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

Citation

Citable link
http://nrs.harvard.edu/urn-3:HUL.InstRepos:40614411

Terms of Use
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 http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA
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
Information Flow Control for Distributed Trusted Execution Environments

Technical Report (TR-01-19)

Anitha Gollamudi
Harvard University

Stephen Chong
Harvard University

Owen Arden
University of California, Santa Cruz

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 distrusting, 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, but it also prevents the host from performing general computation on encrypted data. Lack of trust between entities may require data to be hosted separately from computations that use it, hurting performance. Worse, it is possible that no entity is sufficiently trusted to both access the data and compute the result, limiting what the application can do.

Trusted Execution Environments (TEEs) such as SGX [30, 4] and Sanctum [14] address some of these limitations with application enclaves. An enclave is a protected user-level process that is strongly isolated from the OS and other applications by trusted hardware. Remote nodes can verify the integrity of code running in an enclave using a remote attestation protocol. Once verified, the remote node knows that runtime security checks are still present in the code, and that static properties verified during compilation are still valid.

TEEs by themselves are insufficient to enforce security policies. For instance, inputs and outputs to TEEs must be correctly encrypted, signed, decrypted, and verified to protect against malicious hosts. Even with correct use of cryptography, the application must be written to ensure that it does not inappropriately reveal confidential information nor allow entities to inappropriately influence computations. Although previous work has combined techniques to enforce strong application-level confidentiality and integrity guarantees with correct-by-construction use of cryptography [29, 43, 41], no such previous work supports TEEs, and extending them to do so is nontrivial.

This work presents Distributed Flow-Limited Authorization for Trusted Execution (DFLATE), a core calculus for secure decentralized distributed applications. DFLATE extends the Flow-Limited Authorization Calculus (FLAC) [5] with distributed execution, communication channels, concurrency, and TEEs. DFLATE’s type system enforces confidentiality and integrity guarantees that are consistent with standard cryptographic mechanisms and TEE platforms.

To better understand how TEEs work, and the challenges in building secure applications that use them, consider an example of a simple distributed application, illustrated in Figure 1. Here, “Enclave” refers to code running in a TEE on Bob’s node. The only way for Alice to interact with the enclave is via Bob, whom Alice does not trust. To establish the authenticity of the enclave, Alice uses a remote attestation protocol. First, Alice requests a remote attestation from Bob (message 0), who requests a secure measurement of the enclave code from the TEE: a cryptographic hash of the loaded binary (message 1). This hash, as well as additional parameters for establishing a secure channel, is signed by a key that has been securely provisioned to the TEE (message 2). Next, Bob relays the signed message to Alice (message 3), who inspects the measurement to ensure the expected code is running, and verifies the signature to ensure it is from an authentic TEE.

Once the signature is verified, Alice uses the security parameters included in the message to establish a secure authenticated
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`.

```plaintext
if h then send ch (enc (sign msg)) 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 permutate 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

Fig. 1: Remote enclave attestation and secret provisioning.
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 $\mathcal{N}$. 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 $\pi \in \{\rightarrow, \leftarrow, -\}$ allow us to represent the partial authority of a principal. For example, the principal $p^\rightarrow$ 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 $\mathcal{P}$ of FLAM principals for any setting is given by the closure of the operations $\land$, $\lor$, $\leftarrow$, and $\rightarrow$ over the set of primitive principals $\mathcal{N}$, 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 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 $p \subseteq q$ when information labeled $p$ may safely flow to principal $q$. The flows-to relation also forms a distributive lattice with $\top \rightarrow \bot$ (public and trusted) as the least restrictive element, and $\bot \rightarrow \bot$ (secret and untrusted) as the most restrictive element. The flows-to relation and joins and meets in the information lattice are defined in terms of their authority lattice counterparts:

\[
P \subseteq q \triangleq p^{\triangleright} \triangleright q^{\triangleright} \text{ and } q^{\triangleright} \triangleright p^{\triangleright}
\]

\[
P \lor q \triangleq (p^{\triangleright} \land q^{\triangleright}) \land (p^{\triangleright} \lor q^{\triangleright})
\]

\[
P \land q \triangleq (p^{\triangleright} \lor q^{\triangleright}) \land (p^{\triangleright} \land q^{\triangleright})
\]

Every principal $p$ is equivalent (under the trust ordering) to a principal in normal form, $q^{\triangleright} \land r^{\triangleright}$, i.e., the conjunction of a confidentiality authority and an integrity authority. The voice of a principal $p$, $\nabla(p)$, is the integrity authority necessary to act on the behalf of the principal. Formally, if $q^{\triangleright} \land r^{\triangleright}$ is the normal form of $p$, then $\nabla(p) = \nabla(q^{\triangleright} \land r^{\triangleright}) = q^{\triangleright} \land r^{\triangleright}$.

**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 $pc$ range over principals. We assume the set of primitive principals $\mathcal{N}$ includes computation principals $t$ and nodes $n$, representing, respectively, code executed in a TEE and host machines. Nodes and computation...
 principals represent the places where computation occurs, and we use metavariable \( pl \) to range over them.

Metavariables \( v \) and \( e \) range over values and expressions. (Shaded values and expressions are not part of the surface syntax but arise during evaluation.) DFLATE includes standard syntax for variables, tuples, projections of types, tagged unions, case expressions, function application, and type-abstraction application. Term and type abstractions have annotations (principal \( pc \), channel environment \( \Theta \), set of places \( P \), and delegation context \( II \)) that restrict how abstractions can be applied; we discuss this further when we present the type system. We explain non-standard parts of the syntax below, as they arise.

The operational semantics for DFLATE uses two judgments: one for sequential semantics and one for distributed semantics (see Section III-C). Sequential semantic judgment \( pl, D \vdash e \rightarrow e' \) indicates that at place \( pl \), under delegation sequence \( D \), expression \( e \) takes a small step to \( e' \). Figure 4 presents some of the inference rules for this judgment.

A delegation sequence is a sequence of delegations \( \langle p_1 > q_1 \rangle \ldots \langle p_n > q_n \rangle \), indicating that principal \( q \) has delegated its authority to principal \( p \). We assume that there is a well-known initial delegation sequence \( D_{init} \). Expression \( assume \langle p > q \rangle \) in \( e \) adds delegation \( \langle p > q \rangle \) to the delegation sequence used to evaluate \( e \). This can be thought of as an annotation indicating that more information flows are permitted during the computation \( e \). However, note that the type system ensures that it is secure to add this delegation, i.e., that the delegation to add and the decision to add it have sufficiently high integrity. We use term \( e \) where \( v \) to record that delegation \( v \) holds for evaluation of \( e \). Rules DE-ASSUME and DE-WHERE show how these terms operate. (Runtime representation of the delegation sequence and where terms are needed only for proof purposes and do not need to be present in an implementation of DFLATE.)

The monadic unit term \( \eta_l \) protects \( e \) at security level \( l \). This syntax is similar to that used by DCC [2] and FLAC [5], but the

5All inference rules are given in Appendix A.

DFLATE type system treats monadic terms slightly differently in order to better model cryptographic protection mechanisms. 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 \( \eta_l \) evaluates \( e \) to a value, and then encrypts and signs the value with keys appropriate for \( l \) to protect it. Protected value \( \eta_l \) represents the encrypted and signed value \( v \) (see rule DE-UnitM). For example, \( \eta_{Alice} = \rightarrow_{ABob} \rangle v \) represents value \( v \) 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 \( bind \ v = \eta_l \) 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 \( \eta_l \).

Expression \( TEE^l \) 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 \( runTEE^l \). Note that the \( t \) in \( runTEE^l \) is related to the source-level expression \( s \); additional steps evaluate \( s \), but \( t \) remains fixed.

C. Distributed semantics

Process \( \langle n, e \rangle \) is expression \( e \) running on node \( n \). A distributed configuration \( \langle n_1, e_1 \rangle \cdots \langle n_m, e_m \rangle \) is the parallel composition of processes \( \langle n_i, e_i \rangle \). Without loss of generality, we assume that each node \( n_i \) 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: \( E[e] \) is an expression...
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 $\nu$ over the channel $\nu$ and node $n_2$ is ready to receive it. Observe that the result of stepping $send\ ch\ \nu$ then $e$ with rule PAR-SEND-RECV results in the expression $e;\Box$ and $recv\ ch\ as\ x$ in $e'$ becomes $e'[x \rightarrow \nu];\Box$. The ;$\Box$ term is used to denote the end of the process: $e;\Box$ reduces to an output value $\nu';\Box$. While $\nu';\Box$ is a valid expression, output values are not in the syntactic category of internal values $\nu$ 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 $spawn\ @ n\ (pl,\ ch_1[pc_1;\ell_1],\ ch_2[pc_2;\ell_2]).e_1$ 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 $pc_1$, $\ell_1$, $pc_2$, and $\ell_2$ 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 $A$ cannot 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 $\eta_{\ell_1} v$ and $\eta_{\ell_2} v'$ (which represent values $v$ and $v'$ encrypted and signed by principal $\ell$) if the attacker does not have the authority to decrypt $\eta_{\ell_1} v$ and $\eta_{\ell_2} v'$. 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 $(p \gg q)$ is inhabited by a single value $(p \gg q)$. Monadic
type $\ell$ says $\tau$ protects an expression of type $\tau$ at level $\ell$; it is the type of values such as $\eta_\ell v$ (where $v$ has type $\tau$).

The grammar presented in Figure 3 splits types into two kinds: output types, which have the form $\check{\tau}\square$, and internal types of the form $\check{\tau}$. 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 $\text{chan}_{\pi_1\rightarrow\pi_2} pc \check{\tau}$ and $\text{chan}_{\pi_1\rightarrow\pi_2} pc \check{\tau}$. These types specify channels that connect places $\pi_1$ and $\pi_2$ (either nodes or TEEs) and may exchange values of type $\check{\tau}$ in contexts up to $pc$. Recall that channels are uni-directional. The former type specifies a send channel, (indicated by the subscript $\pi_1\rightarrow\pi_2$) meaning $\pi_1$ may use the channel to send values to $\pi_2$, the latter specifies a receive channel (subscript $\pi_1\leftarrow\pi_2$) meaning $\pi_1$ may use the channel to receive values from $\pi_2$.

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 $\Pi; \Gamma; \Theta; \tau; \Psi; pc \vdash \tau: \check{\tau}$ 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 $x:\check{\tau}$. Channel variable scope $\Theta$. Principal $\pi$ indicates the place the term is typed at, either a node $\pi$ 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 $\Pi \vdash p \triangleright q$ 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 $\sqsubseteq$ is defined in terms of $\triangleright$ 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 $\Pi; \sqsubseteq \rightarrow T; \vdash p \triangleright q$ in the more general FLAM judgment form $\Pi; pc \vdash p \triangleright q$. 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 $p \triangleright q$, is considered public and trusted, or $\sqsubseteq \rightarrow T$. 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-LBL1:

\[
[\text{DP-LBL1}]
\Pi \vdash \ell \leq \ell' \quad \Pi \vdash \ell \leq \ell' \text{ says } \check{\tau}
\]

This rule connects acts-for judgments to protected types. If $\ell$ flows to $\ell'$, then the type $\ell'$ says $\check{\tau}$ protects level $\ell$. Singleton types like unit and $(p \triangleright q)$ protect any level since the type itself encodes the value: observing the runtime value carries no information. However, the type $\check{\tau}_1 + \check{\tau}_2$ 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.

\[
[\text{DP-LBL1}]
\Pi \vdash \ell \leq \tau \quad \Pi \vdash \ell \leq \tau' \text{ says } \check{\tau}
\]
This rule is not compatible with the cryptographic mechanisms DFLATE seeks to model: it makes nested says types commutative in the sense that $p$ says $q$ says $\tau$ protects the same levels as $q$ says $p$ says $\tau$. 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 $p$ says $q$ says $\tau$ 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.

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 $\Pi \vdash pl \triangleright pc$ 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 $\tau_1 : \Pi \vdash \ell \subseteq \tau_2$, 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 $\eta \ e$ will evaluate $e$ and then protect the result at level $\ell$ (in implementation, by signing and encrypting it). It has type $\ell$ says $\tau$ (rule DT-UnitM) provided that $e$ 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 $e$ might be influenced by information at level $pc$ and must be protected appropriately.

Clearance $(\Pi \vdash pl \triangleright pc)$ ensures that place $pl$ has appropriate integrity to sign the value. Suppose Alice wants to protect a value at Bob’s integrity by evaluating $\eta_{\text{Bob}} v$. To type check, it must be the case that $\Pi \vdash pc \subseteq \text{Bob}$. By clearance we have $\Pi \vdash \text{Alice} \triangleright pc$, and thus $\Pi \vdash \text{Alice}^r \triangleright \text{Bob}^r$, 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 $\eta_{\text{Alice}} v$ is well-typed at Bob if $v$ is well-typed. Sealed values reflect the security guarantees of cryptographic protection mechanisms: that attackers cannot distinguish ciphertexts or forge signatures.

In bind $x = e$ in $e'$, expression $e$ evaluates to a protected value $\eta_{\text{Alice}} v$, and $x$ is bound to $v$ in $e'$. 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 bind $x = \eta_{\text{Alice}} v$ in $e'$, for $e'$ to type check it must be the case that $\Pi \vdash \text{Bob} \triangleright pc \sqcup \text{Alice}$. It follows that $\Pi \vdash \text{Bob} \triangleright \text{Alice}^r$, 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 we require that $pc$ acts for $\nabla(r)$, the voice of $r$. Premise $\Pi \vdash \nabla(q^r) \triangleright \nabla(r^r)$ 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 $\Pi \vdash pc' \leq \tau'$ 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 $\Pi \vdash pl \triangleright pc_{ch}$ that
ensures $p$ has sufficient authority to use the channel. Finally, notice that whether or not $e'$ has an output type $\tau' \Box$, 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 coordinate on the security and contents of messages sent over the channel.

Expression $TEE^f e$ 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 $a \sqcap c$, 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, $\Pi \vdash a^- \gg c^-$ 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 $\Pi \vdash a \sqsubseteq a \lor b \lor c$, since, by DT-BINDM, the $pc$ at this point is at least as restrictive as the level $a$ on the protected value $\eta_a$, and by DT-SEND, this $pc$ must flow to the channel $pc$, $a \lor b \lor c$. If $\Pi \vdash a \sqsubseteq a \lor b \lor c$
holds, from the definitions of \[\sqsubset, \sqcup, \text{ and } \sqcap\text{ (Section III-A)}, it follows that \(\Pi \models b^* \gg a^*\) and \(\Pi \models c^* \gg a^*, b^*\). A similar argument for the recv at line 3 implies \(\Pi \models c^* \gg a^*\).

Now consider line 3, where function \(f\) is applied and the result protected at \(a \sqcap c\). DT-\textsc{Receive} requires that the pc of the continuation is at least \(a \sqcup b \sqcup c\), and DT-\textsc{Unit}\textsc{M} requires that this pc is protected by \(a \sqcap c\), i.e., \(\Pi \models a \sqcup b \sqcup c \sqsubseteq a \sqcap c\). For this to hold, it must be the case that \(\Pi \models a \sqcup b \sqcup c \gg a\) and \(\Pi \models a \sqcup b \sqcup c \gg c\). These judgments imply all the following:

\[
\begin{align*}
\Pi \models b^* & \gg a^* & \Pi \models c^* & \gg a^* \\
\Pi \models a^* & \gg c^* & \Pi \models b^* & \gg c^* \\
\end{align*}
\]

Figure 8(b) is an implementation of Figure 2(b). Recall that in Figure 2(b), Alice signs and encrypts her message to Carol, and Bob does not learn the contents of this message. In other words, Alice trusts Carol with her confidentiality and integrity but does not trust Bob with her confidentiality. However, she needs to trust Bob’s integrity because of his power to suppress the message. The DFLATE program shown in Figure 8(b) reflects the same trust relations. Values are protected when sent over channels. Hence, the channel type for \(ch_b\) and \(ch_c\) is \(a\text{ says }\text{int}\) rather than just \text{int} as in Figure 8(a). This program requires Alice to delegate her confidentiality and integrity to Carol, but does not require her to delegate her confidentiality to Bob. However, Alice and Carol must still trust Bob’s integrity since he can influence the computation by suppressing Alice’s message. To see why: the protected value \(\eta_a\ v\) is never used in a bind on Bob’s node, so there is no requirement that Alice trust Bob with her secrets. When Carol binds the value in order to apply function \(f\), the pc at the box in line 4 is at \((a \sqcup b \sqcup c)\ \text{via which is equal to } a^\top \land (a \sqcup b \sqcup c)^\top\) by definition of \(\sqcup\) and lattice absorption.\(^6\) Therefore, DT-\textsc{Unit}\textsc{M} requires that \(\Pi \models a^\top \land (a \sqcup b \sqcup c)^\top \subseteq a \sqcap c\), which implies that \(\Pi \models c^* \gg a^*\) 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 \((\tau x)\) at line 9 on behalf of Alice and Carol, they must each delegate integrity to \(t^\tau\) (Alice’s integrity is also required for the assume at line 7).

\[
\begin{align*}
\Pi \models t^\tau & \gg a^\top & \Pi \models t^\tau & \gg c^\top & \Pi \models a^\top & \gg c^\top \\
\end{align*}
\]

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

\[
\begin{align*}
\Pi_{\text{tee}} \models b^* & \gg t^\tau & \Pi_{\text{tee}} \models c^* & \gg a^\top \\
\end{align*}
\]

Introducing temporary delegations in a TEE using \text{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.

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. 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 \( p \). The value \( \Pi p v \) is implemented by first encrypting \( v \) (using the appropriate key for \( p^-1 \)), and then signing the result (using the appropriate key for \( p \)). Conversely, evaluation of bind \( x = \Pi p v \in e \) 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 \( p \succ q \) 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 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 encryptions and signatures only for principals \( p \) such that \( \Pi_{init} \vdash pl \succeq \nabla(p) \) (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 \( \Pi_{init} \vdash t \succeq \nabla(p) \). 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 \( \Pi_{init} \models n \succeq \nabla(p) \), 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 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,\(^{11}\)

\(^{9}\)The public key will likely be a tuple of an encryption key and a verification key, and similarly for the private key.

\(^{10}\)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.
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 weakening, or downgrading, of policies. Downgrading occurs by adding delegations (via assume terms) and by TEE execution (via endorsement of the TEE’s program counter level).

However, downgrading in DFLATE is carefully controlled and restricted: well-typed 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.

The formal definitions of the process trace of node $n$ in a well-typed distributed configuration $D$, we have a delegation approximation $\Pi_k$ that over-approximates delegations that the process may make during execution. See Appendix B for a formal definition.

Suppose all processes in $D = (n_1, e_1) \parallel \cdots \parallel (n_m, e_m)$ are well-typed, and the $i$th process takes an input value protected by $H$ (i.e., it has a free variable of type $H \text{ says } t$) and the $j$th process produces a value of type $\ell \text{ says } \pi \in \Gamma_i$. Moreover, suppose the delegation approximations for the processes ensure that they never downgrade from $H$ (i.e., $\Pi_k^P$ permits the same flows from $H$ as $\Pi_{init}$). If we have two executions of $D$ 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 $\Pi_{init} \not\vdash H \sqsubseteq \ell$. Let $D = (n_1, e_1) \parallel \cdots \parallel (n_m, e_m)$ such that for all $k \in 1..m$ we have

$$\Pi_{init}; \Gamma_k; \Theta_k; n_k; pc_k \vdash e_k: \tau_k,$$

where $\tau_i = \ell \text{ says bool } x$ and $x : H \text{ says } \pi \in \Gamma_i$.

Assume that no process downgrades from $H$, i.e., $\forall k \in 1..m. \forall \ell'$. $\Pi_{init} \vdash H \sqsubseteq \ell' \Rightarrow \Pi_k^P \vdash H \sqsubseteq \ell'$. 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 $D_2 = (n_1, e_1') \parallel \cdots \parallel \{n_j, v_j(x)/x\} \parallel \cdots \parallel (n_m, e_m')$.

If $D_1 \Rightarrow^{*} (n_1, e'_1) \parallel \cdots \parallel (n_j, v'_j) \parallel \cdots \parallel (n_m, e_m')$ and $D_2 \Rightarrow^{*} (n_1, e'_1) \parallel \cdots \parallel (n_j, v''_j) \parallel \cdots \parallel (n_m, e_m')$ 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 $\Pi_{init} \vdash n \not\succ \nabla(p)$. Thus, the attacker cannot observe the contents of protected value $\pi'_{\ell'} v$ if $\Pi_{init} \not\vdash n \succ \nabla(\ell')$, nor can see the contents of a TEE for computation principal $\ell$ if $\Pi_{init} \not\vdash n \succ \nabla(\ell)$.

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.

Our stronger noninterference result is similar to the result of Theorem 1, but holds only for confidentiality.

**Theorem 2** (Compromised-node Noninterference). Let $H \not\succ n_j$ be security levels such that $\Pi_{init} \not\vdash n_j \succ H$. Let

\[\text{Weakening confidentiality is called } \text{declassification} \text{ [37]; weakening integrity is called } \text{endorsement} \text{ [11].}\]
\( D = \langle n_1, e_1 \rangle \parallel \cdots \parallel \langle n_m, e_m \rangle \) such that for all \( k \in 1..m \) we have
\[
\Pi_{init}; \Gamma; \Theta; n_k; pc_k \vdash e_k; \tau_k,
\]
where \( x : H^- \) says \( \hat{\tau} \in \Gamma_i \).

Assume that no process downgrades from \( H^- \), i.e., \( \forall k \in 1..m, \forall \ell. \Pi_{init} \vdash H^- \subseteq \ell \iff \Pi_{init}^\ell \vdash H^- \subseteq \ell. \) For all \( v_1 \) and \( v_2 \), and all \( z \in \{1, 2\} \) such that
\[
\Pi; \Gamma; \Theta; n; pc_i \vdash v_z : H^- \text{ says } \hat{\tau},
\]
let \( D_z = \langle n_1, e_1 \rangle \parallel \cdots \parallel \langle n_i, e_i \langle v_z / x \rangle \rangle \parallel \cdots \parallel \langle n_m, e_m \rangle \).

Then for all executions \( D_1 \Longrightarrow D_1' \) and \( D_2 \Longrightarrow D_2' \) the process traces of node \( u \) 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 \( \eta_i \) true for all inputs \( x \).
\[
\lambda_{true} \left( \text{bind } u = x \text{ in } (\lambda_{unit} u) \right)
\]
where
\[
\lambda_{true} = \lambda_{true} \left( \text{bind } u = x \text{ in } (\lambda_{true} u) \right)
\]
and
\[
\lambda_{unit} = \lambda_{unit} \left( \text{bind } u = x \text{ in } (\lambda_{unit} u) \right)
\]

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

Trace on \( S_1 \)
\[
1. \langle n_j, \lambda_{true} (\lambda_{unit} true) \rangle \quad 2. \langle n_j, \lambda_{false} (\lambda_{unit} false) \rangle \\
3. \langle n_j, \eta_i \rangle
\]

Trace on \( S_2 \)
\[
1. \langle n_j, \lambda_{true} (\lambda_{unit} true) \rangle \quad 2. \langle n_j, \lambda_{true} (\lambda_{unit} false) \rangle \\
3. \langle n_j, \eta_i \rangle
\]

Though the final output is same in both the executions, the traces differ in line 1. This asymmetry is due to the message suppression ability of the attacker. Consider the following program on nodes \( n_1 \) and \( n_2 \).
\[
\begin{array}{c}
\text{bind } u = x \text{ in case } u \text{ of } \\
\text{inj}_1(z), \text{send } ch(z) \text{ then } (y) \\
\text{inj}_2(z), \text{recv } ch'(y) \text{ as } y \text{ in } y'
\end{array}
\]

On the left, the attacker node binds low-integrity input \( x \) (of type \( H^- \) says 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 \( x = \eta_i H^- \) inj \( j_1 \), process \( n_2 \) terminates, but for \( x = \eta_i H^- \) inj \( j_2 \) 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


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), typing rules (Figures 17, 18, 19).

**APPENDIX A**

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

$$\Pi_{init}; \Gamma_1; \Theta_1; p_1; p_{c1} \vdash e_1 : \tau_1 \parallel \cdots \parallel \Pi_{init}; \Gamma_m; \Theta_m; p_m; p_{cm} \vdash e_m : \tau_m$$

The delegation approximation $\hat{\Pi}_p^D$ of the process $\langle p_1, e_1 \rangle$ is the union of the set of all delegations in the initial delegation context $\Pi$ and those that are assumed during the evaluation of the process $\langle p_1, e_1 \rangle$. $$\langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_1, e_1' \rangle$$

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

$$\langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \parallel \ast$$

The delegation approximation $\hat{\Pi}_p^D$ of the process $\langle p_i, e_i \rangle$ is the union of the set of all delegations in the initial delegation context $\Pi$ and those that are assumed during the evaluation of the process $\langle p_i, e_i \rangle$. $\vdash e_i : \tau_i$.
Fig. 12: DFLATE evaluation step for case terms

Fig. 13: Propagation of where terms

Fig. 14: DFLATE distributed semantics

Fig. 16: Type protection levels

Proposition 1. Let S be the well-typed distributed system from Definition B.1. If $\Pi_{\mathcal{D}}^p$ is the delegation approximation of the process $\langle p_i, e_i \rangle$, then the following hold.

1) If $\Pi \vdash \ell \leq \ell'$, then $\Pi_{\mathcal{D}}^p \vdash \ell \not\leq \ell'$

2) $\forall \ell, \ell'. \Pi \vdash \ell \subseteq \ell' \Rightarrow \Pi_{\mathcal{D}}^p \vdash \ell \not\subseteq \ell'$

3) $\forall \ell, \ell'. \Pi_{\mathcal{D}}^p \not\vdash \ell \subseteq \ell' \Rightarrow \Pi \not\vdash \ell \subseteq \ell'$
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.

$$\langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_k, e_k \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle$$

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, $O((p_j, e_j), \Pi, \ell), \ldots, O((p_j, e_j), \Pi, \ell)$ where, 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 is associated with the node $p_j$. The trace is computed as follows:

$$Tr(S, p_j, \Pi, \ell) = O((p_j, e_j), \Pi, \ell), \ldots, O((p_j, e_j), \Pi, \ell)$$

where $\Pi_{\ell}^D$ 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, $Tr_1$ and $Tr_2$, are equivalent, denoted as $Tr_1 \approx Tr_2$, if they are equal after removing the duplicates. That is

$$Tr_1 \approx Tr_2 \iff U(Tr_1) = U(Tr_2)$$

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 against this attacker.
Fig. 18: DFLATE typing rules for secure operations

\[
\begin{align*}
\text{[DT-UNIT]} & : \Gamma; \Theta; pl; pc \vdash e : \top & \Pi \vdash pc \sqsubseteq \ell & \Pi \vdash pl \triangleright pc \\
\text{[DT-SEALED]} & : \Gamma; \Theta; pl; pc \vdash e : \top & \Pi \vdash pl \triangleright pc \\
\text{[DT-BIND]} & : \Gamma; \Theta; pl; pc \vdash e : \ell \quad \ell \text{ says } \top \\
\text{[DT-ASSUME]} & : \Gamma; \Theta; pl; pc \vdash e : (p \triangleright q) & \Pi \vdash (p \triangleright q) \triangleright pl \triangleright e : \top \\
\text{[DT-WHERE]} & : \Gamma; \Theta; pl; pc \vdash v : \top & \Pi \vdash pl \triangleright pc \\
\text{[DT-HALT]} & : \Gamma; \Theta; pl; pc \vdash e : \top & \Pi \vdash pl \triangleright pc \\
\text{[DT-HALT2]} & : \Gamma; \Theta; pl; pc \vdash e : \bot & \Pi \vdash pl \triangleright pc \\
\text{[DT-SPAWN]} & : \Gamma; \Theta; pc \vdash ch : \text{spawn}(q) & \Pi \vdash pl \triangleright pc ; ch \vdash q : pc \triangleright e : \top \\
\text{[DT-SEND]} & : \Gamma; \Theta; pc \vdash e : \top \quad \Pi \vdash pc \sqsubseteq pc' \quad \Pi \vdash pc' \sqsubseteq pc'' \quad \Pi \vdash pc' \leq \tau' \quad \Pi \vdash pl \triangleright pc' \quad \Pi \vdash p \triangleright pc \\
\text{[DT-SENDDEL]} & : \Gamma; \Theta; pc \vdash send(ch, v) \quad \Pi \vdash pl \triangleright pc ; pc' \vdash ch : \text{spawn}(q) \quad \Pi \vdash pl \triangleright pc ; pc'' \vdash e : \top \quad \Pi \vdash pl \triangleright pc' ; \Pi \vdash pl \triangleright pc'' \quad \Pi \vdash pl \triangleright pc'' \\
\text{[DT-RECEIVE]} & : \Gamma; \Theta; pc \vdash e : \top \quad \Pi \vdash pc \sqsubseteq pc' \quad \Pi \vdash pc' \sqsubseteq pc'' \quad \Pi \vdash pc' \leq \tau' \quad \Pi \vdash p \triangleright pc \\
\text{[DT-TEE]} & : \Theta'; t; \tau' \quad \Pi \vdash pl \triangleright pc' \quad \Pi \vdash pl \triangleright pc'' \quad \Pi \vdash pl \triangleright pc \\
\text{[DT-TEEG]} & : \Theta'; t; \tau' \quad \Pi \vdash pl \triangleright pc' \quad \Pi \vdash pl \triangleright pc'' \quad \Pi \vdash pl \triangleright pc \\
\text{[DT-SYS]} & : \forall i \in 1 \ldots n. \Gamma_i; \Theta_i ; pl_i ; pc_i \vdash e_i : \tau_i & \Pi \vdash pl \triangleright pc \\
\end{align*}
\]

Fig. 19: DFLATE typing rules for spawn and communication primitives
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.

\[
\begin{align*}
\hat{e} &:= \ldots | (\hat{e} | \hat{e}) \\
\hat{v} &:= \ldots | (\hat{v} | \hat{v})
\end{align*}
\]

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 a step 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 \( k = \{1, 2\} \).

**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:** Given \( p, D \vdash (\lambda(x: \tau_1)[pc_1, \Theta_1, \Pi_1], \lambda(x: \tau_2)[pc_2, \Theta_2, \Pi_2], e_2) \rightarrow (e_1[x \mapsto [v]_1] | e_2[x \mapsto [v]_2]) \). For \( k \in \{1, 2\} \), we have to prove that

\[
p, D \vdash \lambda(x: \tau_k)[pc_k, \Theta_k, \Pi_k], e_k [v]_k \rightarrow e_k[x \mapsto [v]_k]
\]

Straightforward from DE-APP.

**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.

**Lemma 2** (Soundness for System). If \( \langle p_1, e_1 \rangle \ || \cdots || \langle p_1, e_1 \rangle \ || \cdots || \langle p_n, e_m \rangle \) \( \Rightarrow \) \( \langle p_1, e'_1 \rangle \ || \cdots || \langle p_1, e'_1 \rangle \ || \cdots || \langle p_n, e'_m \rangle \) then

\[
\langle p_1, [e_1]_k \rangle \ || \cdots || \langle p_1, [e_1]_k \rangle \ || \cdots || \langle p_n, [e_m]_k \rangle \) \( \Rightarrow \) \( \langle p_1, [e_1]_k \rangle \ || \cdots || \langle p_1, [e_1]_k \rangle \ || \cdots || \langle p_n, [e_m]_k \rangle \) for \( k \in \{1, 2\} \).

**Proof.** We induct on the system step relation.
\( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_m \rangle \rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_n, e'_{n_1} \rangle \)

\( i \in \{1 \ldots m \} \quad e'_i = (e'_i \mid \varepsilon_{i,j}) \quad j = \begin{cases} n & \text{if } n \neq m \\ \varepsilon_{i,j} & \text{otherwise} \end{cases} \)

\( e'_{ij} = \begin{cases} e'_i & \text{if } n = m \text{ and } j = i \\ e_j & \text{if } n \neq m \\ (e_{n_1} \mid e_{j_2}) & \text{if } n = m, j \neq i \text{ and } e_j = (e_{j_1} \mid e_{j_2}) \\ W[(e_{n_1} \mid e)] & \text{if } n = m, j \neq i \text{ and } e_j = W[e] \end{cases} \)

**BD-PAR-STEP-L**

\( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_m \rangle \rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_n, e'_{n_1} \rangle \)

\( e_i = W[(\text{spawn } \theta q \langle pl, ch_i, [pc_i; \tau_i], ch_s, [pc_s; \tau_s] \rangle, e_q \text{ then } e_n \mid e)] \\
\quad e'_i = W[(e \mid e_s, [\nu/v]; [\nu/v]; [\nu/v]; \bullet)] \)

**BD-PAR-SPAN-L**

\( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_n \rangle \rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_n, e'_n \rangle \)

\( e_i = W[(e \mid \text{send } \nu \text{ as } x \text{ in } e_m \mid e) \parallel \cdots \parallel (e \mid \text{recv } \nu \text{ as } x \text{ in } e_m \mid e)] \\
\quad e'_i = W[(e \mid e_s; \bullet)] \)

**BD-PAR-SEND-RECV-L**

\( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_n \rangle \rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_n, e'_n \rangle \)

\( e_i = W[(e \mid \text{recv } \nu \text{ as } x \text{ in } e_m \mid e)] \\
\quad e'_i = W[(e \mid e_s; \bullet)] \)

**BD-PAR-SEND-RECV-R**

\( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_n \rangle \rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_n, e'_n \rangle \)

\( e_i = W[(e \mid \text{recv } \nu \text{ as } x \text{ in } e_m \mid e)] \\
\quad e'_i = W[(e \mid e_s; \bullet)] \)

**BD-REC-SEND**

\( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_n \rangle \rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_n, e'_n \rangle \)

\( e_i = W[(e \mid \text{send } \nu \text{ as } x \text{ in } e_m \mid e)] \\
\quad e'_i = W[(e \mid e_s; \bullet)] \)

**BD-REC-SEND-R**

\( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_n \rangle \rightarrow \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_n, e'_n \rangle \)

\( e_i = W[(e \mid \text{send } \nu \text{ as } x \text{ in } e_m \mid e)] \\
\quad e'_i = W[(e \mid e_s; \bullet)] \)

**Fig. 21:** DFLATE Evaluation extensions for system
Before proving completeness, we prove if the bracketed term is stuck then either left or right execution are stuck.

Fig. 22: Projection for bracketed expressions. \( \bullet \) denotes empty expression.

---

**Case PAR-STEP:** From the premises of PAR-STEP, we have that \( p_i, D_{\text{init}} \vdash e_i \rightarrow e'_i \). Invoking soundness for single process (Lemma 1), we have that \( p_i, D_{\text{init}} \vdash e_i \rightarrow e'_i \) for some \( i \in \{1 \ldots m\} \) and for all \( k \in \{1, 2\} \). Thus, we have \( \langle p_1, [e_i]_k \rangle \parallel \cdots \parallel \langle p_i, [e_i]_k \rangle \parallel \cdots \parallel \langle p_m, [e_i]_k \rangle \rightarrow \langle p_1, [e_i]_k \rangle \parallel \cdots \parallel \langle p_i, [e_i]_k \rangle \parallel \cdots \parallel \langle p_m, [e_i]_k \rangle \).  

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

**Case BD-PAR-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 \( \langle p_i, [e_i]_1 \rangle \parallel \cdots \parallel \langle p_j, [e_j]_1 \rangle \rightarrow \langle p_i, [e'_i]_1 \rangle \parallel \cdots \parallel \langle p_j, [e'_j]_1 \rangle \) \( \parallel \cdots \parallel \langle p_m, [e_i]_k \rangle \rightarrow \langle p_i, [e_i]_1 \rangle \parallel \cdots \parallel \langle p_i, [e_i]_1 \rangle \parallel \cdots \parallel \langle p_m, [e_i]_k \rangle \). Hence proved.  

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

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

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

**Case BD-PAR-SEND-RECV-L:** Remaining terms unchanged, we have that \( \langle p_i, W_i[\text{send} \ ν \ \nu \ \text{then} \ e_{\alpha}] \rangle \parallel \langle p_j, W_i[\text{recv} \ ν \ \text{as} \ x \ \text{in} \ e_{\alpha}] \rangle \rightarrow \langle p_i, W_i[e_{\alpha}] \rangle \parallel \langle p_j, W_i[e_{\alpha} \rightarrow \nu] \rangle \). 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-RECV-SEND-L:** Similar to the case BD-PAR-SEND-RECV-L.  

**Case BD-PAR-RECV-SEND-R:** Similar to the case BD-PAR-SEND-RECV-L.  

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

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

Case \(\hat{e}\): By assumption, \(e\) is not a value.

Case \(x\): No reduction for a variable. Hence \([x]_i\) is stuck as well.

Case \(e e'\): Since BD-APP and DE-APP are not applicable, it follows that \(e\) is not of the form \(\lambda(x: \tau)[pc', \Theta', \mathcal{P}, \Pi'_\lambda], e_1 | \lambda(x: \tau)[pc', \Theta', \mathcal{P}, \Pi'_\lambda], e_2\) or \(\lambda(x: \tau)[pc', \Theta', \mathcal{P}, \Pi'_\lambda], e\). 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 \(\text{proj} e, \text{inj} e\): Similar to the above case.

Case \(e \tau\): Since BD-TAPP and DE-TAPP are not applicable, it follows that \(e\) is not of the form \((v_1 | v_2)\) or \(\Delta X[pc; \Theta, \mathcal{P}, \Pi], e\). Thus \([e]_i\) is stuck as well.

Case \(e \text{ of inj}(x). e_1 \mid \text{inj}(x). e_2\): Since BD-CASE and DE-CASE are not applicable, it follows that \(e\) is not of the form \((\text{inj}_1(v_1) \mid \text{inj}_2(v_2))\) or \(\text{inj}_1 v\). It follows that \([e \text{ of inj}_1(x). e_1 \mid \text{inj}_2(x). e_2]_i\) is also stuck.

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

Case \(\text{TEE}\ e\): Cannot get stuck.

Case \(\text{runTEE}\ e\): Applying induction to \(e\), we have that \(\text{runTEE}\ e\) is stuck for some \(i \in \{1, 2\}\). \(\text{runTEE}\ [\hat{e}]\) 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 \(\text{Other}\): Remaining expressions do not take a step (single thread step relation \(\rightarrow\)).

Lemma 4 (Stuck Expressions for System). If \(<p_1, e_1> \parallel \cdots \parallel <p_n, e_n>\) gets stuck then the configuration \(<p_1, [e_1]_k> \parallel \cdots \parallel <p_n, [e_n]_k>\) for some \(k \in \{1, 2\}\).

Proof. Induction on the structure of the system configuration.

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W[\text{send} \nu \text{ v then } e_{mn}]\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): There is no matching \(W[\text{recv} \nu \text{ as } x \text{ in } e]\) 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 \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W((\text{send} \nu \text{ v then } e_{mn}) | e')\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): There is no matching \(W[(\text{recv} \nu \text{ as } x \text{ in } e | e')]\) 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 \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W[(\text{recv} \nu \text{ as } x \text{ in } e | e')]\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): Similar to above case.

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W(e' | \text{recv} \nu \text{ as } x \text{ in } e)\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): Similar to above case.

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W(e' | \text{send} \nu \text{ v then } e_{mn})\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): Similar to above cases but \(k = 2\).

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W(e' | \text{recv} \nu \text{ as } x \text{ in } e)\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): Similar to above cases but \(k = 2\).

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W((\text{send} \nu \text{ v then } e_{mn}) | e')\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): There is no matching \(W[(\text{recv} \nu \text{ as } x \text{ in } e | e')]\) or \((W[\text{recv} \nu \text{ as } x \text{ in } e | e'])\), otherwise it would have taken a step using BD-PAR-SEND-RECV-L. Thus \(k = 1\).

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, (e' | \text{send} \nu \text{ v then } e_{mn})\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): There is no matching \(W[(\text{recv} \nu \text{ as } x \text{ in } e | e')]\) or \((e' | \text{recv} \nu \text{ as } x \text{ in } e)\), otherwise it would have taken a step using BD-PAR-SEND-RECV-R. Thus \(k = 2\).

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, W(\text{recv} \nu \text{ as } x \text{ in } e | e')\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): There is no matching \(W[\text{recv} \nu \text{ v then } e_{mn}]\) or \((W[\text{recv} \nu \text{ v then } e_{mn}) | e')\), otherwise it would have taken a step using BD-PAR-SEND-RECV-L. Thus \(k = 1\).

Case \(<p_1, e_1> \parallel \cdots \parallel \langle p_i, (e' | W(\text{recv} \nu \text{ as } x \text{ in } e))\rangle \parallel \cdots \parallel \langle p_n, e_n]\rangle\): There is no matching \(W[\text{recv} \nu \text{ v then } e_{mn}]\) or \((e' | W[\text{recv} \nu \text{ v then } e_{mn})\), otherwise it would have taken a step using BD-PAR-SEND-RECV-R. Thus \(k = 2\).

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

Case \(\text{other}\): 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 \(<p_1, [e_1]_k> \parallel \cdots \parallel <p_i, [e_i]_k> \parallel \cdots <p_n, [e_m]_k> \Rightarrow^* <p_1, e'_1> \parallel \cdots <p_i, e'_i> \parallel \cdots <p_n, e'_n>\) for all \(k \in \{1, 2\}\) then there exists a \(\hat{v}_1\) such that \(<p_1, e_1> \parallel \cdots <p_i, e_i> \parallel \cdots <p_n, e_m> \Rightarrow^* <p_1, e'_1> \parallel \cdots <p_i, e'_i> \parallel \cdots <p_n, e'_m>\).

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 $\Pi_1; \emptyset; \Theta_1; p_1; pc_1 \vdash e_1: \tau_1 \parallel \cdots \parallel \Pi_n; \emptyset; \Theta_n; p_n; pc_n \vdash e_n: \tau_n \parallel \cdots \parallel \Pi_m; \emptyset; \Theta_m; p_m; pc_m \vdash e_m: \tau_m$. If $\langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_n, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \Rightarrow^* \langle p_1, e'_1 \rangle \parallel \cdots \parallel \langle p_m, W'[\text{send } v \text{ then } e_n] \rangle \parallel \cdots \parallel \langle p_n, e'_n \rangle$ then $\emptyset; \emptyset; p'_i; pc'_i \vdash v: \tau$.

**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 $\Pi; \Gamma; \Theta; p; pc \vdash e: \tau$. Then $\Pi \vdash p \ni pc$

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

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

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

**Lemma 10** (Robust Protection). If $\Pi \vdash pc \ni \tau$, then $\Pi \cdot (p \ni q); \Theta; p; pc \vdash e: \tau$ 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-ASSUME:** Given $\Pi; \Gamma; \Theta; p; pc \vdash assume e \in e': \tau$. From the premises,

\begin{align*}
\Pi; \Gamma; \Theta; p; pc \vdash e: (a \ni b) \\
\Pi \vdash pc \ni \nabla(b) \\
\Pi \vdash \nabla(a^-) \ni \nabla(b^-)
\end{align*}

Applying inductive step to (1) and (4), we have $\Pi \cdot (a \ni b), \langle p \ni q \rangle; \Gamma; \Theta; p; pc \vdash e': \tau$ and $\Pi \cdot (p \ni q); \Gamma; \Theta; p; pc \vdash e: (a \ni b)$. Applying Lemma 8 to premises (C-B) and (C-B) we have $\Pi \cdot (p \ni q) \vdash pc \ni \nabla(b^-)$ and $\Pi \cdot (p \ni q) \vdash \nabla(a^-) \ni \nabla(b^-)$ . 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 $\Pi \cdot (a \ni b); \Gamma; \Theta; p; pc \vdash (e_1 | e_2): \tau$.

**Case DT-BRACKET-VALUES:** Applying induction to premises, we have the conclusion.

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

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

**Case DT-SENDDDEL:** 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 $\Pi \vdash p \ni pc'$, 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-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, $\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau}$. From DT-ASSUME, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (5)
\]

Since $\Pi \vdash p \vdash pc'$, Applying induction to the premises we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash \vdash_{\tau_1} \quad (6)$

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau_1} \quad (7)$

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau_1} \quad (8)$

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau_1} \quad (9)$

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau_1} \quad (10)$

Hence we can apply induction to the premise and the rest of the proof os straight forward.

Case DT-Assume: Given, $\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau}$ From DT-ASSUME, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (11)
\]

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau}$ From DT-ASSUME, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (12)
\]

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau}$ From DT-ASSUME, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (13)
\]

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau}$ From DT-ASSUME, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (14)
\]

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau}$ From DT-ASSUME, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (15)
\]

Applying inductive hypothesis to (11) and (14) we have $\Pi; \Gamma; \Theta; \rho; pc' \vdash e \vdash_{\tau}$ From DT-ASSUME, we have

Case DT-WHERE: Given, $\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau}$ From DT-WHERE, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (16)
\]

Applying inductive hypothesis to (16) and (19) (and weakening delegation context (Lemma 10)), we have $\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau}$ From DT-WHERE, we have

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (17)
\]

Applying inductive hypothesis to (16) and (19) (and weakening delegation context (Lemma 10)), we have $\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (18)$

Combining, we have all the premises for DT-ASSUME and thus

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (19)
\]

Combining, we have all the premises for DT-ASSUME and thus

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (20)
\]

Combining, we have all the premises for DT-ASSUME and thus

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (21)
\]

Combining, we have all the premises for DT-ASSUME and thus

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (22)
\]

Combining, we have all the premises for DT-ASSUME and thus

\[
\Pi; \Gamma; \Theta; \rho; p; q; \rho \vdash e \vdash_{\tau} \quad (23)
\]
Before applying induction to the premises, we have to prove that \( \Pi \vdash t \gg t' \land pc' \gg \). From clearance (Lemma 7, we have that \( \Pi \vdash t \gg t' \land pc' \gg \). Combined with \( \Pi \vdash pc' \sqsubseteq pc \), we have that

\[ \Pi \vdash t \gg t' \land pc' \gg \]

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 \( \Pi; \Gamma; \Theta; pl; pc \vdash \text{recv } ch \ as \ x \ in \ e' : \tau \). We therefore have the premises

\[
\Pi; \Gamma; \Theta; pc' \vdash ch : \text{chan}_{p\rightarrow q} \ pc_{ch} \ \tau
\]

Using \text{R-TRANS}, from (22) and (24), we have

\[ \Pi \vdash pc' \sqsubseteq pc'' \]

and

\[ \Pi \vdash pc' \sqsubseteq pc_{ch} \]

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

**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 \( \Pi; \Gamma; \Theta; pl; pc \vdash \text{spawn } ch \mapsto \text{chan}_{p\rightarrow q} \ pc_{ch} \ \tau \) then \( e_1 \) then \( e_2 : \tau \). From the premises, we have

\[ \Pi; \Gamma; \Theta; [ch_1 \mapsto \text{chan}_{p\rightarrow q} \ pc_{ch} \ \tau_1; ch_2 \mapsto \text{chan}_{p\rightarrow q} \ pc_{ch} \ \tau_2]; p; pc \vdash e_2 : \tau \]

\[ \Pi; \Theta; [ch_1 \mapsto \text{chan}_{q\rightarrow p} \ pc_{ch} \ \tau_1; ch_2 \mapsto \text{chan}_{q\rightarrow p} \ pc_{ch} \ \tau_2]; q; pc \vdash e_1 : \text{unit} \Pi \vdash pc \sqsubseteq pc \]

\[ \Pi \vdash p \gg pc \]

\[ \Pi \vdash q \gg pc \]

Straightforward application of induction hypothesis to the premises.

**Case DT-BRACKET:** The premise \( \Pi \vdash H^\pi \sqcup pc \sqsubseteq pc'' \) implies \( \Pi \vdash H^\pi \sqcup pc' \sqsubseteq pc'' \).

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

\[ \square \]

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

**Proof.** Proof is by induction on the structure of the values.

**Case Var:** Trivial

**Case Unit:** Trivial

**Case Delegation:** Trivial

**Case \( \eta \ell \ v \):** Apply induction to the premise of DT-UNITMSEALED.

**Case inj \ i \ 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; □:** Apply induction to the premise of DT-HALT and DT-HALT2.
Case \((\hat{v}_1 \mid \hat{v}_2)\): From DT-BRACKET-VALUES, we have that

\[
\begin{align*}
\Pi \vdash H^\pi &\leq \tau \quad \text{(31)} \\
\Pi; \Gamma; \Theta; \rho; \hat{v}_1 \vdash e_1 : \tau \quad \text{(32)} \\
\Pi; \Gamma; \Theta; \rho; \hat{v}_1 \vdash \hat{v}_1 : \tau \quad \text{(33)}
\end{align*}
\]

Applying induction to the premises, we have that

\[
\begin{align*}
\Pi \vdash H^\pi &\leq \tau \quad \text{(34)} \\
\Pi; \Gamma; \Theta; \rho; \hat{v}_1 \vdash e_1 : \tau \quad \text{(35)} \\
\Pi; \Gamma; \Theta; \rho; \hat{v}_1 \vdash \hat{v}_1 : \tau \quad \text{(36)}
\end{align*}
\]

Thus \(\Pi; \Gamma; \Theta; \rho; \hat{v}_1 \vdash (\hat{v}_1 \mid \hat{v}_2) : \tau\).

\[\Box\]

**Lemma 13** (Non-Bracket Values PC). Let \(\Pi_1; \Gamma_1; \Theta_1; p_1; p_1c_1 \vdash e_1 : \tau_1 \parallel \cdots \parallel \Pi_m; \Gamma_m; \Theta_m; p_m; p_mc_m \vdash e_m : \tau_m\). If \(\Pi_1; \Gamma_1; \Theta_1; p_1; p_1c_1 \vdash \hat{v} : \tau\) for some \(i = \{1 \ldots m\}\) such that \(\hat{v}\) is not a bracket then \(\Pi_i; \Gamma_i; \Theta_i; p_i; p_i'c_i \vdash \hat{v} : \tau\) for any \(p_i'c_i\) such that \(\Pi_i \parallel p_i \gg p_i'c_i\).

**Proof.** Recall that \(p_1c = \bigcap_i T_i \cap \bigcap_i p_i\). Proof is by induction on the values. Also the condition \(\Pi_i \parallel p_i \gg p_i'c\) ensures that the proof is straightforward for all values except functions and where terms. We prove important cases.

**Case Function:** Given \(\Pi_i; \Gamma_i; \Theta_i; p_i; p_i c_i \vdash \lambda(x:)p_i'c_i\), \(\Theta''\), \(\Pi\), \(\lambda_i\), \(e : \tau \vdash p_i'c_i\). We have to prove that:

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_i'c_i \vdash \lambda(x:)p_i'c_i\), \(\Theta''\), \(\Pi\), \(\lambda_i\), \(e : \tau \vdash p_i'c_i\).
\]

**Case Where:** Given \(\Pi_i; \Gamma_i; \Theta_i; p_i; p_i c_i \vdash \hat{v}\) where \(\langle p \gg q \rangle : \tau_i\). We have to prove that:

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; p_i'c_i \vdash \hat{v}\) where \(\langle p \gg q \rangle : \tau_i\).
\]

From DT-WHERE, we have that \(\Pi_i \parallel p_1 \gg p_i'c_i\). Note that \(p_1c\) is constant for a given distributed configuration and does not change with the \(p_i'c_i\). We are already given that \(\Pi_i \parallel p_i \gg p_i'c_i\). Thus we have all premises for DT-WHERE.

\[\Box\]

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

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

\[
\Pi; \Gamma; \Theta; \rho; p; p \vdash (e_1[x \mapsto [\hat{v}_1]] \mid e_2[x \mapsto [\hat{v}_2]]) : \tau.
\]

We first describe the case DT-BRACKET. The proof for the case DT-BRACKET-VALUES is analogous. From DT-BRACKET, we have that

\[
\begin{align*}
\Pi; \Gamma; x : \tau'; \Theta; \rho; p; p \vdash e_1 : \tau \quad \text{(37)} \\
\Pi; \Gamma; x : \tau'; \Theta; \rho; p; p \vdash e_2 : \tau \quad \text{(38)} \\
\Pi \parallel (H^\pi \uplus p_1c) \subseteq p_1c' \quad \text{(39)} \\
\Pi \vdash H^\pi \leq \tau \quad \text{(40)}
\end{align*}
\]

Applying clearance (Lemma 7), we have that \(\Pi \vdash p \gg p_1c'\). Depending on whether \(\hat{v}\) is a bracket value, we have two cases

**Case \(\hat{v} = (\hat{v}_1 \mid \hat{v}_2)\):** From DT-BRACKET-VALUES, we have that

\[
\begin{align*}
\Pi; \Gamma; \Theta; \rho; p; p \vdash \hat{v}_1 : \tau' \quad \text{(41)} \\
\Pi; \Gamma; \Theta; \rho; p; p \vdash \hat{v}_2 : \tau' \quad \text{(42)} \\
\Pi \vdash H^\pi \leq \tau' \quad \text{(43)}
\end{align*}
\]

Since values can be typed under any \(p_1c\) which acts for the place under which value is typed (Lemma 13), we have that \(\Pi; \Gamma; \Theta; \rho; p; p \vdash \hat{v}_i : \tau\) for all \(i \in \{1, 2\}\). Applying induction to the premises (37) and (38), we get

\[
\begin{align*}
\Pi; \Gamma; \Theta; \rho; p; p \vdash e_1[x \mapsto \hat{v}_1] : \tau \quad \text{(44)} \\
\Pi; \Gamma; \Theta; \rho; p; p \vdash e_2[x \mapsto \hat{v}_2] : \tau \quad \text{(45)}
\end{align*}
\]

and thus

\[
\Pi; \Gamma; \Theta; \rho; p; p \vdash (e_1[x \mapsto \hat{v}_1] \mid e_2[x \mapsto \hat{v}_2]) : \tau
\]
Case \( \hat{v} \neq (\hat{v}_1 | \hat{v}_2) \): Since values can be typed under any \( pc \) which acts for the place under which value is typed (Lemma 13), we have that \( \Pi; \Gamma; \Theta; p; pc' \vdash \hat{v} : \tau \). Applying induction to the premises (37) and (38), we get

\[
\Pi; \Gamma; \Theta; p; pc' \vdash e_1[x \mapsto \hat{v}] : \tau
\]

and thus

\[
\Pi; \Gamma; \Theta; p; pc \vdash (e_1[x \mapsto \hat{v}] | e_2[x \mapsto \hat{v}]) : \tau
\]

\[ \square \]

Lemma 15 (Projection Preserves Types). If \( \Pi; \Gamma; \Theta; p; pc \vdash e : \tau \), then \( \Pi; \Gamma; \Theta; p; pc \vdash \tau_i : \tau \) for \( i = \{1, 2\} \).

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. \( \square \)

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

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

Case DT-Var: Depending on whether \( \tau \) uses \( X \) two cases arise. Either \( \Pi; \Gamma, x : \tau, X, \Gamma'; p; pc; x : \tau \vdash o : r \). In the former case, since \( \Pi; \Gamma, x : \tau \) does not use \( X \), we have that \( \tau[X \mapsto \tau'] \) is same as \( \tau \).

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

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

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

Case DT-App: Given \( \Pi; \Gamma, X, \Gamma'; \Theta; p; pc \vdash e : \tau \). Applying induction hypothesis to the premises, we have

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

From DT-APP, we thus have \( \Pi; \Gamma, X, \Gamma'[X \mapsto \tau']; \Theta; p; pc \vdash e[X \mapsto \tau'] : \tau[X \mapsto \tau'] \).

Case DT-Lam: Given \( \Pi; \Gamma; \Gamma' ; \Theta; p; pc \vdash \lambda x : \tau_1 (pc', \Theta, P, \Pi_1) ; e_1 : \tau_1 \). Applying induction hypothesis to the premise, we have \( \Pi; \Gamma; \Gamma'[X \mapsto \tau']; \Theta; p; pc \vdash e[X \mapsto \tau'] : \tau[X \mapsto \tau'] \).

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

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

Case DT-BindM: 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 \( \Pi; \Gamma, X, \Gamma'[X \mapsto \tau'] ; \Theta; p; pc \vdash e[X \mapsto \tau'] : \forall Y [pc', \Theta, P, \Pi'] . \tau[X \mapsto \tau'] \).

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

**Lemma 17** (Non-bracket values sent over a channel). Let $\forall \Pi. \Pi \vdash p \triangleright pc \implies \Pi; \emptyset; p; pc \vdash v: \tau$. Then $\Pi'; \emptyset; q; pc' \vdash v: \tau$ for any $pc'$ and $q$ such that $\Pi' \vdash q \triangleright pc'$.

**Proof.** Induction on the structure of values.

- **Case Unit**: Given that $\Pi' \vdash q \triangleright pc'$. From DT-UNIT, we thus have $\Pi'; \emptyset; q; pc' \vdash (): \text{unit}$.
- **Case Pair**: Given $\Pi; \emptyset; p; pc \vdash (v_1, v_2): \tau_1 \times \tau_2$ for all $\Pi$ such that $\Pi \vdash p \triangleright pc$. Inverting DT-PAIR, we have $\Pi; \emptyset; p; pc \vdash v_1; \tau_1$. Also given that $\Pi' \vdash q \triangleright pc'$. Applying induction hypothesis, we have $\Pi'; \emptyset; q; pc' \vdash v_1; \tau_1$. From DT-PAIR, we thus have all premises to prove $\Pi'; \emptyset; q; pc' \vdash (v_1, v_2): \tau_1 \times \tau_2$.

**Case Del**: Similar to the above case.

**Case Inj**: Similar to the above case.

**Case Seal**: Similar to the above case.

**Case Where**: Similar to the above case.

**Case Lam**: Given $\Pi; \emptyset; p; pc \vdash \lambda(x: \tau)[pc'', \Theta'', \mathcal{P}, \Pi_\lambda]. e: \tau$ such that for every $j \in \{1 \ldots m\}$. If $p_j, D_j \vdash e_j \rightarrow e'_j$ then $\Pi_j; \emptyset; p_j; pc_j \vdash e_j: \tau_j$, for every $\tau_j$, for every $j \in \{1 \ldots m\}$. From DT-LAM, we have

$$\forall p' \in \mathcal{P}, \Pi_\lambda; x: \tau; \Theta''; p'; pc'' \vdash e: \tau$$

We are also given that $\Pi' \vdash q \triangleright pc'$. Combining this with above, from DT-LAM, we thus have all premises to prove $\Pi'; \emptyset; q; pc'' \vdash \lambda(x: \tau')[pc'', \Theta'', \mathcal{P}, \Pi_\lambda]. e: \tau$.

**Case TLam**: Similar to above.

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 $j \in \{1 \ldots m\}$, we have

$$\Pi_j; \Gamma_j; x: \tau'; \Theta_j; p_j; pc_j \vdash e: \tau_j$$

and $\Pi_j; \Gamma_j; x: \tau'; \Theta_j; p_j; pc_j \vdash e: \tau_j$. From the premises we have,

$$\Pi_j; \Gamma_j; x: \tau'; \Theta_j; p_j; pc_j \vdash e: \tau_j$$

Since $\Pi_j \vdash p_j \triangleright pc_j$, 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 $e'_j = e_j[x/v]$. Invoking Lemma 14, we have $\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e[j/x]: \tau_j$.

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

**Case DE-CASE1**: Given

$$e_j = \text{case } (\text{inj}_1 v) \circ \text{inj}_1(x). e_{j1} | \text{inj}_2(x). e_{j2}$$

and $e'_j = e_{j1}[x/v]$. Also, $\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash \text{case } (\text{inj}_1 v) \circ \text{inj}_1(x). e_{j1} | \text{inj}_2(x). e_{j2}: \tau$. From the premises we have, $\Pi_j; \Gamma_j; x: \tau'; \Theta_j; p_j; pc_j \vdash e_{j1}: \tau_j$. From DT-INJ, we have $\Pi_j; \Gamma_j; x: \tau'; \Theta_j; p_j; pc_j \vdash e: \tau_j$. 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 $\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash \eta_\ell v: \ell$ says $\tau$.

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

$$\Pi; \Gamma; \Theta; p; pc \vdash v: \tau'$$

$$\Pi; \Gamma, x: \tau'; \Theta; p; pc \vdash e: \tau$$

$$\Pi \vdash pc \cup \ell \leq \tau$$

(50) (51) (52) (53)
We have to prove that \( \Pi; \Gamma; \Theta; p; pc \vdash e' \{ x/v \}: \tau \). Since we have that \( \Pi \vdash p \succ pc \), applying PC reduction (Lemma 11) to the premise (51), 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 \( e = \text{assume } v \text{ in } e' \text{ and } e' = e' \text{ where } v \). Also, \( \Pi; \Gamma; \Theta; p; pc \vdash \text{assume } v \text{ in } e' : \tau \). Let \( D \) be such that for every \( \langle p \succ q \rangle \in \Pi, \langle p \succ q \rangle \in D \). From DT-ASSUME, we have

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; pc & \vdash v : (p \succ q) \\
\Pi; \langle p' \succ q \rangle; \Gamma; \Theta; pt; pc & \vdash e' : \tau \\
\Pi & \vdash pc \succ \nabla(q) \\
\Pi & \vdash \nabla(p') \succ \nabla(q^-) \\
\Pi & \vdash p' \succ pc
\end{align*}
\]

We need to prove:

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

Comparing with the given premises, we already have the required premises.

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; pc & \vdash v : (p \succ q) \\
\Pi; \langle p \succ q \rangle; \Gamma; \Theta; p'; pc & \vdash e : \tau \\
\Pi & \vdash pc \succ \nabla(q) \\
\Pi & \vdash \nabla(p') \succ \nabla(q^-) \\
\Pi & \vdash p' \succ pc
\end{align*}
\]

Hence proved.

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

\[
\begin{align*}
\Pi; \langle a \succ b \rangle; \Gamma; \Theta; p; pc & \vdash e : \tau \\
\Pi; \Gamma; \Theta; p; pc & \vdash v : (a \succ b)
\end{align*}
\]

From DE-WHERE, we have \( p, D \cdot v \vdash e \rightarrow e' \). So, we have that \( v \in D, v \in \Pi \cdot (a \succ b) \). Applying inductive to the premise (66), we have that \( \Pi; \langle a \succ b \rangle; \Gamma; \Theta; p; pc \vdash e' : \tau \) and so \( \Pi; \Gamma; \Theta; p; pc \vdash e' \text{ where } v : \tau \)

**Case DE-TEE:** Given \( e = \text{TEE} e \text{ and } e' = \text{runTEE} e \). Also given \( \Pi; \Gamma; \Theta; p; pc \vdash \text{TEE} e : \text{unit};\emptyset \). From DT-TEE, we trivially have that \( \Pi; \Gamma; \Theta; p; pc \vdash \text{runTEE} e : \text{unit};\emptyset \).

**Case DE-TEE**': Given \( e = \text{runTEE} e \text{ and } e' = \text{runTEE} e' \). Also given \( \Pi; \Gamma; \Theta; p; pc \vdash \text{runTEE} e : \text{unit};\emptyset \). From the premises of DT-TEE, we have

\[
\begin{align*}
\Pi; \emptyset; \Theta; t; t^- \land pc^- & \vdash e : \tau
\end{align*}
\]

From the premises of DE-TEE, we have

\( t, D \vdash e \rightarrow e' \)

Applying induction hypothesis to the premise, we have

\[
\begin{align*}
\Pi; \emptyset; \Theta; t; t^- \land pc^- & \vdash e' : \tau
\end{align*}
\]

Hence proved.

**Case DE-TEE:** Given \( e = \text{TEE} e \text{ and } e' = (\emptyset) : \emptyset \). Also given \( \Pi; \Gamma; \Theta; p; pc \vdash \text{runTEE} v : \text{unit};\emptyset \). From DT-UNIT and DT-HALT, we have that \( \Pi; \Gamma; \Theta; p; pc \vdash (\emptyset) : \text{unit};\emptyset \). Thus \( \Pi; \Gamma; \Theta; p; pc \vdash e' : \text{unit};\emptyset \).

**Case DE-SEND:** Given \( p, D \vdash \langle p, \text{send } \nu \text{ v then } e_{sn} \rangle \rightarrow \langle p, \text{send } \nu \text{ v' then } e_{sn} \rangle \) where \( v' = \text{closure}_\text{del}(D, v) \). Also, \( \Pi; \Gamma; \Theta; p; pc \vdash \text{send } \nu \text{ v then } e_{sn} : \text{unit} \). We need to prove that

\[
\begin{align*}
\Pi; \Gamma; \Theta; p; pc & \vdash \overline{\text{send } \nu \text{ v'}} \text{ then } e_{sn} : \emptyset
\end{align*}
\]
Inverting the premises of DT-SEND, we have that

\[
\Pi; \Gamma; \Theta; pl; pc \vdash ch: \text{chan}_{p \to q} \quad pc_{ch} \xrightarrow{\tau}
\]

\[
\Pi; \Gamma; \emptyset; pc \vdash \tau: \hat{\tau}
\]

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

\[
\tau' \in \{ \hat{\tau}', \hat{\tau}'\hat{\square}\}
\]

\[
\Pi \vdash pc \sqsubseteq pc_{ch}
\]

\[
\Pi \vdash pc_{ch} \sqsubseteq pc'
\]

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

\[
\Pi \vdash p \gg pc
\]

\[
\Pi \vdash p \gg pc_{ch}
\]

To prove what we want, we have all the required premises except

\[
\Pi'; \emptyset; \emptyset; p; pc \vdash \nu': \tau
\]

for some \( \Pi' \) such that \( \Pi' \subseteq \Pi \). Since \text{closure}_\text{del}(D, \nu) \) closes over required delegations, \( \nu' \) 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 \( e = v; \Box; \Box \) and \( e' = v; \Box \). From DT-HALT, the type of \( v; \Box \) is \( \hat{\tau}; \Box \). From DT-HALT2, the type of \( e \) is thus \( \hat{\tau}; \Box \). We already have that the type of \( e' \) is also \( \hat{\tau}; \Box \). Hence proved.

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

\[
\Pi; \Gamma; \Theta; p; pc \vdash (v \nu') \text{ where } \langle p \gg q \rangle; \tau
\]

From DT-App we have:

\[
\Pi; \Gamma; \Theta; pl; pc \vdash v \text{ where } \langle p \gg q \rangle; \tau
\]

\[
\Pi; \Gamma; \Theta; pl; pc \vdash \nu'; \tau_1
\]

\[
\Pi \vdash pc \sqsubseteq pc'
\]

\[
pl \in \mathcal{P}
\]

\[
\Theta \mid \text{dom}(\nu') = \Theta'
\]

\[
\forall\langle p \gg q \rangle \in \Pi'. \Pi \vdash p \gg q
\]

\[
\Pi \vdash pl \gg pc
\]

Rule DT-WHERE gives us the following:

\[
\Pi; \Gamma; \Theta; p; pc \vdash \langle p \gg q \rangle; \langle p \gg q \rangle
\]

\[
\Pi \vdash pc \gg \nabla(q)
\]

\[
\Pi \vdash \nabla(p^{-}) \gg \nabla(q^{-})
\]

\[
\Pi \cdot \langle p \gg q \rangle; \Gamma; \Theta; p; pc \vdash v; \tau_1
\]

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

\[
\Pi \cdot \langle p \gg q \rangle; \Gamma; \Theta; p; pc \vdash \nu' \gg \tau
\]

First, from (79), (80), (89) to (84) and lemma extending delegation contexts (Lemma 10 and Lemma 8):

\[
\Pi \cdot \langle p \gg q \rangle; \Gamma; \Theta; p; pc \vdash \nu'; \tau_1
\]

\[
\Pi \cdot (p \gg q) \vdash pc \sqsubseteq pc' pl \in \mathcal{P}
\]

\[
\Theta \mid \text{dom}(\nu') = \Theta'
\]

\[
\forall(a \gg b) \in \Pi'. \Pi \cdot \langle p \gg q \rangle \vdash a \gg b
\]

\[
\Pi \cdot \langle p \gg q \rangle \vdash pl \gg pc
\]
Combining with (88), we have (89). Remaining clauses give us

$$\Pi; \Gamma; \Theta; p; pc \vdash (v \, v') \quad \text{where} \quad \langle p \gg q \rangle : \tau$$

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

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

From DT-TAPP we have:

$$\Pi; \Gamma; \Theta; pl; pc \vdash v \quad \text{where} \quad \langle p \gg q \rangle : \forall X[pc', \Theta', \varphi, \Pi']. \tau$$

$$\Pi \vdash pc \subseteq pc'$$  \hspace{1cm} (96)

Rule DT-WHERE gives us the following:

$$\Pi; \Gamma; \Theta; p; pc \vdash (p \gg q) : (p \gg q)$$

$$\Pi \vdash pc \gg \nabla(q)$$  \hspace{1cm} (98)

$$\Pi \vdash \nabla(p^-) \gg \nabla(q^-)$$  \hspace{1cm} (99)

$$\Pi \cdot (p \gg q); \Gamma; \Theta; p; pc \vdash v : \forall X[pc', \Theta', \varphi, \Pi']. \tau$$

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,

$$\Pi \cdot (p \gg q); \Gamma; \Theta; p; pc \vdash v \, \tau' : \tau[X \mapsto \tau']$$

First, from (96) and extending delegation context (Lemma 8), we get:

$$\Pi \cdot (p \gg q) \vdash pc \subseteq pc'$$  \hspace{1cm} (102)

Combining with (100), we have (101). Remaining clauses give us

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

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

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

From DT-UNPAIR, we have:

$$\Pi; \Gamma; \Theta; p; pc \vdash (v_1, v_2) \quad \text{where} \quad \langle p \gg q \rangle : \tau_1 \times \tau_2$$  \hspace{1cm} (103)

From (103) and DT-WHERE, we have:

$$\Pi; \Gamma; \Theta; p; pc \vdash (p \gg q) : (p \gg q)$$

$$\Pi \vdash pc \gg \nabla(q)$$  \hspace{1cm} (105)

$$\Pi \vdash \nabla(p^-) \gg \nabla(q^-)$$  \hspace{1cm} (106)

$$\Pi \cdot (p \gg q); \Gamma; \Theta; p; pc \vdash (v_1, v_2) : \tau_1 \times \tau_2$$  \hspace{1cm} (107)

From (107) and DT-UNPAIR, we have: \( \Pi \cdot (p \gg q)\, pc \sqcup e; \Gamma; \Theta; p; pc \vdash \text{proj} \_i (v_1, v_2) : \tau_i \). Combining with remaining premises ((104) to (107)) we have \( \Pi; \Gamma; \Theta; p; pc \vdash \text{proj} \_i (v_1, v_2) : \tau_i \). Continuing with remaining premises ((104) to (107)) we have \( \Pi; \Gamma; \Theta; p; pc \vdash \text{proj} \_i (v_1, v_2) : \tau_i \). Continuing with remaining premises ((104) to (107)) we have \( \Pi; \Gamma; \Theta; p; pc \vdash \text{proj} \_i (v_1, v_2) : \tau_i \).

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

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

From DT-CASE we have:

$$\Pi; \Gamma; \Theta; p; pc \vdash v \quad \text{where} \quad \langle p \gg q \rangle : \tau_1 + \tau_2$$

$$\Pi \vdash pc \sqcup e \leq \tau$$

$$\Pi \vdash pc \subseteq e$$

$$\Pi; \Gamma; x : \tau_1; \Theta; p; pc \sqcup e \vdash e \_1 : \tau$$

$$\Pi; \Gamma; x : \tau_2; \Theta; p; pc \sqcup e \vdash e \_2 : \tau$$
From (108) and rule DT-WHERE, we get the following:

\[ \begin{align*}
\Pi; \Gamma; \Theta; p; pc \vdash (p \Rightarrow q) & : (p \Rightarrow q) \\
\Pi \vdash pc \Rightarrow \nabla(q) & \\
\Pi \vdash \nabla(p^-) \Rightarrow \nabla(q^-) & \\
\Pi; \Gamma; \Theta; p; pc \vdash v: \tau_1 + \tau_2 &
\end{align*} \] (113)

The key premise to prove is that:

\[ \Pi \cdot (p \Rightarrow q) pc \sqcup \ell; \Gamma; \Theta; p; pc \vdash (\text{case } v \text{ of } \text{inj}_1(x). e_1 | \text{inj}_2(x). e_2): \tau \]

which follows from (116) and extending delegations in equations (109) to (112) (Lemma 10). Combining with remaining premises, we have

\[ \Pi; \Gamma; \Theta; p; pc \vdash (\text{case } v \text{ of } \text{inj}_1(x). e_1 | \text{inj}_2(x). e_2) \text{ where } (p \Rightarrow q): \tau \]

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

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

From DT-UNITM we have:

\[ \Pi; \Gamma; \Theta; pk; pc \vdash v \text{ where } (p \Rightarrow q): \tau \] (117)

From DT-WHERE, we have:

\[ \Pi; \Gamma; \Theta; p; pc \vdash (p \Rightarrow q): (p \Rightarrow q) \] (118)

\[ \Pi \vdash pc \Rightarrow \nabla(q) \] (119)

\[ \Pi \vdash \nabla(p^-) \Rightarrow \nabla(q^-) \] (120)

\[ \Pi \cdot (p \Rightarrow q); \Gamma; \Theta; p; pc \vdash v: \tau \] (121)

From (121) and DT-UNITM, we have

\[ \Pi \cdot (p \Rightarrow q); \Gamma; \Theta; p; pc \vdash \eta_\ell v: \ell \text{ says } \tau \]

Combining with other premises ((118) to (121)), we have \( \Pi; \Gamma; \Theta; p; pc \vdash \eta_\ell v \text{ where } (p \Rightarrow q): \ell \text{ says } \tau \).

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

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

From DT-BINDM we have:

\[ \Pi; \Gamma; \Theta; pk; pc \vdash (v \text{ where } (p \Rightarrow q)): \ell \text{ says } \tau' \] (122)

\[ \Pi; \Gamma; x: \tau'; \Theta; p; pc \sqcup \ell \vdash e: \tau \] (123)

\[ \Pi \vdash pc \sqcup \ell \leq \tau \] (124)

From (122) and rule DT-WHERE, we get the following:

\[ \begin{align*}
\Pi; \Gamma; \Theta; p; pc \vdash (p \Rightarrow q) & : (p \Rightarrow q) \\
\Pi \vdash pc \Rightarrow \nabla(q) & \\
\Pi \vdash \nabla(p^-) \Rightarrow \nabla(q^-) & \\
\Pi \vdash (p \Rightarrow q); \Gamma; \Theta; p; pc \vdash v: \ell \text{ says } \tau' &
\end{align*} \] (125) \( (126) \) \( (127) \) \( (128) \)

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

\[ \begin{align*}
\Pi \cdot (p \Rightarrow q); \Gamma; \Theta; p; pc & \vdash \text{bind } x = v \text{ in } e: \tau \\
\Pi; \Gamma; \Theta; p; pc & \vdash (p \Rightarrow q): (p \Rightarrow q) \\
\Pi \vdash pc \Rightarrow \nabla(q) & \\
\Pi \vdash \nabla(p^-) \Rightarrow \nabla(q^-) &
\end{align*} \] (129) \( (130) \) \( (131) \) \( (132) \)

Extending the delegation context (Lemma 10) in the premises (123), (124) and from (128) we have (129).
We already have (130) from (125); (131) from (126); (132) from (127). Combining, we have

$$\Pi; \Gamma; \Theta; p; pc \vdash (\text{bind } x = v \text{ in } e) \text{ where } \langle p \gg q \rangle : \tau$$

**Case DW-ASSUME:** Given $e = \text{assume } v \text{ where } \langle a \gg b \rangle \text{ in } e$ and $e' = \text{assume } v \text{ in } e$ where $\langle a \gg b \rangle$. From DT-ASSUME, we have

$$\Pi; \Gamma; \Theta; p; pc \vdash e: \tau$$

$$\Pi \parallel pc \gg \nabla(s)$$

$$\Pi \parallel \nabla(r^-) \gg \nabla(s^-)$$

Expanding the first premise using DT-WHHERE, we have

$$\Pi; \Gamma; \Theta; p; pc \vdash \langle a \gg b \rangle: \langle a \gg b \rangle$$

$$\Pi \cdot \langle a \gg b \rangle; \Gamma; \Theta; p; pc \vdash v: \langle r \gg s \rangle$$

$$\Pi \parallel pc \gg \nabla(b)$$

$$\Pi \parallel \nabla(a^-) \gg \nabla(b^-)$$

We want to show

$$\Pi; \Gamma; \Theta; p; pc \vdash \langle a \gg b \rangle: \langle a \gg b \rangle$$

$$\Pi \cdot \langle a \gg b \rangle; \Gamma; \Theta; p; pc \vdash \text{assume } v \text{ in } e: \tau$$

$$\Pi \parallel pc \gg \nabla(b)$$

$$\Pi \parallel \nabla(a^-) \gg \nabla(b^-)$$

Extending delegation context (Lemma 10) in the premises (134), (135), (140) and combining with topmost premise we have the (142). Remaining premises follow from (137), (139) and (140).

**Case DW-TEEG:** Given $e = \text{runTEE}^\tau(\hat{v} \text{ where } \langle a \gg b \rangle)$ and $e' = (\text{runTEE}^f \hat{v}) \text{ where } \langle a \gg b \rangle$. Also given $\Pi; \Gamma; \Theta; p; pc \vdash e: \text{unit}$. From DT-TEEG, we have

$$\Pi; \emptyset; \Theta'; t; t^- \land pc^- \vdash \hat{v} \text{ where } \langle a \gg b \rangle: \tau$$

$$\tau \in \{\text{unit, unit}^\square\}$$

$$C = \{ch | \Theta(ch) = \text{chan}_{t\gg p} pc' \gg \land \Pi \parallel pc \gg pc' \}$$

$$\Theta |_{C'} = \Theta'$$

$$\Pi \parallel p \gg pc$$

Expanding the first premise using DT-WHHERE, we have

$$\Pi; \emptyset; \Theta'; t; pc^- \land \hat{v} \vdash \langle a \gg b \rangle: \langle a \gg b \rangle$$

$$\Pi \cdot \langle a \gg b \rangle; \emptyset; \Theta'; t; pc^- \land \hat{v} \vdash \hat{v}: \tau$$

$$\Pi \parallel pc \gg \nabla(b)$$

$$\Pi \parallel \nabla(a^-) \gg \nabla(b^-)$$

$$\Pi \parallel t \gg pc^- \land t^-$$

To prove $\Pi; \Gamma; \Theta; p; pc \vdash e' : \text{unit}^\square$, we need the following premises:

$$\Pi; \Gamma; \Theta; p; pc \vdash \langle a \gg b \rangle: \langle a \gg b \rangle$$

$$\Pi \cdot \langle a \gg b \rangle; \Gamma; \Theta; p; pc \vdash \text{runTEE}^f \hat{v}: \text{unit}^\square$$

$$\Pi \parallel pc \gg \nabla(b)$$

$$\Pi \parallel \nabla(a^-) \gg \nabla(b^-)$$

$$\Pi \parallel p \gg pc$$

(155) follows from (149) using DT-UNIT. To prove (156), we need the following premises

$$\Pi; \emptyset; \Theta'; t; t^- \land pc^- \vdash \hat{v}: \tau$$

$$C' = \{ch | \Theta(ch) = \text{chan}_{t\gg p} pc' \gg \land \Pi \cdot \langle a \gg b \rangle \parallel pc \gg pc' \}$$

$$\Theta |_{C'} = \Theta'$$

$$\Pi \parallel p \gg pc$$
Invoking lemma that values do not depend on the channel environment (Lemma 12) on premise (151), we have (160). From premises (161) to (163) we thus have the premise (156). Weakening the delegation context in (148), we have (163). Premises (157) and (158) follow from (152) and (153). Hence proved.

Case DW-HALT: Given \( e = p, D \vdash (\hat{v} \text{ where } \langle a \gg b \rangle); \square \) and \( e' = p, D \vdash (\hat{v}; \square \text{ where } \langle a \gg b \rangle). \) 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 sealed values can not take a step, inverting the well-typedness of bracket is only possible through DT-BRACKET and not through DT-BRACKET-VALUES. From DT-BRACKET, we have
\[
\Pi; \Gamma; \Theta; p; pc \vdash e_1 : \tau
\]

Since (164) 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 ((165) to (167)) 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 \( e = \text{proj}_i ((v_{11}, v_{12}) | (v_{21}, v_{22})) \) and \( e' = (v_{11} | v_{21}) \) Also \( \Pi; \Gamma; \Theta; p; pc \vdash \text{proj}_i ((v_{11}, v_{12}) | (v_{21}, v_{22})): \tau_i. \) We have to prove
\[
\Pi; \Gamma; \Theta; p; pc \vdash (v_{11} | v_{21}): \tau_i
\]

From DT-UNPAIR, we have:
\[
\Pi; \Gamma; \Theta; p; pc \vdash ((v_{11}, v_{12}) | (v_{21}, v_{22})): \tau_1 \times \tau_2
\]

Since they are already values, they can be inverted using DT-BRACKET-VALUES. This approach is more conservative.
\[
\Pi; \Gamma; \Theta; p; pc \vdash (v_{11}, v_{12}): \tau_1 \times \tau_2
\]

From (169), (170) 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 (171) and DP-PAIR, we have \( \Pi \vdash H^\tau \leq \tau. \) Combining with other premises, from DT-BRACKET-VALUES, we have \( \Pi; \Gamma; \Theta; p; pc \vdash (v_{1i} | v_{2i}): \tau_i. \)

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

Case BD-BINDM3: Given \( e = \text{bind} x = (\eta_\ell \ v_1 | \eta_\ell \ v_2) \) in \( e. \) Here \( e' = ([e]_1[x \mapsto v_1] | [e]_2[x \mapsto v_2]). \) Also \( \Pi; \Gamma; \Theta; p; pc \vdash \text{bind} x = (\eta_\ell \ v_1 | \eta_\ell \ v_2) \) in \( e: \tau. \) From DT-BINDM, we have
\[
\Pi; \Gamma; \Theta; pl; pc \vdash (\eta_\ell \ v_1 | \eta_\ell \ v_2): \ell \text{ says } \tau'
\]
\[
\Pi; \Gamma; x: \tau'; \Theta; p; pc \vdash \ell: \tau
\]
\[
\Pi \vdash pc \sqcup \ell \leq \tau
\]
\[
\Pi \vdash p \not\triangleright pc
\]

From (172) and DT-BRACKET-VALUES, we have
\[
\Pi; \Gamma; \Theta; p; pc \vdash \eta_\ell \ v_1: \ell \text{ says } \tau'
\]
\[
\Pi; \Gamma; \Theta; p; pc \vdash \eta_\ell \ v_2: \ell \text{ says } \tau'
\]
\[
\Pi \vdash H^\tau \subseteq \ell
\]

We have to prove that
\[
\Pi; \Gamma; \Theta; p; pc \vdash ([e]_1[x \mapsto v_1] | [e]_2[x \mapsto v_2]): \tau
\]
For some \(\hat{pc}\) we need the following premises to satisfy DT-BRACKET:

\[
\Pi; \Gamma; \Theta; p; \hat{pc} \vdash e[x \rightarrow v_1]: \tau \\
\Pi; \Gamma; \Theta; p; \hat{pc} \vdash e[x \rightarrow v_2]: \tau \\
\Pi \vdash (H^\pi \sqcup pc) \sqsubseteq \hat{pc} \\
\Pi \vdash H^\pi \leq \tau
\]

(179) (180) (181) (182)

A natural choice for \(\hat{pc}\) is \(pc \sqcup \ell\). From (173)

\[
\Pi; \Gamma, x : \tau'; \Theta; p; \hat{pc} \vdash e: \tau
\]

Invoking clearance lemma (Lemma 7) on the premise (173) we have that

\[
\Pi \vdash p \gg pc \sqcup \ell
\]

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

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

Lemma 15 (bracket projection) and Lemma 14 (substitution), we have (179) and (180). From (178) and (174) we have (182).

Thus we have all premises necessary to prove \(\Pi; \Gamma; \Theta; p; pc \vdash \Pi' \vdash H\pi\).

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

Case BD-WHERE: 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.

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

Figure 24 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 \(\Pi \vdash W[e] : \tau\) then \(\exists \Pi', \Gamma', \tau', pc', p' \vdash \Pi' \vdash W[e] : \tau \vdash \Pi'; \Gamma'; \Theta'; p'; pc' \vdash e : \tau'\) such that \(\Pi; \Gamma; \Theta; p; pc \vdash W[e] : \tau \vdash \Pi'; \Gamma'; \Theta'; p'; pc' \vdash e : \tau'\) 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 \(\Pi; \Gamma; \Theta'; p; pc \vdash e : \tau\) such that \(\Theta' |_{dom(\Theta)} = \Theta\).

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

**Lemma 21** (Weakening Channel Env for Contexts). If \(\Pi; \Gamma; \Theta; p; pc \vdash W[e] : \tau\) then for all \(\Theta'\) such that \(\Theta' |_{dom(\Theta)} = \Theta\), \(\Pi; \Gamma; \Theta'; p; pc \vdash W[e] : \tau\).

**Proof.** Straightforward invocation of Lemma 20.

**Lemma 22** (Hole Substitution). Let \(\Pi; \Gamma; \Theta; p; pc \vdash W[e] : \tau\) and \(\Pi; \Gamma; \Theta; p; pc \vdash W[e'] : \tau \vdash \Pi'; \Gamma'; p'; pc' \vdash e : \tau'. If \(\Pi'; \Gamma'; \Theta'; p'; pc' \vdash e' : \tau'\) then \(\Pi; \Gamma; \Theta; p; pc \vdash W[e'] : \tau\).

**Proof.** Proof is by induction on the structure of W.

**Lemma 23** (Hole Substitution by Weakening Channel Env). Let \(\Pi; \Gamma; \Theta; p; pc \vdash W[spawn \ q \ (pl, ch_1[pc_1, \tau_1], ch_2[pc_2, \tau_2]), e_1 \ then \ e_2] : \tau\). Then \(\Pi; \Gamma; \Theta'; p; pc \vdash W[e_2] : \tau\) where

\[
\Theta' = \Theta | \{ch_1 \mapsto chan_{p \rightarrow q} pc_1 \ \tau_1, ch_2 \mapsto chan_{p \rightarrow q} pc_2 \ \tau_2\}
\]

**Proof.** Proof is by induction on the structure of W. (This is actually E since spawn doesn’t occur inside TEE).

Case [ ] Given \(\Pi; \Gamma; \Theta; p; pc \vdash [spawn \ q \ (pl, ch_1[pc_1, \tau_1], ch_2[pc_2, \tau_2]), e_1 \ then \ e_2] : \tau\). Inverting using DT-HOLE and then using DT-SPAWN, we have that:

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

Using DT-HOLE, we have \(\Pi; \Gamma; \Theta'; p; pc \vdash [e_2] : \tau\).

36
\[
\begin{array}{ll}
\text{W-HOLE} & \Pi; \Gamma; \Theta; p; \pc \vdash e : \tau \\
\end{array}
\]

\[
\begin{array}{ll}
\text{W-LAM} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash e : \tau'' \quad \Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \tau'' \\
\Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \tau'' \quad \Pi; \Gamma; \Theta; p; \pc \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-ARG} & \Pi; \Gamma; \Theta; p; \pc \vdash e : \tau'' \quad \Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \tau'' \quad \Pi; \Gamma; \Theta; p; \pc \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-PAIR-LEFT} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \tau_1 \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-PAIR-RIGHT} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \tau_2 \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-UNIT} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \tau \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-UNITM} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash \eta \ W[e] : \ell \ says \ \tau \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau
\end{array}
\]

\[
\begin{array}{ll}
\text{W-RUNTEE} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash \text{runTEE} \ W[e] : \tau \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau
\end{array}
\]

\[
\begin{array}{ll}
\text{W-BIND} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \tau'' \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-ASSUME} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash W[e] : \ell_1 \rightarrow \ell_2 \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-SEND} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash \text{send} \ W[e] : \tau \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-CASE} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash \text{case} \ W[e] \ of \ inj_1(x) . e_1 \ | \ inj_2(x) . e_2 : \unit \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

\[
\begin{array}{ll}
\text{W-WHERE} & \\
\Pi; \Gamma; \Theta; p; \pc \vdash v : (p \equiv q) \quad \Pi; (p \equiv q) ; \Gamma; \Theta; p; \pc \vdash W[e] : \tau \rightarrow \Pi' \quad \Theta' ; p' ; \pc' \vdash e : \tau'
\end{array}
\]

Fig. 24: Extracting holes from well-typed contexts

Case \(W\ e\): Given \(\Pi; \Gamma; \Theta; p; \pc \vdash W[\text{spawn @} (pl, ch_1[pc_1; \tau_1], \ ch_2[pc_2; \tau_2])]. \ e_1 \ then \ e_2\ e : \tau\). Inverting using DT-APP, we have that:

\[
\begin{array}{ll}
\Pi; \Gamma; \Theta; p; \pc \vdash W[\text{spawn @} (pl, ch_1[pc_1; \tau_1], \ ch_2[pc_2; \tau_2])]. \ e_1 \ then \ e_2\ e : \tau & (184) \\
\Pi; \Gamma; \Theta; p; \pc \vdash e : \tau_1 & (185)
\end{array}
\]

Applying induction hypothesis to (184), we have

\[
\begin{array}{ll}
\Pi; \Gamma; \Theta'; p; \pc \vdash W[e_2] : \tau_1 & (184) \\
\Pi; \Gamma; \Theta; p; \pc \vdash e : \tau_1 & (185)
\end{array}
\]

Weakening channel environment in (185) (Lemma 20), we have

\[
\begin{array}{ll}
\Pi; \Gamma; \Theta'; p; \pc \vdash e : \tau_1
\end{array}
\]
The condition $\Theta' \mid_{\text{dom}(\Theta')}$ still holds. Thus from DT-APP, we have

$$
\Pi; \Gamma; \Theta'; p; \text{pc} \vdash W[\text{e}_2] \text{ e : } \tau
$$

Case $\nu W$: Straight forward application of induction hypothesis.
Case $\langle W, e \rangle$: Straight forward application of induction hypothesis.
Case $\langle \nu, W \rangle$: Straight forward application of induction hypothesis.
Case proj, $W$: Straight forward application of induction hypothesis.
Case inj, $W$: Straight forward application of induction hypothesis.
Case bind $x = W \text{ in e}$: Straight forward application of induction hypothesis.
Case $W \tau$: Straight forward application of induction hypothesis.
Case assume $W \text{ in e}$: Straight forward application of induction hypothesis.
Case send $\nu W$ then $e$: Straight forward application of induction hypothesis.
Case case $W$ of inj$_1(x), e \mid$ inj$_2(x), e$: Straight forward application of induction hypothesis.
Case W where $\nu$: Straight forward application of induction hypothesis.
Case runTEE$'$ $W$: Syntactically not possible.

\[\square\]

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

1. $\Pi \vdash H^\pi \sqcup \text{pc} \sqsubseteq \text{pc}_H$
2. $\Pi; \Gamma; \Theta; p; \text{pc}_H \vdash W[\text{e}]: \tau$
3. $\Pi \vdash H^\pi \leq \tau$

then $\exists \text{pc'}_H$ such that

1. $\Pi' \vdash H^\pi \sqcup \text{pc'} \sqsubseteq \text{pc'}_H$
2. $\Pi'; \Gamma'; \Theta'; p'; \text{pc'}_H \vdash e: \tau'$
3. $\Pi' \vdash H^\pi \leq \tau'$

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

Case W-HOLE: Straightforward as $\text{pc'} = \text{pc}$. Choose $\text{pc'}_H = \text{pc}_H$.
Case W-LAM: Straightforward application of induction hypothesis.
Case W-APP: Straightforward application of induction hypothesis.
Case W-ARG: Straightforward application of induction hypothesis.
Case W-PAIR-LEFT: Straightforward application of induction hypothesis.
Case W-PAIR-RIGHT: Straightforward application of induction hypothesis.
Case W-PROJ: Straightforward application of induction hypothesis.
Case W-INJ: Straightforward application of induction hypothesis.
Case W-UNITM: Straightforward application of induction hypothesis.
Case W-RUNTEE: Does not occur syntactically.
Case W-BINDM: Straightforward application of induction hypothesis.
Case W-ASSUME: Straightforward application of induction hypothesis.
Case W-SEND: Straightforward application of induction hypothesis.
Case W-CASE: Straightforward application of induction hypothesis.
Case W-WHERE: Applying induction to the premises, we have

$$
\begin{align*}
\Pi \cdot (r \gg s) & \vdash H^\pi \sqcup \text{pc} \sqsubseteq \text{pc}_H \land \\
\Pi \cdot (r \gg s) & ; \Gamma; \Theta; p; \text{pc}_H \vdash E[\text{e}]: \tau \land \\
\Pi \cdot (r \gg s) & \vdash H^\pi \leq \tau
\end{align*}
\[\implies\]

$$
\begin{align*}
\exists \text{pc'}_H. \Pi' & \vdash H^\pi \sqcup \text{pc'} \sqsubseteq \text{pc'}_H \land \\
\Pi'; \Gamma'; \Theta'; p'; \text{pc'}_H & \vdash e: \tau' \land \\
\Pi & \vdash H^\pi \leq \tau'
\end{align*}
\text{(186)}
$$

We are given that

$$
\begin{align*}
\Pi & \vdash H^\pi \sqcup \text{pc} \sqsubseteq \text{pc}_H \land \\
\Pi & \vdash H^\pi \leq \tau
\end{align*}
$$

38


This means the delegation \( r \gg s \) 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 \( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \implies \langle p_1, e_1' \rangle \parallel \cdots \parallel \langle p_i, e_i' \rangle \parallel \cdots \parallel \langle p_m, e_m' \rangle \) such that \( n \geq m \) and \( \forall k \in \{1, \ldots, m \} \), \( \Pi_k; \Gamma_k; p_k; pc_k \vdash e_k: \tau_k \). Also let,

\[
\begin{align*}
&\forall \ell'. \forall \{i, j\} \subseteq \{1, \ldots, m \}. \Pi_i \vdash \tau^* \subseteq \ell' \iff \Pi_j \vdash \tau^* \subseteq \ell' \\
&\forall \ell'. \forall \ell. \Pi_k \vdash \tau^* \subseteq \ell' \iff \Pi_k \vdash \tau^* \subseteq \ell' 
\end{align*}
\]

Then the following hold.

1. \( \forall k \vdash \tau^* \subseteq \ell' \iff \Pi_k \vdash \tau^* \subseteq \ell' \)
2. If \( n = m + 1 \), then \( \forall i \vdash \tau^* \subseteq \ell' \iff \forall \{i, j\} \subseteq \{1, \ldots, m \}. \Pi_i \vdash \tau^* \subseteq \ell' \)
3. If \( n = m + 1 \), then \( \forall \ell' \), \( \forall \ell. \Pi_i \vdash \tau^* \subseteq \ell' \iff \Pi_j \vdash \tau^* \subseteq \ell' \)
4. \( \forall \ell'. \forall \{i, j\} \subseteq \{1, \ldots, n \}. \Pi_i \vdash \tau^* \subseteq \ell' \iff \Pi_j \vdash \tau^* \subseteq \ell' \)

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

**Par-Step:** Given

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i: \tau_i \parallel \cdots \parallel \Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m: \tau_m
\]

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, \( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \implies \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \). From the premises we have that \( p_i, \emptyset \vdash e_i \rightarrow e_i' \) for some \( i \in \{1, \ldots, m \} \). Thus we have \( n = m \) and \( e_i' = e_k \) for every \( k \in \{1, \ldots, m \} \setminus \{i\} \).

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

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

**Par-Spawn:** Given

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i: \tau_i \parallel \cdots \parallel \Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m: \tau_m
\]

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, \( \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \implies \langle p_1, e_1 \rangle \parallel \cdots \parallel \langle p_i, e_i \rangle \parallel \cdots \parallel \langle p_m, e_m \rangle \). From the premises we have that \( p_i, \emptyset \vdash e_i \rightarrow e_i' \) for some \( i \in \{1, \ldots, m \} \). Thus we have \( n = m \) and \( e_i' = e_k \) for every \( k \in \{1, \ldots, m \} \setminus \{i\} \).

For \( k = i \), invoking type preservation for single process (Lemma 18) gives us that \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i' \vdash \tau_i \). It remains to show that

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

Invoking Lemma 19, we have \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash W[\text{spawn } \# q [\text{pl, ch}_r [pc_i; \tau_i], \text{ch}_s [pc_i; \tau_s]]]. e \then e' \vdash \tau_i \lor \Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_i \vdash W[\text{spawn } \# q [\text{pl, ch}_r [pc_i; \tau_i], \text{ch}_s [pc_i; \tau_s]]]. e \then e' \vdash \tau_i \). From DT-SPAWN, we have \( \Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_i \vdash W[e_i'] \vdash \tau_i \).

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

**Par-Send-Recv:** Here \( n = m \). Without loss of generality, let \( (e_i, e_j) = (W[\text{send } \nu v \then e_{sn}], W[\text{recv } \nu v \as x \in e]) \).

Then \( e_i' = e_j' = W[\text{send } \nu v \then e_{sn}], W[\text{recv } \nu v \as x \in e] \).

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 \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash W[\text{send } \nu v \then e_{sn}] \vdash \tau_i \) and \( \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash W[\text{recv } \nu v \as x \in e] \vdash \tau_j \). Since holes can be typed under some pc (Lemma 19), we have that \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash W[\text{send } \nu v \then e_{sn}] \vdash \tau_i \lor \Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc'_i \vdash W[\text{recv } \nu v \as x \in e] \lor \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash W[\text{recv } \nu v \as x \in e] \lor \Pi_j; \Gamma'_j; \Theta'_j; p'_j; pc'_j \vdash W[\text{recv } \nu v \as x \in e] \lor \tau_i \lor \Pi_j; \Gamma'_j; \Theta'_j; p'_j; pc'_j \vdash W[\text{recv } \nu v \as x \in e] \lor \tau_i \).

From DT-SEND, we have that \( \Pi'_i; \emptyset; \emptyset; \Pi'_i; \vdash v: \tau \) for some \( \Pi'_i \) such that \( \Pi'_i \subseteq \Pi_i \) and \( \Pi'_i \vdash p_i \gg p_i' \).

Since non-branch values sent over a channel can be typed on other places such that \( \Pi'_i \vdash p_i' \gg p_i' \) (Lemma 17), we have \( \Pi'_i; \emptyset; \emptyset; p_i'; pc_i' \vdash v: \tau \).

If \( v = (v_1 \parallel v_2) \), a bracket value, then from DT-BRACKETVALUES, we have that \( \Pi'_i \vdash H^* \leq \tau \). From the given conditions on the upward closure of \( H^* \), we have that \( \Pi'_i \vdash H^* \leq \tau \). Thus from DT-BRACKETVALUES, we have \( \Pi'_i; \emptyset; \emptyset; p_i'; pc_i' \vdash v: \tau \).

This implies \( \Pi'_i; \Gamma'_i; \Theta'_i; p_i'; pc_i' \vdash v: \tau \) (weakening delegation and variable contexts, channel environment by invoking Lemma 12, Lemma 10)
From DT-RECV, we have $\Pi_I^j; \Gamma_I^j, x : \tau; \Theta_I^j; p_I^j; pc_I^j \vdash e_n : \tau_j$. Applying PC reduction (Lemma 11), we have that $\Pi_{I'}^j; \Gamma_{I'}^j, x : \tau; \Theta_{I'}^j; p_{I'}^j; pc_{I'}^j \vdash e_n : \tau_j$. Invoking variable substitution (Lemma 14), we have that $\Pi_{I'}^j; \Gamma_{I'}^j; \Theta_{I'}^j; p_{I'}^j; pc_{I'}^j \vdash e_n [x \to v]; \square : \tau_j$. Invoking hole substitution (Lemma 22), on $\Pi_{I''}; \Gamma_{I''}; \Theta_{I''}; p_{I''}; pc_{I''} \vdash W [recv v as x \ in e; \square : \tau_j$, we have

$$\Pi_{I''}; \Gamma_{I''}; \Theta_{I''}; p_{I''}; pc_{I''} \vdash e_{I''} : \tau_j$$

From DT-SENDDEL, we also have that $\Pi_{I'}^j; \Gamma_{I'}^j; \Theta_{I'}^j; p_{I'}^j; pc_{I'}^j \vdash e_{sn} : \square$. Applying PC reduction (Lemma 11), we have that $\Pi_{I''}^j; \Gamma_{I''}^j; \Theta_{I''}^j; p_{I''}^j; pc_{I''}^j \vdash e_{sn} : \square$. Invoking hole substitution (Lemma 22), on $\Pi_{I''}; \Gamma_{I''}; \Theta_{I''}; p_{I''}; pc_{I''} \vdash W [send v then e_{sn}] : \tau_j$, we have

$$\Pi_{I''}; \Gamma_{I''}; \Theta_{I''}; p_{I''}; pc_{I''} \vdash e_{I''} : \tau_j$$

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

**BD-PAR-STEP-L:** Given

$$\langle p_1, e_1 \rangle \ || \cdots \ || \langle p_i, (e_i | e_{i2}) \rangle \ || \cdots \ || \langle p_m, e_m \rangle \ \Rightarrow \ \langle p_1, e'_1 \rangle \ || \cdots \ || \langle p_i, e'_i \rangle \ || \cdots \ || \langle p_n, e'_n \rangle$$

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

$$\langle p_1, e_1 \rangle \ || \cdots \ || \langle p_i, e_{i2} \rangle \ || \cdots \ || \langle p_m, e_m \rangle \ \Rightarrow \ \langle p_1, e_1 \rangle \ || \cdots \ || \langle p_i, e_{i2} \rangle \ || \cdots \ || \langle p_n, e_n \rangle$$

Also from the remaining premises we have

$$i \in \{1 \cdots m\}$$

$$e_i' = (e_i | e_{i2})$$

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

$$e_j' = \begin{cases} e_j' & \text{if } n = m \text{ and } j = i \\ e_i' & \text{if } n \neq m \text{ and } j \neq i \\ (e_{j1} | e_{j2}) & \text{if } n = m, j \neq i \text{ and } e_j = (e_{j1} | e_{j2}) \\ W[\langle e_{j1} | e \rangle] & \text{if } n = m, j \neq i \text{ and } e_j = W[e] \end{cases}$$

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 ≠ m and j ≠ i:** $e_i$ is a **spawn** expression. That is, we have

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

$$e_i' = (W_i[e_n] | e_{i2})$$

$$e_j' = e_{i2} = (e | \bullet)$$

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

(192)

Note that TEE’s do not have any spawn statement. Thus $W_i$ is actually $E_i$. That is,

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

$$e_i' = (E_i[e_n] | e_{i2})$$

$$e_j' = e_{i2} = (e | \bullet)$$

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

(194)
From the DT-Bracket (since it is not a sealed bracket, we cannot invert using DT-Bracket-Values), we have that \( e_i \) is protected for some \( pc'_i \) and so:

\[
\Pi_i \vdash (H^\pi \sqcup pc_i) \sqsubseteq pc'_i
\]  
(195)

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc'_i \vdash W_i[\text{spawn } @q (pl, ch_r[pc_c; \tau_r], ch_s[pc_s; \tau_s])]. e \text{ then } e_{e_k}; \tau_i
\]  
(196)

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc'_i \vdash e_{i1}; \tau \triangleright \Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc' \vdash \text{spawn } @q (pl, ch_r[pc_c; \tau_r], ch_s[pc_s; \tau_s]). e \text{ then } e_{e_k}; \tau
\]  
(197)

\[
\Pi_i \vdash H^\pi \leq \tau_i
\]  
(198)

Invoking Lemma 19 on (196), we have \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc'_i \vdash e_{i1}; \tau \triangleright \Pi'_i; \Gamma'_i; \Theta'_i; p'_i; pc' \vdash \text{spawn } @q (pl, ch_r[pc_c; \tau_r], ch_s[pc_s; \tau_s]). e \text{ then } e_{e_k}; \tau \). Inverting the above expression using DT-Spawn, we have:

\[
\Pi_i' \vdash \emptyset; \emptyset[\text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_r \tau_r, \text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_s \tau_s]; \text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_s \tau_s]; q; pc'' \vdash e : \tau_n
\]  
(199)

\[
\Pi_i' \vdash \emptyset; \emptyset[\text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_r \tau_r, \text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_s \tau_s]; \text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_s \tau_s]; p'_i; pc' \vdash e_{e_k} : \tau
\]  
(200)

\[
\Pi_i \vdash pc' \sqsubseteq pc''
\]  
(201)

\[
\Pi_i \vdash p'_i \triangleright pc'
\]  
(202)

\[
\Pi_i \vdash pc'' \leq \tau_n
\]  
(203)

Invoking hole substitution (Lemma 23) with (200) we have

\[
\Pi_i; \Gamma_i; \Theta_i'; p_i; pc'_i \vdash W_i[e_{e_k}] : \tau_i
\]

where \( \Theta'_i = \Theta_i[\text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_r \tau_r, \text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_s \tau_s] \). Weakening channel environment on (210) using Lemma 20, we have Thus, from DT-Bracket, we have that

\[
\Pi_i; \Gamma_i; \Theta_i'; p_i; pc_i \vdash (W_i[e_{e_k}] \mid e_{i2}) : \tau_i
\]

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

\[
\Pi_n; \Gamma_n; \Theta_n; q; pc_n \vdash (e \mid \bullet) : \tau_n
\]

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

\[
\Pi_i' \vdash (H^\pi \sqcup pc'') \sqsubseteq pc''_H
\]  
(204)

\[
\Pi_i' \vdash \emptyset; \emptyset[\text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_r \tau_r, \text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_s \tau_s]; q; pc'' \vdash e : \tau_n
\]  
(205)

\[
\Pi_i' \vdash H^\pi \leq \tau_n
\]  
(206)

Since high contexts (without TEE’s) have high holes, applying Lemma 24 on (195), we have that

\[
\exists pc''_H. \ \Pi_i' \vdash H^\pi \sqcup pc' \sqsubseteq pc''_H
\]  
(207)

\[
\Pi_i'; \Gamma_i'; \Theta_i'; p'_i; pc'_i \vdash \text{spawn } @q (pl, ch_r[pc_c; \tau_r], ch_s[pc_s; \tau_s]). e \text{ then } e_{e_k}; \tau
\]  
(208)

\[
\Pi_i' \vdash H^\pi \leq \tau
\]  
(209)

Invoking (208) using DT-Spawn we have that for some \( pc''_{iH} \):

\[
\Pi_i'; \emptyset; \emptyset[\text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_r \tau_r, \text{chan}_q \rightarrow \text{chan}_q \rightarrow pc_s \tau_s]; q; pc'' \vdash e : \tau_n
\]  
(210)

\[
\Pi_i' \vdash pc''_H \sqsubseteq pc''_{iH}
\]  
(211)

Premise (204) follows from (207) and (211). Premise (206) follows from (203) Premise (205) follows from (210). We thus have that \( (e \mid \bullet) \) 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 \( \hat{\Pi}_n \subseteq \hat{\Pi}_i \) (Lemma ??). Thus we have the results stated in condition 3 and 4.

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

\[
e_i = (W_i[\text{send } \nu v \text{ then } e_{sk}] | e_{i2}) \tag{212}
\]
\[
e_j = (W_j[\text{recv } \nu \text{ as } x \in e_n] | e_{j2}) \tag{213}
\]
\[
e_i' = (W_i[e_{sk}] | e_{i2}) \tag{214}
\]
\[
e_j' = (W_j[e_n[x \rightarrow v]] | e_{j2}) \tag{215}
\]
\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i; \tau_i \tag{216}
\]
\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j; \tau_i \tag{217}
\]

We have to show that:

\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1; \tau_1 \parallel \cdots \parallel \tag{218}
\]
\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash W_i[\text{send } \nu v \text{ then } e_{sk}] : \tau_i \tag{219}
\]
\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i' : \tau_i \parallel \cdots \parallel \tag{220}
\]
\[
\Pi_i \vdash H \leq \tau_i \tag{221}
\]

and

\[
\Pi_j \vdash (H \parallel pc_j) \subseteq pc_j' \tag{222}
\]
\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j' \vdash W_j[\text{recv } \nu \text{ as } x \in e_n] : \tau_j \tag{223}
\]
\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j' \vdash e_{j2} : \tau_j \tag{224}
\]
\[
\Pi_j \vdash H \leq \tau_j \tag{225}
\]

Applying induction to the step relation in the premise:

\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1: \tau_1 \parallel \cdots \parallel \tag{226}
\]
\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash W_i[e_{sk}; \emptyset] : \tau_i \parallel \cdots \parallel \tag{227}
\]
\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash W_j[e_n[x \rightarrow v]; \emptyset] : \tau_j \parallel \cdots \parallel \tag{228}
\]
\[
\Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m; \tau_m \tag{229}
\]

Replacing (219) and (223) with (226) and (227) we have the proof.

\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_1: \tau_1 \parallel \cdots \parallel \tag{230}
\]
\[
\Pi_1; \Gamma_1; \Theta_1; p_1; pc_1 \vdash e_i' : \tau_i \parallel \cdots \parallel \tag{231}
\]
\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j : \tau_j \parallel \cdots \parallel \tag{232}
\]
\[
\Pi_m; \Gamma_m; \Theta_m; p_m; pc_m \vdash e_m; \tau_m \tag{233}
\]

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

**Case \( n = m \) and \( e_j = W[e] \):** Applying induction hypothesis to the premise of \texttt{BD-PAR-STEP-L}, we have that \( \Pi_1; \Gamma_1; \Theta_i; pc_i \vdash e_{i1} : \tau_i \). We already have \( \Pi_1; \Gamma_1; \Theta_i; pc_i \vdash e_{i2} : \tau_i \) and so from \texttt{DT-BRACKET} (proving for a more restrictive case) we have

\[
\Pi_1; \Gamma_1; \Theta_i; p_i; pc_i \vdash e_i' : \tau_i \tag{234}
\]

Since both \( e_i \) and \( e_j \) take a step, it must be the case that they are \texttt{senddel} and \texttt{recv} pairs. We then have two more cases.
Case \( e_j = \textit{send} \ \nu \ \tau \) then \( e_{sk} \): Without loss of generality assume that \( e_j = \overline{\textit{send}} \ \nu \ \tau \) then \( e_{sk} \). We then have the following:

\[
e_i = (W_i[\textit{recv} \ \nu \ \text{as x in } e_{sk}] \mid e_{i2})
\]

\[
e_i' = (W_i[e_{sk}[x \rightarrow \nu]; \square] \mid e_{i2}) \tag{228}
\]

\[
\Pi; \Gamma; \Theta; p_i; pc^i \vdash (W_i[\textit{recv} \ \nu \ \text{as x in } e_{sk}] \mid e_{i2}) : \tau_i \tag{230}
\]

\[
\Pi; \Gamma; \Theta; p_i; pc^i \vdash (W_i[e_{sk}[x \rightarrow \nu]; \square] \mid e_{i2}) : \tau_i \tag{231}
\]

\[
e_j' = W_j([e_{sk} \mid \overline{\textit{send}} \ \nu \ \tau \ \text{then } e_{sk}; \square]) \tag{232}
\]

\[
\Pi; \Gamma; \Theta; p_j; pc_j \vdash W_j[\overline{\textit{send}} \ \nu \ \tau \ \text{then } e_{sk}]: \tau_j \tag{233}
\]

We have to show that

\[
\Pi; \Gamma; \Theta; p_j; pc_j \vdash W_j((e_{sk} \mid \overline{\textit{send}} \ \nu \ \tau \ \text{then } e_{sk}); \square): \tau_j
\]

From (230) and DT-BRACKET (since it is not a sealed bracket, we cannot invert using DT-BRACKET-VALUES), we have the following:

\[
\Pi; \Gamma; \Theta; p_i; pc^i \vdash W_i[\textit{recv} \ \nu \ \text{as x in } e_{sk}] : \tau_i \tag{235}
\]

\[
\Pi; \Gamma; \Theta; p_i; pc^i \vdash \textit{recv} \ \nu \ \text{as x in } e_{sk} : \tau_i \tag{236}
\]

\[
\Pi \vdash H^n \leq \tau_i \tag{237}
\]

Since holes can be typed under an appropriate \(pc_{ir} \), invoking Lemma 19 on (235) we have

\[
\Pi; \Gamma; \Theta; p_i; pc^i \vdash W_i[\textit{recv} \ \nu \ \text{as x in } e_{sk}] : \tau_i \tag{238}
\]

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

**Case** \( W_i = E_i \): Invoking Lemma 24 on (238) we have that

\[
\Pi' \vdash (H^n \cup pc_{ir}) \subseteq pc_{ir}' \tag{239}
\]

\[
\Pi'; \Gamma'; \Theta'; p_i'; pc_{ir}' \vdash \textit{recv} \ \nu \ \text{as x in } e_{sk} : \tau_i' \tag{240}
\]

\[
\Pi' \vdash H^n \leq \tau_i' \tag{241}
\]

Inverting (240) using DT-RECV we have

\[
\Pi'; \Gamma'; \Theta'; p_i'; pc_{ir}' \vdash \nu : \text{chan}_{p_i' \rightarrow p_i'} \ \text{pc}_{ch} \ \tau \tag{242}
\]

\[
\Pi; \Gamma, x : \dot{\tau}; \Theta; p \ \text{pc}' \vdash e : \tau_i' \tag{243}
\]

\[
\tau_i' \in \{\tau_i', \tau_i' \square\} \tag{244}
\]

\[
\Pi' \vdash pc_{ir}' \subseteq pc_{ch} \tag{245}
\]

\[
\Pi' \vdash pc_{ir}' \subseteq pc_{ir}'' \tag{246}
\]

\[
\Pi' \vdash pc_{ch} \subseteq pc_{ir}'' \tag{247}
\]

\[
\Pi' \vdash pc_{ir}'' \leq \tau_i' \tag{248}
\]

\[
\Pi' \vdash p_i' \Rightarrow pc_{ch} \tag{249}
\]

\[
\Pi' \vdash p_i' \Rightarrow pc_{ir}' \tag{250}
\]

Applying R-TRANS to (239) and (245), we have

\[
\Pi' \vdash H^n \subseteq pc_{ch} \tag{251}
\]

**Case** \( W_i \neq E_i \): Consider the premises in (235) and (234). If \( W_i \) includes \( \textit{runTEE} \) and \( W_i[\textit{recv} \ \nu \ \text{as x in } e_{sk}] \) is well-typed under \( pc_{ir}' \), then \( \exists pc_{ir}'' \) (since nested TEEs aren’t allowed and from Lemma 24 we have monotonic \( pc \)) such that

\[
\Pi'' \vdash H^n \subseteq pc_{ir}'' \tag{252}
\]

\[
\Pi''; \Gamma''; \Theta''; p_i; pc_{ir}'' \vdash \textit{runTEE}'[E_i[\textit{recv} \ \nu \ \text{as x in } e_{sk}]] : \text{unit}\square \tag{253}
\]

Recall the premise from DT-TEEG

\[
C = \{ ch \mid ch \in \Theta(ch) = \textit{chan}_{\tau \rightarrow p} \ \text{pc}' \ \tau \land \ \Pi'' \vdash pc_{ir}'' \subseteq pc' \}
\]

43
for some $\Pi'''$ such that $\Pi'''_{\text{dom}(\Pi')} = \Pi''$. Since $E_i$ cannot contain any runTEE or spawn, we have $\Theta'''_{|c} = \Theta'$. This implies

$$\Pi''' \vdash H^x \sqsubseteq pc_{ch} \tag{254}$$

Let us now focus on $j$th node. Since holes can be typed under appropriate $pc$, invoking Lemma 19 on (233), we have

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash W_j[send \nu v \text{ then } e_{sk}]: \tau_j \triangleright$$

From (255) and DT-SENDDEL we have

$$\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{js} \vdash \text{send } \nu v \text{ then } e_{sk}: \tau'_j \square \tag{255}$$

From (255) and DT-SENDDEL we have

$$\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{js} \vdash \text{send } \nu v \text{ then } e_{sk}: \tau'_j \square \tag{255}$$

To show that $e'_j$ is well-typed, we first need to find a $pc'_{js}$ such that DT-BRACKET holds for $(e_{sk}; \square \mid \text{send } \nu v \text{ then } e_{sk})$. That is, we need the following premises of the DT-BRACKET to type $\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{js} \vdash (e_{sk}; \square \mid \text{send } \nu v \text{ then } e_{sk}): \tau'_j \square$

$$\Pi'_j \vdash (H^x \sqsubseteq pc_{js}) \sqsubseteq pc'_{js} \tag{267}$$

$$\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc'_{js} \vdash \text{send } \nu v \text{ then } e_{sk}: \tau'_j \square \tag{268}$$

$$\Pi'_j \vdash \tau'_j \sqsubseteq \tau'_j \square \tag{269}$$

$$\Pi'_j \vdash H^x \sqsubseteq \tau'_j \square \tag{270}$$

Let $pc'_{js} = pc_{ch}$. From premises (251), (254) and given conditions on the upward closure of $H^x$ we have

$$\Pi'_j \vdash H^x \sqsubseteq pc_{ch}$$

Since we have that $\Pi'_j \vdash p'_j \sqsubseteq pc_{ch}$ (from (268)), combining with the premise (240), we have (268). Premise (269) holds because the label on the channel is bounded by the place $p'_j$ authority and premise (270) follows from $\Pi'_j \vdash pc'_{js} \sqsubseteq \tau'_j$, $\Pi'_j \vdash pc_{ch} \sqsubseteq pc'_{js}$ and DP-HALT. We thus have

$$\Pi'_j; \Gamma'_j; \Theta'_j; p'_j; pc_{js} \vdash (e_{sk}; \square \mid \text{send } \nu v \text{ then } e_{sk}): \tau'_j \square \tag{271}$$

Invoking hole substitution (Lemma 22) on (233) using the above premise and (255) we have the required proof.

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

Case $e_j = \text{recv } \nu \text{ as } x \text{ in } e$: Given $e_j = \text{recv } \nu \text{ as } x \text{ in } e$, we then have the following:

$$e_i = (W_i[send \nu v \text{ then } e_{sk}] \mid e_{i2}) \tag{272}$$

$$e'_i = (W_i[e_{sk}; \square \mid e_{i2}] \tag{273}$$

$$\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i: \tau_i \tag{274}$$

$$\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e'_i: \tau_i \tag{275}$$

$$e'_j = W_j[(e_{sk}[x \rightarrow v]; \square \mid \text{recv } \nu \text{ as } x \text{ in } e)] \tag{276}$$

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e_j: \tau_j \tag{277}$$

We have to show that

$$\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash e'_j: \tau_j$$
From (274) and DT-BRACKET (since it is not a sealed bracket, we cannot invert using DT-BRACKET-VALUES), we have the following:

\[
\Pi_i \vdash (H^x \cup pc_i) \subseteq pc'_i
\]  
(278)

\[
\Pi_i; \Gamma; \Theta; p_i; pc'_i \vdash W_i[\text{send } v \text{ then } e_{sx}] : \tau_i
\]  
(279)

\[
\Pi_i; \Gamma; \Theta; p_i; pc'_i \vdash e_{i2} : \tau_i
\]  
(280)

\[
\Pi_i \vdash H^x \leq \tau_i
\]  
(281)

Since holes can be typed under an appropriate \(pc_{is}\), invoking Lemma 19 on (279) we have

\[
\Pi_i; \Gamma; \Theta; p_i; pc'_i \vdash W_i[\overline{\text{send } v \text{ then } e_{sx}}] : \tau_i \triangleright
\]  
(282)

From DT-SENDDEL we have

\[
\Pi''_i; \Gamma''_i; \Theta'_i; p'_i; pc_{is} \vdash v : \tau
\]  
(283)

\[
\Pi''_i; \Theta; p'_i; pc_{is} \vdash v : \tau
\]  
(284)

\[
\Pi''_i \vdash pc_{is} \subseteq pc_{ch}
\]  
(285)

\[
\Pi''_i; \Gamma; \Theta; p; pc'_{is} \vdash e_{sx} : \tau'_i
\]  
(286)

\[
\tau'_i = \{\tau'_i, \tau'_i\}
\]  
(287)

\[
\Pi''_i \vdash pc_{is} \subseteq pc'_{is}
\]  
(288)

\[
\Pi''_i \vdash pc_{ch} \subseteq pc''_{is}
\]  
(289)

\[
\Pi''_i \vdash pc''_{is} \leq \tau'_i
\]  
(290)

\[
\Pi''_i \subseteq \Pi''_i
\]  
(291)

\[
\Pi''_i \vdash p'_{is} \geq pc_{is}
\]  
(292)

\[
\Pi''_i \vdash p'_{is} \geq pc_{is}
\]  
(293)

\[
\Pi''_i \vdash p'_{is} \geq pc_{ch}
\]  
(294)

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

**Case** \(W_i = E_i\): Invoking Lemma 24 on (282) we have that

\[
\Pi''_i \vdash (H^x \cup pc_{is}) \subseteq pc''_{is}
\]  
(295)

\[
\Pi''_i; \Gamma''_i; \Theta'_i; p_i; pc'_{is} \vdash \text{send } v \text{ then } e_{sx} : \tau'_i
\]  
(296)

\[
\Pi''_i \vdash H^x \leq \tau'_i
\]  
(297)

Applying R-TRANS to (296) and (295), we have

\[
\Pi''_i \vdash H^x \subseteq pc_{ch}
\]  
(298)

**Case** \(W_i \neq E_i\): Consider the premises in (279) and (278). If \(W_i\) includes \(\text{runTEE}\) and \(W_i[\overline{\text{send } v \text{ then } e_{sx}}]\) is well-typed under \(pc'_i\), then \(\exists pc''_i\) (nested TEEs aren’t allowed and for non-TEEs we have monotonic \(pc\) from Lemma ??) such that

\[
\Pi''_i \vdash H^x \subseteq pc''_i
\]  
(299)

\[
\Pi''_i; \Gamma''_i; \Theta''_i; p_i; pc''_i \vdash \text{runTEE}[E_i[\overline{\text{send } v \text{ then } e_{sx}}]] : \text{unit}\square
\]  
(300)

\[
\Pi''_i \vdash H^x \leq \text{unit}\square
\]  
(301)

Recall the premise from DT-TEE

\[
C = \{ch \mid ch \in \Theta(ch) = \text{chan}_{t=p} \text{ pc' } \tau \land \Pi''_i \vdash pc''_i \subseteq pc'\}
\]

Since \(E_i\) cannot contain any \(\text{runTEE}\) or \(\text{spawn}\), we have \(\Theta''_i | C = \Theta'_i\). This implies

\[
\Pi''_i \vdash H^x \subseteq pc_{ch}
\]  
(302)
Let us now focus on \( j \)th node. Since holes can be typed under an appropriate \( pc_{jr} \), invoking Lemma 19 on (277), we have

\[
\Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash W_j[\text{recv } \nu \text{ as } x \in e_n]: \tau_j \triangleright
\]

Inverting (303) using DT-RECEIVE we have

\[
\Pi_j'; \Gamma_j'; \Theta_j'; p_j'; pc_{jr} \vdash \nu: \text{chan}_{p_j'} - \nu' pc_{ch} \tau
\]

(304)

\[
\Pi_j' \vdash pc_{jr} \equiv pc_{ch}
\]

(305)

To show that \( e_j' \) is well-typed, we first need to find a \( pc_{jr}' \) such that DT-BRACKET holds for \((e_n[x \mapsto v] \mid \text{recv } \nu \text{ as } x \in e_n)\). That is, we need the following premises to get

\[
\Pi_j'; \Gamma_j'; \Theta_j'; p_j'; pc_{jr}' \vdash (e_n[x \mapsto v] \mid \text{recv } \nu \text{ as } x \in e_n): \tau_r.
\]

(307)

\[
\Pi_j' \vdash H^\pi \leq \tilde{\tau}_r
\]

(309)

Let \( pc_{jr}' = pc_{ch} \). From premises (298), (302) and given input conditions on the upward closure of \( H^\pi \) we have

\[
\Pi_j' \vdash H^\pi \subseteq pc_{ch}
\]

Premise (306) follows from (305). We prove (307) as shown below: Inverting (277) using DT-RECV\. Summarized as inference rule below.

\[
\Pi_j'; \Gamma_j'; \Theta_j'; p_j'; pc_{ch} \vdash ch: \text{chan}_{p_j - q} pc_{ch} \tau \quad \Pi_j'; \Gamma_j'; x: \tau; \Theta_j'; p_j'; pc_{jr}' \vdash e_n: \tau'_r
\]

To show (308), we first have to show that

\[
\Pi_j'; \Gamma_j'; \Theta_j'; p_j'; pc_{jr}' \vdash: \tau
\]

(310)

For this, we invoke the lemma that states that values sent are well-typed under places that satisfy the clearance requirement (Lemma 17) to (284). Premise (308) now follows from invoking substitution lemma on the premises of (307). We still need to show that \( \Pi_j' \vdash H^\pi \leq \tilde{\tau}_r \) holds. Consider the above premises: \( \Pi_j' \vdash pc_{ch} \subseteq pc_{jr}' \) and \( \Pi_j' \vdash pc_{jr}' \leq \tau'_r \). From these (306) and DP-HALT, the result follows. We now have all the premises to show

\[
\Pi_j'; \Gamma_j'; \Theta_j'; p_j'; pc_{jr} \vdash (e_n[x \mapsto v] \mid \text{recv } \nu \text{ as } x \in e_n): \tilde{\tau}_r
\]

(311)

Invoking hole substitution (Lemma 22) on (277) 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

\[
e_i = W_i[\overline{\text{send } \nu v \text{ then } e_{sk} \mid e}]
\]

(311)

\[
e_j = W_j[\text{recv } \nu \text{ as } x \in e_n \mid e']
\]

(312)

\[
e_i' = W_i[\overline{e_{sk} \square \mid e}]
\]

(313)

\[
e_j' = W_j[\overline{e_n[x \mapsto v] \square \mid e'}]
\]

(314)

Also given that \( e_i \) and \( e_j \) are well-typed.

\[
\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash W_i[\overline{\text{send } \nu v \text{ then } e_{sk} \mid e}]: \tau_i
\]

(315)

Invoking Lemma 19 we have that \( \overline{\text{send } \nu v \text{ then } e_{sk} \square \mid e} \) is well typed for some \( pc_s \). That is,

\[
\Pi_i' \vdash (H^\pi \cup pc_s) \subseteq pc_s'
\]

(316)

\[
\Pi_i'; \Gamma_i'; \Theta_i'; p_i'; pc_s' \vdash \overline{\text{send } \nu v \text{ then } e_{sk} \mid e}: \tilde{\tau}_s^\square
\]

(317)

\[
\Pi_i'; \Gamma_i'; \Theta_i'; p_i'; pc_s \vdash \overline{\text{send } \nu v \text{ then } e_{sk} \mid e}: \tilde{\tau}_s^\square
\]

(318)
So, from the second premise (following DT-SENDDEL) we have:

\[
\begin{align*}
\Pi'_i; \emptyset; \emptyset; p_i; pc'_s & \vdash v : \tau \\
\Pi'_i; \Gamma; \Theta; p; pc''_{is} & \vdash e_{sc}; \tau'_{s} \\
\tau'_l = \{ \dot{\tau}'_s, \dot{\tau}'_\Box \} \\
\Pi'_i; pc_{is} & \subseteq pc''_{is} \\
\Pi'_i; pc_{ch} & \subseteq pc'' \\
\Pi'_i; pc''_{is} & \leq \tau'_s \\
\Pi'_i & \subseteq \Pi'_i \\
\Pi''_i & \not\vdash p'_i \gg pc_{is} \\
\Pi''_i & \not\vdash p'_i \gg pc_{is} \\
\Pi''_i & \not\vdash p'_i \gg pc_{ch}
\end{align*}
\]

We already have \( H^e \leq \dot{\tau}'_s \). Applying PC reduction (Lemma 11 to the fourth premise, we have \( \Pi'_i; \Gamma; \Theta; p; pc''_{s} \vdash e_{sc}; \Box \dot{\tau}'_s \)). So

\[
\Pi'_i; \Gamma; \Theta; p; pc_{s} \vdash (e_{sc}; \Box \dot{\tau}'_s)
\]

Depending on whether or not \( e_j \) is bracketed, we have two more cases.

**Case** \( e_j = (W_j[recv \nu as x in e_\kappa] | e') \):

We are given that:

\[
\begin{align*}
e_j & = W_j[(recv \nu as x in e_\kappa | e')] \\
e'_j & = W_j[(e_\kappa[x \mapsto v] | e')]
\end{align*}
\]

Also given

\[
\Pi; \Gamma; \Theta; p; pc_j \vdash W_j[(recv \nu as x in e_\kappa | e')] : \tau_j
\]

Invoking Lemma 19 we have that \((recv \nu as x in e_\kappa | e')\) is well typed for some \(pc_r\). That is,

\[
\Pi''_j; \Gamma; \Theta; p; pc'_{s} \vdash (recv \nu as x in e_\kappa | e') : \dot{\tau}'_r
\]

So, from the second premise (following DT-RECEIVE) we have:

\[
\begin{align*}
\Pi'_j; \Gamma; \Theta; p'_j; pc'_{s} & \vdash ch: chan_{p_j \tau - p'_j}; pc_{ch} \tau \\
\Pi'_j; \Gamma; x; \tau; \Theta; p'_j; pc'_{r} & \vdash e_{\kappa}; \tau'_{r} \\
\tau'_r = \{ \dot{\tau}'_r, \dot{\tau}'_\Box \} \\
\Pi'_j & \vdash pc'_{r} \subseteq pc_{ch} \\
\Pi'_j & \vdash pc_{ch} \subseteq pc'' \\
\Pi'_j & \vdash pc''_{r} \leq \tau'_r \\
\Pi'_j & \not\vdash p'_j \gg pc'_{r} \\
\Pi'_j & \not\vdash p'_j \gg pc_{ch}
\end{align*}
\]

We now prove the \( recv \) part. First we have to prove that the value \( v \) is well-typed under the new context. From premise (315), 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 (315) using (333), it then follows that

\[
\Pi'_j; \emptyset; \emptyset; p'_j; pc''_{r} \vdash v : \tau
\]

Weakening channel environment for values (Lemma 12) and variable context in the above judgment, we have:

\[
\Pi'_j; \Gamma; \Theta; p'_j; pc''_{r} \vdash v : \tau
\]

From variable substitution lemma (Lemma 14) we have

\[
\Pi'_j; \Gamma; \Theta; p'_j; pc''_{r} \vdash e_{\kappa[x \mapsto v]} : \tau'_r
\]
Thus we have

\[ \Pi_j; \Gamma_j; \Theta_j; p_j; pc_r \vdash (e_k[x \mapsto v]; e') \vdash_e^* \]

Invoking hole substitution (Lemma 22), we thus have

\[ \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash W_i[(e_{sa}; e) \vdash_e \tau_i] \]

and

\[ \Pi_j; \Gamma_j; \Theta_j; p_j; pc_j \vdash W_j[(e_j [x \mapsto v]; \square) \vdash_e \tau_j] \]

**Case** \( e_j = W_j[\text{recv } \nu \text{ as } x \text{ in } e_n] \):

\[
e_j = W_j[\text{recv } \nu \text{ as } x \text{ in } e_n]
\]

(335)

\[
e_j' = W_j[(e_j [x \mapsto v]; \square) \vdash_e \tau_j]
\]

(336)

The proof is similar to the case \( e_j = \text{recv } \nu \text{ as } v \text{ in } e_k \) in the proof of BD-PAR-STEP-L.

**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

\[ W_i([() | \text{send } \nu \text{ v then } e_{sa}]) \text{ is well-typed.} \]

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

\[ \Pi_{init}; \Gamma_k; \Theta_k; p_k; pc_k \vdash e_k \vdash_e \tau_k \]

where \( \tau_j = \ell \) says bool and \( x : H \) says \( * \in \Gamma_i \) for some \( H \), and for all \( k \)

Processes do not downgrade \( H \):

\[ \forall k \in \{1 \ldots m\}, \forall \ell', \Pi_{init} \vdash H \sqsubseteq \ell' \iff \Pi'_k \vdash H \sqsubseteq \ell' \]

(337)

The attacker has limited authority:

\[ \Pi_{init} \vdash H \notin \ell \]

then for all \( v_z, z \in \{1, 2\} \) such that

\[ \langle p_1, e_1 \rangle \| \cdots \| \langle p_1, e_1[ x \mapsto v_z] \rangle \| \cdots \| \langle p_m, e_m \rangle \]

steps to \( \langle p_1, e'_1 \rangle \| \cdots \| \langle p_1, e'_{i_2} \rangle \| \cdots \| \langle p_j, e'_{j_z} \rangle \| \cdots \| \langle p_m, e'_{n2} \rangle \)

we have \( \hat{v}_{j_1} = \hat{v}_{j_2} \).

**Proof.** Given that

\[ \langle p_1, e_1 \rangle \| \cdots \| \langle p_1, e_1[ x \mapsto v_z] \rangle \| \cdots \| \langle p_m, e_m \rangle \| \cdots \| \langle p_m, e'_{m} \rangle \| \cdots \| \langle p_m, e'_{n2} \rangle \]

Also given that

\[ \Pi_i; \Gamma_i, x : H^* \text{ says } *; \Theta_i; p_i; pc_i \vdash e_i \vdash_e \tau_i \]

From DT-BRACKET-VALUES, we have that \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash (v_1 | v_2) : H^* \text{ says } * \). Invoking substitution lemma (Lemma 14) we have that \( \Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash e_i[ x \mapsto (v_1 | v_2)] \vdash_e \tau_i \). From the type preservation (Lemma 25) we have that for all \( k \in \{1 \ldots n\} \)

\[ \Pi_k; \Gamma_k; \Theta_k; p_k; pc_k \vdash e'_k \vdash_e \tau_k \] such that \( \Theta'_k \supseteq \Theta_k \). We prove for each case separately.

From the completeness property (Lemma 5), we have that

\[ \langle p_1, e_1 \rangle \| \cdots \| \langle p_1, e_1[ x \mapsto (v_1 | v_2)] \rangle \| \cdots \| \langle p_m, e_m \rangle \| \cdots \| \langle p_1, e'_{12} \rangle \| \cdots \| \langle p_j, \hat{v}_{j_1} \rangle \| \cdots \| \langle p_m, e'_m \rangle \| \cdots \| \langle p_m, e'_{n2} \rangle \]

and from the soundness property (Lemma 2), we have that \( [v'_z]_z = [v'_z]_z \) for \( z = \{1, 2\} \).

From the type preservation lemma, we have that \( \Pi_j; \Gamma_j; \Theta'_j; p_j; pc_j \vdash v'_j : \ell \text{ says bool.} \) We have to prove that

\[ [v'_j]_1 = [v'_j]_2 \]

Let us assume that \( \hat{v}_j \) is a bracket value. Then by DT-BRACKET-VALUES, we have the following:

\[ \Pi_j; \Gamma_j; \Theta'_j; p_j; pc \vdash [v'_j]_1 : \tau_j \]

(339)

\[ \Pi_j; \Gamma_j; \Theta'_j; p_j; pc \vdash [v'_j]_2 : \tau_j \]

(340)

\[ \Pi_j \vdash H^* \leq \tau_j \]

(341)
Fig. 25: Erasure function for sealed values and TEEs

From (341), we require that $\Pi_j \vdash H^\tau \subseteq \ell$ (rule DP-LBL). But from condition (338) we are already given that $\Pi_j \not\vdash H^- \wedge H^- \subseteq \ell$. Thus $\Pi_j; \Gamma_j; \Theta_j; p_j; p_c \vdash \hat{\nu}_j$: $\tau_j$ cannot be well-typed by DT-BRACKET-VALUES and so $\hat{\nu}_j$ itself isn’t a bracket term.

Note that $\hat{\nu}_j$ can only be a where term. We can prove this by inducting on the structure of the value. The only interesting case is $\eta_\ell \nu''$. In this case, we can easily prove that $\nu''$ cannot be a bracket term because sumtypes ($\text{bool} = \text{unit} + \text{unit}$) cannot protect any principal.

Without loss of generality, let $\hat{\nu}_j = w$ where $\langle \rho \rightarrow q \rangle$. 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 $\hat{\nu}_j$ is not a bracket term.

j) **Induction Hypothesis:** Let $\hat{\nu}_j = w$ where $n^{-1}\langle p_{n-1} \Rightarrow q_{n-1} \rangle$ where $\langle p_n \Rightarrow q_n \rangle$. For $k = \{0 \ldots n-1\}$, $w$ where $k(p_k \Rightarrow q_k)$ is not a bracket term.

k) **Induction Step:** For the induction step, we need to prove that $\hat{\nu}_j = w$ where $\langle \rho \rightarrow q \rangle$ where $n^{-1}\langle p_{n-1} \Rightarrow q_{n-1} \rangle$ where $\langle p_n \Rightarrow q_n \rangle$ is not a bracket term. From the induction hypothesis, we already have that $w$ where $\langle \rho \rightarrow q \rangle$ where $k(p_k \Rightarrow q_k)$ where $\langle p_n \Rightarrow q_n \rangle$ is not a bracket term for $k = \{1 \ldots n\}$. Thus it remains to prove that $w$ where $\langle \rho \rightarrow q \rangle$ is not a bracket term.

**Case $\pi \Rightarrow$:** From condition (338), we have $\Pi_j \not\vdash H^- \subseteq \ell^- \wedge H^\ell$ and so we have that $\Pi_j \not\vdash H^- \subseteq \ell^- \wedge H^\ell$. Running an argument similar to the base case, we have that $w$ cannot be a bracket term (as $\Pi_j \not\vdash p_c \leq \tau_j$).

**Case $\pi \Leftarrow$:** Similar to above the above case, using condition (338), we have $\Pi_j \not\vdash H^- \subseteq \ell^-$. Again $w$ cannot be a bracket term.

This completes the proof that $\hat{\nu}_j$ isn’t a bracket term and so $[\hat{\nu}_j]_1 = [\hat{\nu}_j]_2$.

We elaborate the erasure/observation function in the below table.

| $\nu(x, \Pi, A)$ | $= \ x$ |
| $\nu(\eta_\ell \ e', \Pi, A)$ | $= \ \eta_\ell \ \nu(e', \Pi, A)$ |
| $\nu(\eta_\ell \ e', \Pi, A)$ | $= \ \eta_\ell \ \nu(e', \Pi, A)$ |
| $\nu(\lambda x: \tau)[p, \Theta, \mathcal{P}, \Pi_\lambda]. e', \Pi, A)$ | $= \ \lambda x: \tau)[p, \Theta, \mathcal{P}, \Pi_\lambda]. \nu(e', \Pi, A)$ |
| $\nu(\text{bind} \ x = e' \ \nu''', \Pi, A)$ | $= \ \nu(e', \Pi, A) \ \nu(e''', \Pi, A)$ |
| $\nu(\text{assume} \ e' \ \nu''', \Pi, A)$ | $= \ \nu(e', \Pi, A) \ \nu(e''', \Pi, A)$ |
| $\nu(\text{runTEE} \ e', \Pi, A)$ | $= \ \nu(\text{runTEE} \ e', \Pi, A)$ |
| $\nu(\text{spawn} \ \text{ref} \ (p, \text{ch}[pc; \tau], \text{ch}[pc; \tau]). e' \ \nu''', \Pi, A)$ | $= \ \nu(\text{spawn} \ \text{ref} \ (p, \text{ch}[pc; \tau], \text{ch}[pc; \tau]). \nu(e', \Pi, A) \ \nu(e''', \Pi, A)$ |
| $\nu(\text{send} \ (e') \ \nu''', \Pi, A)$ | $= \ \nu(\text{send} \ (e') \ \nu''', \Pi, A)$ |
| $\nu(\text{recv} \ \text{as} \ x \ \nu''', \Pi, A)$ | $= \ \nu(\text{recv} \ \text{as} \ x \ \nu''', \Pi, A)$ |

Erasure functions for sealed values and TEEs are defined in Figure 25. We lift the erasure of expressions to a process as follows.

$$\nu((q, e), \Pi, A) = \langle q, \nu(e, \Pi, A) \rangle$$

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.1 (Trace Deduplication).

\( \mathcal{U}(\langle q, e^{1}\rangle, \Pi, p), \mathcal{O}(\langle q, e^{2}\rangle, \Pi, p), \mathcal{O}(\langle q, e^{3}\rangle, \Pi, p), \ldots, \mathcal{O}(\langle q, e^{n}\rangle, \Pi, p)) = \)

\[
\begin{cases}
\mathcal{O}(\langle q, e^{1}\rangle, \Pi, p), \mathcal{U}(\mathcal{O}(\langle q, e^{2}\rangle, \Pi, p), \ldots, \mathcal{O}(\langle q, e^{n}\rangle, \Pi, p)) & \text{if } \mathcal{O}(\langle q, e^{1}\rangle, \Pi, p) \neq \mathcal{O}(\langle q, e^{2}\rangle, \Pi, p) \\
\mathcal{U}(\mathcal{O}(\langle q, e^{1}\rangle, \Pi, p), \mathcal{O}(\langle q, e^{2}\rangle, \Pi, p), \ldots, \mathcal{O}(\langle q, e^{n}\rangle, \Pi, p)) & \text{if } \mathcal{O}(\langle q, e^{1}\rangle, \Pi, p) = \mathcal{O}(\langle q, e^{2}\rangle, \Pi, p)
\end{cases}
\]

Two traces are equivalent if they are equal after removing the duplicates.

Definition C.2 (Trace Equivalence). Two traces, Tr1 and Tr2, are equivalent, denoted as Tr1 \( \approx \) Tr2, 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

\[ \langle p_1, e_{1}^{1} \rangle \parallel \cdots \parallel \langle p_i, e_{i}^{k_i} \rangle \parallel \cdots \parallel \langle p_m, e_{m}^{1} \rangle \]

\[ \Rightarrow^* \]

\[ \langle p_1, e_{1}^{k_1} \rangle \parallel \cdots \parallel \langle p_i, e_{i}^{k_i} \rangle \parallel \cdots \parallel \langle p_m, e_{m}^{k_m} \rangle \]

then, schedule, \( S = (P_i)_{i=1}^{k} \) 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.

\[ \langle p, \text{bind } x = v \text{ in send } ch \ x \text{ then } e_{ss} \rangle \parallel \langle q, \text{recv } ch \text{ as } y \text{ in } y \rangle \]

\[ \Rightarrow \]

\[ \langle p, \text{send } ch \ v \text{ then } e_{ss} \rangle \parallel \langle q, \text{recv } ch \text{ as } y \text{ in } y \rangle \]

\[ \Rightarrow \]

\[ \langle p, () \rangle \parallel \langle q, v \rangle \]

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.

\[ S_1 = \langle p_1, e_{1}^{1} \rangle \parallel \cdots \parallel \langle p_i, e_{i}^{k_i} \rangle \parallel \cdots \parallel \langle p_m, e_{m}^{1} \rangle \Rightarrow^* \langle p_1, e_{1}^{k_1} \rangle \parallel \cdots \parallel \langle p_i, e_{i}^{k_i} \rangle \parallel \cdots \parallel \langle p_m, e_{m}^{k_m} \rangle \]

\[ S_2 = \langle p_1, e_{1}^{1} \rangle \parallel \cdots \parallel \langle p_i, e_{i}^{k_i} \rangle \parallel \cdots \parallel \langle p_m, e_{m}^{1} \rangle \Rightarrow^* \langle p_1, e_{1}^{k_1} \rangle \parallel \cdots \parallel \langle p_i, e_{i}^{k_i} \rangle \parallel \cdots \parallel \langle p_m, e_{m}^{k_m} \rangle \]

such that \( [S_1]_p = [S_2]_p \), then \( \langle p_i, e_{i}^{k_i} \rangle = \langle p_i, e_{i}^{k_i} \rangle \)

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.

\[
\begin{array}{c|c}
|S|_p & |S|_p \\
\hline
S_1 = \{p, \{p, q\}, \{r\}, \{p\}, \{p, r\} & \{p\}, \{p, q\}, \{p, r\} \\
S_2 = \{p\}, \{p, q\}, \{p\}, \{r\}, \{p\}, \{p, r\} & \{p\}, \{p, q\}, \{p, r\} \\
S_3 = \{p\}, \{p\}, \{p, q\}, \{r\}, \{p\}, \{p, r\} & \{p\}, \{p, q\}, \{p, r\}
\end{array}
\]

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). □

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 \(S_l\) and \(S_r\) be the left and right executions shown below.

\(S_l = \langle p_1, e_1 \rangle \mid \cdots \mid \langle p_k, e_k \mid x \mapsto v_l⟩ \mid \cdots \mid \langle p_m, e_m \rangle \Rightarrow \ast \langle p_1, e'_1 \rangle \mid \cdots \mid \langle p_k, e'_k \rangle \mid \cdots \mid \langle p_m, e'_m \rangle\)

\(S_r = \langle p_1, e_1 \rangle \mid \cdots \mid \langle p_k, e_k \mid x \mapsto v_r⟩ \mid \cdots \mid \langle p_m, e_m \rangle \Rightarrow \ast \langle p_1, e''_1 \rangle \mid \cdots \mid \langle p_k, e''_k \rangle \mid \cdots \mid \langle p_m, e''_m \rangle\)

Let \(S_{(1)}\) be the corresponding bracketed execution shown below.

\(S_{(1)} = \langle p_1, e_1 \rangle \mid \cdots \mid \langle p_k, e_k \mid x \mapsto (v_l \mid v_r)⟩ \mid \cdots \mid \langle p_m, e_m \rangle \Rightarrow \ast \langle p_1, e''_1 \rangle \mid \cdots \mid \langle p_k, e''_k \rangle \mid \cdots \mid \langle p_m, e''_m \rangle\)

If \(P\) is the set of processes in \(S_{(1)}\), then \(\forall p \in P, |S_{(1)}|_p \leq |S_l|_p\) when \(\leq\) is a prefix where \(|S_{(1)}|_1\) 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 \(S_{(1)}\) which is same as the number of the evaluation steps of the bracketed execution.

**Base Case:** Given \(|S_{(1)}|_1 = P_1\). Hence

\(|S_{(1)}|_1 = P_1\) if \(p \in P_1\) otherwise

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 \(|S_l|_p = P_1\) if \(p \in P_1\) else \(\emptyset\). Thus,

\(|S_{(1)}|_p \leq |S_l|_p\)

This proves the base case.

**Inductive Case:** Let \(\text{len}(S_{(1)}) = k + 1\). Given that

\(\forall p, |S_{(1)}|_{[1 : k + 1]}_p \leq |S_l|_p\)

Let \(|S_{(1)}|_{[k + 1]}_1 = P_{k + 1}\). Hence

\(|S_{(1)}|_{[k + 1]} = |S_{(1)}|_{[1 : k]}_p, \text{len}(S_{(1)}|_{[1 : k]}_p, P_{k + 1})\)

\(|S_{(1)}|_p \leq |S_l|_p\)

Let \(\text{len}(S_{(1)}|_{[1 : k]}_p, P_{k + 1}) = k'\). This implies that the bracketed execution has taken \(k'\) number of steps for process \(p\). From induction hypothesis, we have that \(|S_{(1)}|_{[1 : k]}_p \leq |S_l|_p\). That implies, \(|S_{(1)}|_{[1 : k]}_p = |S_l|_p\). 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 \(|P_{k + 1}| = 2\), then \(\exists q \text{ such that } q \neq p\) 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 \(|S_{(1)}|_{[1 : k + 1]}_p = |S_l|_p, |S_{(1)}|_{[1 : k + 1]}_p \leq |S_l|_p\).

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 \(\Pi_{init}; \sqsubseteq \Gamma_k; \Theta_k; p_k; p_c \vdash e_k : \tau_k\) and \(x : H^+\) says \(\vdash \in \Gamma_i\) for some \(H\), and

Processes do not downgrade \(H^+\):

(342)

\(\forall k \in \{1 \ldots m\}, \forall \ell. \Pi_{init} \vdash H \subseteq \ell \iff \Pi_{init} \vdash H \subseteq \ell\)

The attacker has limited authority:

(343)

\(\Pi_{init} \not\vdash p_j \geq H^+\)

\(H^+\)
For all $v, z \in \{1, 2\}$ such that $\Pi_i; \Gamma_i; \Theta_i; p_i; pc_i \vdash v_z : H \rightarrow \tau$, if

$$S_t = \{p_1, e_1\} \parallel \cdots \parallel \{p_i, e_i[x \mapsto v_i]\} \parallel \cdots \parallel \{p_j, e_j\} \parallel \cdots \parallel \{p_m, e_m\}$$

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,

$$O((p_j, e_{j1}), \hat{\Pi}_{D(j)}, p_j^-), \ldots, O((p_j, e_{j1}, \hat{\Pi}_{D(j)}, p^-)$$

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,

$$\{p_1, e_1\} \parallel \cdots \parallel \{p_i, e_i[x \mapsto v_i]\} \parallel \cdots \parallel \{p_m, e_m\} = \{p_1, e_1\} \parallel \cdots \parallel \{p_i, e_i[x \mapsto v_i]\} \parallel \cdots \parallel \{p_m, e_m\}$$

From the completeness property (Lemma 5), we have that

$$S_t(1) = \{p_1, e_1\} \parallel \cdots \parallel \{p_i, e_i[x \mapsto (v_i | v_r)]\} \parallel \cdots \parallel \{p_m, e_m\} \Rightarrow^* \{p_1, e_1^s\} \parallel \cdots \parallel \{p_j, e_j^s\} \parallel \cdots \parallel \{p_m, e_m^s\}$$

and from the soundness property (Lemma 2), we have that $[v_j^s]_1 = v_{j1}$ and $[v_j^s]_2 = v_{j2}$. Now, consider any intermediate step: $(p_j, e_j^s)$. From type preservation (Lemma 25), we have $\Pi_i; \Gamma_i; \Theta_i; p_i; pc_j \vdash e_j^s: \tau$. We have to prove that:

$$O((p_j, [e_j^s], \hat{\Pi}_{D(j)}, p_j^-) = O((p_j, [e_j^s], \hat{\Pi}_{D(j)}, p_j^-)$$

It is clear that $e_j^s$ itself is not a bracket expression as it would invalidate the clearance requirement if it were well-typed as per DT-BRACKET. That is, as per DT-BRACKET, we have $\Pi_j \vdash pc \subseteq H^\rightarrow$ for some $pc'$. Then, consider any intermediate step: $(p_j, e_j^s)$. From type preservation (Lemma 25), we have $\Pi_i; \Gamma_i; \Theta_i; p_i; pc_j \vdash e_j^s: \tau$. We have to prove that:

$$O((p_j, [e_j^s], \hat{\Pi}_{D(j)}, p_j^-) \neq O((p_j, [e_j^s], \hat{\Pi}_{D(j)}, p_j^-)$$

Then there should be some subterm $e$ of $e_j^s$ such that

$$O((p_j, [e], \hat{\Pi}_{D(j)}, p_j^-) \neq O((p_j, [e], \hat{\Pi}_{D(j)}, p_j^-)$$

We have 2 cases: either $e$ is some bracketed value $(\hat{v}_1 | \hat{v}_2)$ that is well-typed by DT-BRACKET-VALUES or $e$ is some well-typed TEE$(e_1 | e_2)$.

**Case 1:** Let $(\hat{v}_1 | \hat{v}_2)$ be a well-typed bracket term. That is, $\Pi''_j; \Gamma''; \Theta_j''; p_j; pc_j'' \vdash (\hat{v}_1 | \hat{v}_2): \tau$. Then from DT-BRACKET-VALUES, we require that $\Pi''_j \vdash H^\rightarrow \leq \tau$. This implies that for $k \in \{1, 2\}$, $\hat{v}_k \in \{(), (v', v''), p \gg q\}, (v_v', v_v'; c_r, \text{runTEE} \hat{\nu})$ as other values cannot be protected. Note that $(v_1 \in (v_2 | v_3 \in (v_4))$ is not well-typed if $v_2 \neq v_4$.

It is clear that for runTEE $\hat{\nu}$ to be well-typed $\hat{\nu}$ is $()$. Also, the erasure function for $((), (p \gg q)$ returns same values. If $v_k = \tau_{v_v'} v_v'$, then, $\hat{v}_k = \tau_{v_v'} v_v'$, then we require that $\Pi_j'' \vdash H^\rightarrow \leq \ell$. Since all delegations in $\Pi''_j$ belong to $\hat{\Pi}_{D(j)}$ and $\hat{\Pi}_{D(j)}$, we have that $\tau_{\hat{\nu}_{v_v'} v_v'}(\hat{\Pi}_{D(j), \tau}) = \tau_{\hat{\nu}_{v_v'} v_v'}(\hat{\Pi}_{D(j), \tau}) = \tau_{\hat{\nu}_{v_v'} v_v'}$. 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 TEE$(e_1 | e_2)$. Then from DT-BRACKET, we require that $\Pi_j'' \vdash pc'' \gg H^\rightarrow$ and $\Pi_j''; \Theta_j''; t; pc_j'' \vdash e_i: \tau$ 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, clearance (Lemma 7), we have that $\Pi_j'' \vdash t^- \gg H^-$. Hence, they are equal after erasure.
Repeatedly applying type preservation will thus give that
\[
\mathcal{O}(\langle p_j, [e_j]_1 \rangle, \hat{\Pi}_{\mathcal{D}(j)}, p_j^-) \ldots \mathcal{O}(\langle p_j, [v_j']_1 \rangle, \hat{\Pi}_{\mathcal{D}(j)}, p_j^-) 
\approx \mathcal{O}(\langle p_j, [e_j]_2 \rangle, \hat{\Pi}_{\mathcal{D}(j)}, p_j^-) \ldots \mathcal{O}(\langle p_j, [v_j']_2 \rangle, \hat{\Pi}_{\mathcal{D}(j)}, p_j^-)
\]
(345)

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 \( S \) and bracketed execution projected on the left side with schedule, \( S_{(1)} \). Further, we assume that the length of the \( S \) is the minimum number of steps required to reduce \( [e_j]_1 \) 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 \( S_{(1)} \) commutes with \( S \) for the first \( s \) steps. Lemma 29 allows us to reschedule \( S \) to \( S_{(1)} \) such that \( [S_{(1)}[1 : s]]_1 = S_{(1)}[1 : s'] \) (upto stuttering). The schedule can be completed such that it satisfies the property
\[
\forall p, [S_i]_p = [S_{(1)}]_p
\]
Note that such a construction exists but we elide the actual details. Since \( S \) and \( S_{(1)} \) are commuting, their traces for node \( p_j \) are same (Lemma 28). Also note that trace of node \( p_j \) after \( s \) steps in \( S_{(1)} \) is simply a chain of \( \langle p_j, v_j^\ell \rangle \) and deduplication removes them completely. So we only consider the trace generated by the schedule \( S_{(1)}[1 : s] \). However, this is equal to the \( S_{(1)} \). 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 \( S_{(1)} \) (and hence \( S \) and \( S_{(1)} \) are equal.

Similarly, we can prove that trace of node \( p_j \) generated by the second execution \( S \), and bracketed execution \( S_{(1)} \) is same. This implies that we can now use traces of bracketed execution to reason about the trace equivalence. From (345), 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
\[
\Pi; pc; \ell \vdash \Box q; \ell \vdash \mathcal{H}(q)
\]
From (346) and \( \text{DEL} \), we have that
\[
\mathcal{H}; c; pc; \ell \vdash p \gg q
\]
From (347) and [ Weaken], we get that \( \mathcal{H}; c; pc; \ell \vdash \mathcal{H}(q); \ell \vdash p \gg q \). From the (348), (349) and \( \text{R-Lift} \) we thus have \( \mathcal{H}; c; pc; \ell \vdash p \gg q \).

**Case R-Static:** Since \( L \vdash p \gg q \), we have that
\[
\mathcal{H}; c; c \vdash \bot \vdash \mathcal{H}; c; \ell \vdash p \gg q
\]
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. □