket term. From the induction hypothesis, we already have that \( w \) where \( \langle p \iddots q \rangle \) where \( \langle p_k \iddots q_k \rangle \) where \( \langle p \iddots q \rangle \) is not a bracket term for \( k = \{1 \ldots n\} \). Thus it remains to prove that \( w \) where \( \langle p \iddots q \rangle \) is not a bracket term.

Case \( \pi \rightarrow \): From condition (361), we have \( \Pi_j \not\vdash H^\tau \subseteq \ell^\rightarrow \) and so we have that \( \Pi_j \not\vdash \ell^\rightarrow \supseteq H^\tau \) where \( \Pi_j = \Pi_j \), \( \langle p \iddots q \rangle \).

Note that this is the same as \( \Pi_j \not\vdash H^\tau \subseteq \ell^\rightarrow \). Running an argument similar to the base case, we have that \( w \) cannot be a bracket term (as \( \Pi_j \not\vdash \ell \leq \tau_j \)).

Case \( \pi \leftarrow \): Similar to above, using condition (361), we have \( \Pi_j \not\vdash H^\tau \subseteq \ell^\rightarrow \). Again \( w \) cannot be a bracket term.

This completes the proof that \( v_j' \) isn’t a bracket term and so \( |v_j'|_1 = |v_j'|_2 \).

We elaborate the erasure/observation function in the below table.

| \( O((\cdot), \Pi, A) \) | = \cdot |
| \( O(\langle p \iddots q \rangle, \Pi, A) \) | = \cdot |
| \( O(x, \Pi, A) \) | = x |
| \( O(\eta, e', \Pi, A) \) | = \eta \, O(e', \Pi, A) |
| \( O(\lambda(x: \tau)[p; \Theta, P, \Pi \Lambda], e', \Pi, A) \) | = \lambda(x: \tau)[p; \Theta, P, \Pi \Lambda], O(e', \Pi, A) |
| \( O(e' e'', \Pi, A) \) | = O(e', \Pi, A) \, O(e'', \Pi, A) |
| \( O((e_1, e_2), \Pi, A) \) | = \langle O(e_1, \Pi, A), O(e_2, \Pi, A) \rangle |
| \( O(\text{proj}_1 e', \Pi, A) \) | = \text{proj}_1 O(e', \Pi, A) |
| \( O(\text{proj}_2 e', \Pi, A) \) | = \text{proj}_2 O(e', \Pi, A) |
| \( O(\text{case } e' \text{ of } \text{inj}_1(x). e_1 \mid \text{inj}_2(x). e_2, \Pi, A) \) | = case \( O(e', \Pi, A) \) of \( \text{inj}_1(x) \). \( O(e_1, \Pi, A) \) | \( \text{inj}_2(x) \). \( O(e_2, \Pi, A) \) |
| \( O(\text{bind } x = e' \text{ in } e'', \Pi, A) \) | = bind \( x = O(e', \Pi, A) \) in \( O(e'', \Pi, A) \) |
| \( O(\text{assume } e' \text{ in } e'', \Pi, A) \) | = assume \( O(e', \Pi, A) \) in \( O(e'', \Pi, A) \) |
| \( O(e' \text{ where } v, \Pi, A) \) | = \text{where } v \, O(e', \Pi, A) |
| \( O(\text{TEE}' e', \Pi, A) \) | = O_{\text{tee}}(\text{TEE}' e', \Pi, A) |
| \( O(\text{runTEE}' e', \Pi, A) \) | = O_{\text{runtee}}(\text{TEE}' e', \Pi, A) |
| \( O(\text{spawn } \hat{q} (p_1, ch[p; \tau], ch[p; \tau]), e' \text{ then } e'', \Pi, A) \) | = \text{spawn } \hat{q} (p_1, ch[p; \tau], ch[p; \tau]). \( O(e', \Pi, A) \) then \( O(e'', \Pi, A) \) |
| \( O(\text{send } ch \text{ e' then } e_{sn}, \Pi, A) \) | = \text{send } ch \, O(e', \Pi, A) \text{ then } O(e_{sn}, \Pi, A) |
| \( O(\text{recv } ch \text{ as } x \text{ in } e', \Pi, A) \) | = \text{recv } ch \text{ as } x \text{ in } O(e', \Pi, A) |

Erasure functions for sealed values and TEEs are defined in Figure 25. We lift the erasure of expressions to a process as follows.

\[ O((q, e), \Pi, A) = \langle q, O(e, \Pi, A) \rangle \]
Definition C.1 (Trace Deduplication).

Duplicated value if they are the same. Duplicates in traces are removed using the below definition. It simply compares the pairwise elements and eliminates the duplicated value if they are the same.

Definition C.2 (Trace Equivalence). Two traces, \( Tr_1 \) and \( Tr_2 \), are equivalent, denoted as \( Tr_1 \approx Tr_2 \), if they are equal after removing the duplicates. That is

\[ Tr_1 \approx Tr_2 \iff U(Tr_1) = U(Tr_2) \]

Before we prove the noninterference for the stronger model, we prove that if two non-bracketed executions (left and right) compute a value on a process running on the attacker node \( p_j \), then there exists a bracketed execution such that the projections of the traces of the process in the bracketed execution is equal to that of the left and right executions. We first introduce some scheduling terminology.

Definition C.3 (Schedule). Let a system take \( k \) number of steps. Then schedule, \( S \), is the sequence of set of nodes on which the expressions are reduced in each step. If

\[ \langle p_1, e^1_p \rangle \parallel \cdots \parallel \langle p_i, e^i_p \rangle \parallel \cdots \parallel \langle p_j, e^j_p \rangle \parallel \cdots \parallel \langle p_m, e^m_p \rangle \]

then, schedule, \( S = \langle P_i \rangle_{i=1}^k \) where \( P_i \) is the set of nodes reduced at \( i^{th} \) step.

Remark C.1. Note that the cardinality of \( P_i \) is at least 1 and at most 2.

Example C.1. Consider the following evaluation.

\[ \langle p, \text{bind } x = v \text{ in send } ch x \text{ then } e_{sn} \rangle \parallel \langle q, \text{recv } ch \text{ as } y \text{ in } y \rangle \]

\[ \implies \]

\[ \langle p, \text{send } ch v \text{ then } e_{sn} \rangle \parallel \langle q, \text{recv } ch \text{ as } y \text{ in } y \rangle \]

\[ \implies \]

\[ \langle p, () \rangle \parallel \langle q, v \rangle \]

Remark C.1. Then, \( S = \{p\}, \{p, q\} \).

Definition C.4 (Scheduling order of a node). Let \( S \) be the schedule of a system. Then scheduling order of a node \( p \), written, \( [S]_p \), is the sequence of elements in the schedule containing \( p \). That is,

\[ [S]_p = \begin{cases} hd(S), [tail(S)]_p & \text{if } p \in hd(S) \\ [tail(S)]_p & \text{if } p \notin hd(S) \end{cases} \]

Example C.2. In the example C.1, \( [S]_p = \{p\}, \{p, q\} \) and \( [S]_q = \{p, q\} \)

Lemma 26 (Race Freedom). send and recv are race-free.
**Proof Sketch:** DFLATE channels are unidirectional. It has two endpoints and can either send or recv between these endpoints. Thus the order of communication is deterministic and race-free.

**Lemma 27** (Evaluation of a process is deterministic). Let $S_1$ and $S_2$ be two different schedules of a DFLATE program.

$$S_1 = \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_i, e'_i \rangle \parallel \cdots \parallel \langle p_n, e'_n \rangle$$

$$S_2 = \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e''_1 \rangle \parallel \cdots \parallel \langle p_i, e''_i \rangle \parallel \cdots \parallel \langle p_n, e''_n \rangle$$

such that $|S_1|_p = |S_2|_p$, then $\langle p_i, e'_i \rangle = \langle p_i, e''_i \rangle$

**Proof Sketch:** Given that DFLATE programs are race-free (Lemma 26), evaluation of a process is deterministic.

**Definition C.5** (Commuting Schedules). Two schedules $S_1$ and $S_2$ are said to be commuting if they preserve the scheduling order of all nodes. That is,

$$\forall p, |S_1|_p = |S_2|_p$$

**Example C.3.**

| $S$ | $|S|_p$ |
|-----|-------|
| $S_1 = \langle p \rangle, \{ p, q \}, \{ r \}, \{ p \}, \{ p, r \}$ | $\{ p \}, \{ p, q \}, \{ p \}, \{ p, r \}$ |
| $S_2 = \langle p \rangle, \{ p, q \}, \{ r \}, \{ p \}, \{ p, r \}$ | $\{ p \}, \{ p, q \}, \{ p \}, \{ p, r \}$ |
| $S_3 = \langle p \rangle, \{ p, q \}, \{ r \}, \{ p \}, \{ p, r \}$ | $\{ p \}, \{ p, q \}, \{ p \}, \{ p, r \}$ |

From the second column, we see that $S_1$ and $S_2$ are commuting but $S_3$ does not commute with either $S_1$ or $S_2$.

**Lemma 28** (Trace of a process in commuting schedules). The trace of a process in two commuting schedules is equal (upto stuttering).

**Proof.** Since commuting schedules preserve the scheduling order of a process, trace remains unchanged (upto stuttering). \(\square\)

A schedule for bracketed execution contains a sequence of pairs of processes scheduled at each step.

**Lemma 29** (Bracketed Schedule is a Prefix of First Execution). Let $S_1$ and $S_r$ be the left and right executions shown below.

$$S_1 = \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i[x \mapsto v_i] \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_i, e'_i \rangle \parallel \cdots \parallel \langle p_m, e'_m \rangle$$

Let $S_{(\cdot \cdot \cdot)}$ be the corresponding bracketed execution shown below.

$$S_{(\cdot \cdot \cdot)} = \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i[x \mapsto (v_i \mid v_r)] \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e^*_1 \rangle \parallel \cdots \parallel \langle p_i, e^*_i \rangle \parallel \cdots \parallel \langle p_m, e^*_m \rangle$$

If $P$ is the set of processes in $S_{(\cdot \cdot \cdot)}$, then $\forall p \in P, |S_{(\cdot \cdot \cdot)}|_1 p \leq |S_1|_p$ where $\leq$ is a prefix where $|S_{(\cdot \cdot \cdot)}|_1$ is the left projection of the bracketed schedule. Similar statement holds for right projection of the bracketed schedule.

**Proof.** We induct on the length of the $S_{(\cdot \cdot \cdot)}$ which is same as the number of the evaluation steps of the bracketed execution.

**Base Case:** Given $|S_{(\cdot \cdot \cdot)}|_1 = P_1$. Hence

$$|S_{(\cdot \cdot \cdot)}|_1 p = \begin{cases} \{ P_1 \} & \text{if } p \in P_1 \\ \emptyset & \text{otherwise} \end{cases}$$

Note that both executions start with the same configuration. Since evaluation of a process for the same number of steps is deterministic (Lemma 27), we have $|S_1|_p = P_1$ if $p \in P_1$ else $\emptyset$. Thus,

$$\forall p \in P, |P_1|_p \leq |S_1|_p$$

This proves the base case.

**Inductive Case:** Let $\text{len}(S_{(\cdot \cdot \cdot)}) = k + 1$. Given that

$$\forall p, |S_{(\cdot \cdot \cdot)}|_1 [1 : k]_p \leq |S_1|_p$$

Let $|S_{(\cdot \cdot \cdot)}|[k + 1]_p = P_{k+1}$. Hence

$$|S_{(\cdot \cdot \cdot)}|_1 p = \begin{cases} |S_{(\cdot \cdot \cdot)}|_1 [1 : k]_p, P_{k+1} & \text{if } p \in P_{k+1} \\ |S_{(\cdot \cdot \cdot)}|_1 [1 : k]_p & \text{otherwise} \end{cases}$$

Let $\text{len}(|S_{(\cdot \cdot \cdot)}|_1 [1 : k]_p) = k'$. This implies that the bracketed execution has taken $k'$ number of steps for process $p$. From induction hypothesis, we have that $|S_{(\cdot \cdot \cdot)}|_1 [1 : k]_p \leq |S_1|_p$. That implies, $|S_{(\cdot \cdot \cdot)}|_1 [1 : k]'_p = |S_1|_p [1 : k']$. That is, the left execution has also taken $k'$ number of steps on node $p$. Thus the configuration is same for process $p$ (Lemma 27).
If \( P_{k+1} \models 2 \), then \( \exists q \) such that \( q \neq p \) and \( q \in P_{k+1} \). Following similar reasoning, we have that the configuration for process \( q \) is also same in both bracketed and left execution. Thus they take step in the same way and so \( [\hat{\cal S}(1)]_{[1: k+1]}^p = [\hat{\cal S}]_{[1: k+1]}^p \). Thus \( [\hat{\cal S}(1)]_{[1: k+1]}^p \preceq [\hat{\cal S}]_{[1]}^p \).

Similar proof follows for right execution. Hence the proof. □

We now prove the noninterference for stronger confidentiality attacker stated in Theorem 2 (and restated in an equivalent way below). Note that the statement expands the definition of trace equivalence using the observation function.

**Theorem 4 (DFLATE Noninterference with Stronger Observational Model).** Let \( e_k \) for \( k \in \{1 \ldots m\} \) be DFLATE programs such that \( \Pi^i_\text{init}; \Gamma^i_\text{init} ; \Theta^i_k ; p^i_k ; p^i_c k \vdash e_k : \tau_k \) and \( x : H^\to \) says \( \hat{\tau} \in \Gamma^i_k \) for some \( H^\to \), such that

\[
\forall k \in \{1 \ldots m\}, \forall \ell. \Pi^i_\text{init} \vdash H \subseteq \ell \Leftrightarrow \hat{\Pi}^i_k \vdash H \subseteq \ell
\]

The attacker has limited authority:

\[
\Pi^i_\text{init} \not\models p_j \Rightarrow H^\to
\]

For all \( z, z \in \{1, 2\} \) such that \( \Pi^i; \Gamma^i_\text{init} ; \Theta^i; p^i; p^i_c \vdash v_z : H^\to \) says \( \hat{\tau} \), if

\[
\cal S_l = \langle p_1, e_1 \rangle \cdots \| \cdots \| \langle p_i, e_i[x \rightarrow v_l] \rangle \cdots \| \cdots \| \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \cdots \| \cdots \| \langle p_i, e_i' \rangle \cdots \| \cdots \| \langle p_m, e_m' \rangle \]
\]

and

\[
\cal S_r = \langle p_1, e_1 \rangle \cdots \| \cdots \| \langle p_i, e_i[x \rightarrow v_r] \rangle \cdots \| \cdots \| \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \cdots \| \cdots \| \langle p_i, e_i' \rangle \cdots \| \cdots \| \langle p_m, e_m' \rangle \]
\]

then traces of the process executing on node \( p_j \), as observed by the attacker on node \( p_j \), are equivalent in both executions. That is,

\[
\cal O(\langle p_j, v_{1j} \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-), \ldots, \cal O(\langle p_j, v_{mj} \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-) \approx \cal O(\langle p_j, v_{1j} \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-), \ldots, \cal O(\langle p_j, v_{mj} \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-)
\]

where \( e^s \) represents the \( s \)th step of the system.

**Proof.** We have that the initial configuration of both left and right executions can be projected from bracketed execution. That is,

\[
\langle p_1, e_1 \rangle \cdots \| \cdots \| \langle p_i, e_i[x \rightarrow (v_l \mid v_r)] \rangle \cdots \| \cdots \| \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \cdots \| \cdots \| \langle p_i, e'_i \rangle \cdots \| \cdots \| \langle p_m, e'_m \rangle \]
\]

and from the soundness property (Lemma 2), we have that \( [v^s_{1j}]_1 = v_{1j} \) and \( [v^s_{2j}]_2 = v_{2j}. \) Now, consider any intermediate step: \( \langle p_j, e'_j \rangle \). From type preservation (Lemma 25), we have \( \Pi^i; \Gamma^i_\text{init} ; \Theta^i; p^i; p^i_c \vdash e'_j : \tau_j \). We have to prove that:

\[
\cal O(\langle p_j, e'_j_1 \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-) = \cal O(\langle p_j, e'_j_2 \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-)
\]

It is clear that \( e'_j \) itself is not a bracket expression as it would violate the clearance requirement. That is, assume that \( e'_j \) is a bracket expression. Then as per DT-BRACKET, we have \( \Pi^i \vdash H^\to \subseteq p^i_c \) for some \( p^i_c \) and \( \Pi^i; \Gamma^i_\text{init} ; \Theta^i; p^i; p^i_c \vdash e'_j : \tau_j \) (analogously, \( \Pi^i; \Gamma^i_\text{init} ; \Theta^i; p^i; p^i_c \vdash e'_j_2 : \tau_j \)). From the clearance premise, we have \( \exists \Pi^i_j \vdash p_j^- \Rightarrow p^i_c \). By transitivity, we thus have \( \Pi^i_j \vdash p_j^- \Rightarrow H^\to \). However, we are given that \( \Pi^i_j \not\models p_j^- \Rightarrow H^\to \) which is a contradiction. Thus \( e'_j \) itself is not a bracket.

Now, assume that:

\[
\cal O(\langle p_j, e'_j_1 \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-) \neq \cal O(\langle p_j, e'_j_2 \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-)
\]

Then there should be some subterm \( e \) of \( e'_j \) such that

\[
\cal O(\langle p_j, e_1 \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-) \neq \cal O(\langle p_j, e_2 \rangle, \hat{\Pi}^i_\text{D}(j), p_j^-)
\]
We have 2 cases: either $e$ itself is some bracketed value $(\hat{v}_1 \mid \hat{v}_2)$ that is well-typed by $\mathbb{DT-Bracket-Values}$ or $e$ is some well-typed $\mathbb{TEE}^t(e_1 \mid e_2)$ or $\mathbb{runTEE}^t(e_1 \mid e_2)$.

**Case 1:** Let $(\hat{v}_1 \mid \hat{v}_2)$ be a well-typed bracket term. That is, $\Pi''_j; \Theta''_j; p_j; p_{c'}'' \vdash (\hat{v}_1 \mid \hat{v}_2); \tau$. Then from $\mathbb{DT-Bracket-Values}$, we require that $\Pi''_j \vdash H^- \subseteq \tau$. This implies that for $k \in \{1, 2\}$, $\hat{v}_k \in \{(), \langle \hat{v}', \hat{v}'', \langle p \gg q \rangle \}, \eta, \eta, \eta \}$ as other values cannot be protected.

**What happens for $(v_1 \mid v_2 \mid v_3 \mid v_4)$?** Note that if $(v_1 \mid v_2 \mid v_3 \mid v_4)$ is well-typed under $\mathbb{DT-Bracket-Where}$, then $\mathbb{O}((v_1 \mid v_2 \mid v_3 \mid v_4), \hat{\Pi}_{D_{(i)}}, \ell^-)$ has to be $\bullet$. This is because, if $\Pi''_j; \Theta''_j; p_j; p_{c'}'' \vdash (v_1 \mid v_2 \mid v_3 \mid v_4); \tau$, then investing by $\mathbb{DT-Bracket-Where}$, we have

$$\Pi''_j; \Gamma''_j; \Theta''_j; p_j; p_{c'}'' \vdash v_1 \mid v_2; \tau$$

From the last premise, we have that $v_1$ and $v_3$ are protected. From the grammar of values, we have that $v_1, v_3 \in \{(), \langle p \gg q \rangle \}, \eta, \eta, \eta$ where $v''$. Using induction, we can prove that if $v$'s type is protected, then erasure of $v$ is $\bullet$.

If $v_k = \eta, \eta, \eta$, that is, $(\hat{v}_1 \mid \hat{v}_2) = (\eta, \eta, \eta)$, then we require that $\Pi''_j \vdash H^- \subseteq \ell'$. Since all delegations in $\Pi''_j$ belong to $\hat{\Pi}_{D_{(i)}}, \hat{\Pi}_{D_{(i)}, \ell^-}$, we have that $\mathbb{O}(\eta, \eta, \eta, \eta, \hat{\Pi}_{D_{(i)}}, \ell^-) = \eta, \eta, \eta$: $\bullet$ and $\mathbb{O}(\eta, \eta)$, all $\eta, \eta, \eta, \eta, \eta, \eta$. Hence they are equal after erasure. Remaining terms can be proved using induction that the erasure results in same terms.

**Case 2:** Let the expression be $\mathbb{TEE}^t(e_1 \mid e_2)$. Then from $\mathbb{DT-Bracket}$, we require that $\Pi''_j \vdash p_{c''} \gg H^-$ and $\Pi''_j; \Gamma''_j; \Theta''_j; t; p_{c''} \vdash e_1; \tau$ for $i \in \{1, 2\}$. Then from the clearance (Lemma 7), we have that $\Pi''_j \vdash t^- \gg H^-$. This implies that $\Pi''_j \vdash t^+ \gg H^-$. Then so $\mathbb{O}(\mathbb{TEE}^t e_1, \hat{\Pi}_{D_{(i)}}, \ell^-) = \mathbb{TEE}^t \bullet$ and $\mathbb{O}(\mathbb{TEE}^t e_2, \hat{\Pi}_{D_{(i)}}, \ell^-) = \mathbb{TEE}^t \bullet$. Hence they are equal after erasure. Similarly for $\mathbb{runTEE}^t(e_1 \mid e_2)$.

Repeatedly applying type preservation will thus give that

$$\mathbb{O}(\langle p_j, \lfloor e_j \rfloor_1\rangle, \hat{\Pi}_{D_{(i)}}, p_j^-), \ldots, \mathbb{O}(\langle p_j, \lfloor e_j \rfloor_1\rangle, \hat{\Pi}_{D_{(i)}}, p_j^-)$$

However, we still need to prove that the trace for $p_j$ node in bracketed execution equals the trace in corresponding executions. Consider the following two executions: given individual execution with schedule $S_i$ and bracketed execution projected on the left side with schedule, $S_{\mid j}$. Further, we assume that the length of the $S_i$ is the minimum number of steps required to reduce $\lfloor e_j \rfloor_1$ on node $p_j$ to a value. Note that this may incur evaluating other nodes due to communication. However, the schedule for the bracketed execution eliminates evaluation on unnecessary nodes.

We now argue that $S_\mid j$ commutes with $S_i$ for the first $s$ steps. Lemma 29 allows us to reschedule $S_i$ to $S_{\mid j}$ such that $[S_{\mid j}[1 : s]]_1 = S_{\mid j}[1 : s]'$. The schedule can be completed such that it satisfies the property

$$\forall p, [S_i]_p = [S_{\mid j}]_p$$

Note that such a construction exists but we elide the actual details. Since $S_i$ and $S_{\mid j}$ are commuting, their traces for node $p_j$ are same (Lemma 28).

Also note that trace of node $p_j$ after $s$ steps in $S_{\mid j}$ is simply a chain of $\langle p_j, v''_j \rangle$ and deduplication removes them completely. So we only consider the trace generated by the schedule $S_{\mid j}[1 : s]$. However, this is equal to the $S_{\mid j}$'s. This implies that if both executions start in the same configuration, they take same number of steps on each node and thus end in same configuration. Thus traces generated by $S_{\mid j}$ (and hence $S_i$) and $S_{\mid j}$ are equal.

Similarly, we can prove that trace of node $p_j$ generated by the second execution $S_i$ and bracketed execution $S_{\mid j}$ is same. This implies that we can now use traces of bracketed execution to reason about the trace equivalence. From (368), we already proved that the projected traces of a bracketed execution are equal. Hence proved.

**Appendix D**

**FLAM and FLAC**

The following lemma establishes a tight connection between FLAM and FLAC.

**Lemma 30** (FLAC implies FLAM). Let $\Pi = \mathcal{H}(c)$. If $\Pi; pc; \ell \vdash p \gg q$, then $\mathcal{H}; c; pc; \ell \vdash p \gg q$.

**Proof.** Proof is by induction on the derivation of the robust assumption $\Pi; pc; \ell \vdash p \gg q$. Interesting case is $R-ASSUME$.

**Case R-Assume:** From the premises, we have, that
\( \langle p \gg q \mid \ell \land \nabla(q) \rangle \in \Pi \) \hspace{1cm} (369)
\[ \Pi; pc; \ell \vdash pc \sqcup \ell \leq \tau \] \hspace{1cm} (370)
\[ \Pi; pc; \ell \vdash pc \gg \nabla(q) \] \hspace{1cm} (371)
\[ \Pi; pc; \ell \vdash \nabla(p^{-}) \gg \nabla(q^{-}) \] \hspace{1cm} (372)

From (369) and DEL, we have that
\[ \mathcal{H}; c; pc; \ell' \vdash p \gg q \]

From (370) and [ Weaken], we get that \( \mathcal{H}; c; pc; \ell \land \nabla(q) \vdash p \gg q \). From the (371), (372) and R-LIFT we thus have \( \mathcal{H}; c; pc; \ell \vdash p \gg q \).

**Case R-Static:** Since \( L \models p \gg q \), we have that
\[ \mathcal{H}; c; \bot^{-} \land \top^{-}; \ell \vdash p \gg q \]

From FLAM R-STATIC, we thus have, \( \mathcal{H}; c; pc; \ell \vdash p \gg q \).

**Case R-ConjR:** Straightforward.

**Case R-DisjL:** Straightforward.

**Case R-Trans:** Straightforward.

**Case R-Weaken:** Straightforward.

\( \square \)