**Automatic Enforcement of Expressive Security Policies using Enclaves**

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

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Citable link</td>
<td><a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:30168300">http://nrs.harvard.edu/urn-3:HUL.InstRepos:30168300</a></td>
</tr>
<tr>
<td>Terms of Use</td>
<td>This article was downloaded from Harvard University’s DASH repository, and is made available under the terms and conditions applicable to Other Posted Material, as set forth at <a href="http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA">http://nrs.harvard.edu/urn-3:HUL.InstRepos:dash.current.terms-of-use#LAA</a></td>
</tr>
</tbody>
</table>
Automatic Enforcement of Expressive Security Policies using Enclaves

Anitha Gollamudi
and
Stephen Chong

TR-02-16

Computer Science Group
Harvard University
Cambridge, Massachusetts
Automatic Enforcement of Expressive Security Policies using Enclaves

Anitha Gollamudi  Stephen Chong
Harvard University, Cambridge, MA, USA
agollamudi@g.harvard.edu  chong@seas.harvard.edu

Abstract
Hardware-based enclave protection mechanisms, such as Intel’s SGX, ARM’s TrustZone, and Apple’s Secure Enclave, can protect code and data from powerful low-level attackers. In this work, we use enclaves to enforce strong application-specific information security policies.

We present IMPE, a novel calculus that captures the essence of SGX-like enclave mechanisms, and show that a security-type system for IMPE can enforce expressive confidentiality policies (including erasure policies and delimited release policies) against powerful low-level attackers, including attackers that can arbitrarily corrupt non-enclave code, and, under some circumstances, corrupt enclave code.

We present a translation from an expressive security-typed calculus (that is not aware of enclaves) to IMPE. The translation automatically places code and data into enclaves to enforce the security policies of the source program.

Categories and Subject Descriptors D.3.3 [Programming Languages]: Language Constructs and Features; D.4.6 [Operating Systems]: Security and Protection—Information flow controls

Keywords Enclave programs, information erasure, declassification, security-type system, information-flow control, language-based security.

1. Introduction
Language-based techniques for security can enforce expressive information security policies for applications. Enforceable policies include ensuring that application-level adversaries learn nothing about confidential information [29, 38], that some clearly specified confidential information may be released under controlled circumstances [31], and that sensitive information is correctly removed from the system at appropriate times [7, 10]. However, these language-based guarantees may fail to hold in the presence of low-level attackers, such as attackers that observe execution at the level of operating-system or hardware abstractions, or attackers that can inject arbitrary code into a process.

Recent hardware-based enclave protection mechanisms (including Intel’s SGX [24], ARM’s TrustZone [4], and Apple’s Secure Enclave [2]) can protect code and data from low-level attacks, including compromised kernels. These new mechanisms present an opportunity to extend strong application-specific information security guarantees to hold against low-level attackers.

We take advantage of this opportunity: we present a language model that captures the essence of enclave protection mechanisms, and give a security-type system for this language that enforces strong non-interference-based information security guarantees [12, 18], including delimited release [30] and information erasure [9]. Moreover, we provide a translation from a non-enclave source language that automatically infers which code and data to place in enclaves in order to enforce expressive security policies.

As an example of application-specific information security requirements, consider code that authenticates a user. The user provides a guess that is checked against the actual password. If the guess matches the password, the user is authenticated and the computation continues. After authentication, the guess is no longer needed, and the subsequent computation should in no way depend on the guess. This information security requirement can be expressed as an erasure policy [9] that requires restrictions on the use of sensitive information (i.e., the user’s guess) after certain conditions are satisfied (i.e., the user is successfully authenticated). Language-based techniques can ensure that these restrictions are respected by the subsequent computation (e.g., [7, 23]).

However, these techniques typically enforce security against a language-level attacker that passively observes the program’s output or perhaps provides code that is subject to similar enforcement mechanisms as the program itself (e.g., [3, 23]). The desired security guarantees may fail to hold in settings where an attacker has privileged access to a machine (such as in cloud services or on mobile devices) or attacker is able to exploit vulnerabilities to observe more data than anticipated (such as in the Heartbleed attack) or inject arbitrary code into the program’s process (such as in buffer overrun attacks). In these cases, an attacker that compromises the system sometime after the user has authenticated may be able to learn the user’s password. For example, even though the program may not in any way use...
the user’s guess in the subsequent computation, the bits representing the guess may still be present in physical or virtual memory, and accessible to a low-level attacker [20][21].

Enclave protection mechanisms can secure code and data against powerful attackers, including malicious code within the same process or a malicious operating system. Intel’s SGX extends the x86 instruction set with additional instructions that allow a contiguous region of memory within a process’s address space to be established as an enclave, and subsequently uses hardware-enforced access control to ensure that code outside of an enclave is unable to access data within an enclave. Moreover, execution may enter an enclave only via specified entry points. Memory within an enclave is encrypted before being paged out.

But leveraging enclaves to enforce application-specific information security guarantees is hard. Enclave mechanisms place the onus on the programmer to secure an application to carefully isolate the dependencies requires non-trivial effort [32, 35]. Indeed, hardening an application to carefully isolate the application from the non-critical and/or untrusted parts of the application. Enclave protection mechanisms can secure code and data within an enclave. Moreover, execution may enter an enclave only via specified entry points. Memory within an enclave is encrypted before being paged out.

In this paper we consider the automatic enforcement of application-specific information security policies using enclaves. We make several contributions.

1. We present IMPE, a novel calculus that captures the essence of SGX-like enclave mechanisms (Section 2).
2. We show that a security-type system for IMPE can enforce expressive confidentiality policies (including erasure policies and delimited release policies) against several attackers, including attackers that can arbitrarily corrupt non-enclave code, and, under certain circumstances, corrupt enclave code (Sections 3 and 4).
3. We present a translation from a non-enclave source language to IMPE (Sections 5 and 6). The programmer can focus on the correct handling of information in the source language, and the translation will automatically infer appropriate placement of code and data into enclaves to ensure security guarantees against powerful low-level attackers. The translation can be configured to optimize various criteria, including reducing the size of the trusted computing base, reducing the runtime performance impact of using enclave mechanisms, or removing erased data as soon as possible.

In addition, we validate the translation and the expressiveness of IMPE by implementing several simple models of applications with application-specific security guarantees (Section 8).

2. IMPE: A Calculus for Enclaves

We present IMPE, an imperative higher-order calculus that captures the key features of enclaves and moreover supports the specification of information security policies, including policies for information erasure.

2.1 Security Levels and Policies

We use a set of security levels \( L = \{L, H, \top\} \) to express confidentiality restrictions on information. Security level \( L \) (“low security”) is for public information that anyone, including an attacker, is permitted to learn. Security level \( H \) (“high security”) is for confidential information that only trusted entities are permitted to learn. Security level \( \top \) is for information so confidential that no-one is permitted to learn it. Ideally, the system never contains information with security level \( \top \).

Let partial order \( \sqsubseteq \) be the smallest reflexive and transitive relation such that \( L \sqsubseteq H \) and \( H \sqsubseteq \top \). Intuitively, if \( \ell_1 \sqsubseteq \ell_2 \), then information with security level \( \ell_2 \) is at least as confidential as information with security level \( \ell_1 \). Security levels ordered by \( \sqsubseteq \) form a lattice.

The security level to enforce on information may change over time. In this paper, we focus on information erasure: the requirement that when a specific condition is met, information needs to become more confidential.

Security policies describe how the security level of information must change over time. A security level policy \( \ell \) simply means that information must be handled with security level \( \ell \) at all times. An erasure policy \( \ell_1 \xrightarrow{cnd \downarrow} \ell_2 \) means that initially information can be handled according to security level \( \ell_1 \). However, when condition \( cnd \) is met, the information must be handled according to security level \( \ell_2 \), where \( \ell_1 \sqsubseteq \ell_2 \). Conditions are used to express when information must be “erased” or made more restrictive. In general, conditions for erasure can be arbitrary state predicates [9]. However, we encode conditions using mutable memory locations: a condition \( cnd \) is represented by a single memory location, and the condition is regarded as satisfied exactly when the location contains a non-zero value. The program is responsible for setting the condition location to a non-zero value to correctly reflect the intended meaning of the condition. Once set (i.e., assigned a non-zero value), we do not allow a condition to be unset. This approach is sufficiently expressive and simplifies specification and reasoning about erasure policies [7].

We write \( P \) to denote the set of policies, and use metavariables \( p, q \) to range over policies. We refer to any information labeled with a policy more restrictive than \( L \) as confidential information.

Consider a program that authenticates a password. Let password be a memory location that stores password input from a user. Once authentication succeeds, it is desirable to erase password entirely from the memory. If end is a condition that indicates whether the authentication session has ended, a suitable policy for password can be \( L \xrightarrow{end \downarrow} \top \).

The policy says that the confidentiality level of password is initially \( L \) and once end is set, it must be \( \top \).
$e ::= n \mid x \mid e_1 \oplus e_2 \mid l \mid \ast e \mid \text{isunset} (\text{cnd}) \mid \lambda \mu . c$

$v ::= \lambda \mu . c \mid n \mid l$

c ::= \text{skip} \mid x := e \mid x := \text{declassify} (e) \mid e_1 \leftarrow e_2$

\begin{align*}
| \text{output } e \text{ to } \ell & \mid \text{call}(e) \mid \text{set}(\text{cnd}) \mid \text{enclave}(i, c) \\
| \text{kill}(i) \mid c_1; \ldots; c_n & \mid \text{if } e \text{ then } c_1 \text{ else } c_2 \mid \text{while } e \text{ do } c
\end{align*}

$l \in \text{Loc} \mid \text{cnd} \in \text{Cond} \mid \text{Cond} \subset \text{Loc}$

$x \in \text{Vars} \mid i, n \in \mathbb{N}$

$\mu \in \text{Mode} = \{N, E_1, E_2, \ldots \}$

---

**Figure 1.** IMP Syntax

### 2.2 Syntax

IMP is a simple imperative language. However, it includes first-class locations and functions, output commands, and models enclaves. An enclave consists of code and memory locations. Memory locations within an enclave can be accessed only by that enclave’s code. Control can be transferred to code inside an enclave only through a predefined set of entry points. Thus, data stored inside an enclave’s memory locations is protected from non-enclave code (and also from code in other enclaves). In IMP, enclaves provide a simple yet expressive model of architectural features—such as Intel’s SGX [24]—that can provide strong isolation guarantees for code and data from other code within the same process or machine.

We allow an arbitrary number of enclaves, indexed with natural numbers. We use modes to indicate which enclave code or data exists in, or whether it is outside of any enclave. Specifically, we use metavariable $\mu$ to range over the set $\text{Mode} = \{N, E_1, E_2, \ldots \}$, where $E_i$ indicates the $i$th enclave and $N$ indicates non-enclave (or “normal”) mode.

Figure 1 shows the syntax of IMP. Expressions $e$ include integers $n$, variables $x$, and memory locations $l$. All variables have global scope. Variables are analogous to registers: they are mutable locations, but are not first-class values. By contrast, memory locations are first class, and can be passed as values. Conditions $\text{Cond}$ are a subset of the memory locations and $\text{cnd}$ ranges over conditions. We write $\text{Loc}$ for the set of memory locations.

Operator $\oplus$ ranges over arbitrary (total) binary operations over integers. Dereference $\ast e$ evaluates $e$ to a memory location and evaluates to the contents of that location.

Expression $\text{isunset}(\text{cnd})$ tests whether condition $\text{cnd}$ has been set, and evaluates to 1 if it is not set, 0 otherwise. Although this expression is semantically equivalent to $\ast \text{cnd} \neq 0$, our type system gains precision through the use of $\text{isunset}(\text{cnd})$.

Expression $\lambda \mu . c$ is a first-class function. It can be thought of as a code pointer to command $c$. Arguments to the function are given via variables and memory locations, as are any values returned by the function. Annotation $\mu$ indicates the mode in which the function is defined. It can be thought of as indicating whether the code pointer is to an enclave or non-enclave region of memory. The annotation is used to restrict how functions can be invoked, to ensure that non-enclave code cannot enter an enclave by invoking a function that resides in the enclave.

Values $v$ in IMP include integers, memory locations (including conditions), and first-class functions.

Commands in IMP include standard imperative commands (skip, $x := e$, if $e$ then $c_1$ else $c_2$, and while $e$ do $c$). We assume sequences $c_1; \ldots; c_n$ are flattened (i.e., that none of $c_1; \ldots; c_n$ are sequence commands), and for convenience assume that all sub-commands are sequences (possibly of length 1). Indirect assignment $e_1 \leftarrow e_2$ evaluates $e_1$ to a memory location, and updates the contents of that location with the result of $e_2$. We further require that $c_1$ does not evaluate to a condition. Command $\text{set}(\text{cnd})$ updates the contents of $\text{cnd}$ to 1. Conditions can be updated only with a set command.

Command output $e$ to $\ell$ evaluates $e$ to a value and outputs it to channel $\ell$. Output commands model observations by trusted and untrusted entities. We restrict $\ell$ to be either $L$ or $H$. Intuitively, an output to channel $L$ may be observed by an untrusted entity, such as an attacker, whereas output to channel $H$ may be observed only by trusted entities.

Command $x := \text{declassify}(e)$ is semantically equivalent to assignment $x := e$, but indicates a declassification, which is relevant for both our semantic security conditions (Section 3.2) and type system (Section 4). To simplify our semantic security condition, we require that expression $e$ does not contain any variables (although it may contain memory locations). Command $\text{call}(e)$ evaluates $e$ to a function, and invokes the function.

Command $\text{enclave}(i, c)$ defines an entry point for the enclave $E_i$. That is, command $c$ is code that resides inside enclave $E_i$, and non-enclave code is permitted to execute $c$. We require that $c$ does not contain any subcommands of the form $\text{enclave}(i', c')$, i.e., enclave commands cannot be nested, regardless of whether for the same enclave or a different enclave. Commands not lexically nested in an enclave($i, \ldots$) are non-enclave code.

We allow an enclave to have multiple entry points. That is, a program may contain multiple commands of the form $\text{enclave}(i, c)$ with the same enclave identifier $i$.

Command $\text{kill}(i)$ tears down enclave $E_i$. Once killed, an enclave cannot be used: its memory locations can not be accessed, nor can its code be executed.

### 2.3 Operational Semantics

A configuration $(c, r, m, K)$ describes the current state of the system. Command $c$ is the rest of the program to execute. Register file $r$ maps variables to values, and memory $m$ maps locations to values. Kill set $K$ is the set of enclaves that have been killed so far in the execution.
Figure 2 presents the inference rules for expression evaluation. The rules are straightforward except for Deref. Integers, locations, and functions are already values.

Rule Deref evaluates expression \( e \) to a memory location \( l \) and reads the contents of \( l \). The premise \( \delta(l) \in \{N,\mu\} \setminus K \) states that in normal mode (i.e., \( \mu = N \)), only normal locations can be read; in enclave mode \( E_i \) (i.e., \( \mu = E_i \)), both normal and enclave \( E_i \) locations may be read (i.e., \( \delta(l) \in \{N, E_i\} \)). Locations from a different enclave cannot be read, and if an enclave has been killed (\( E_i \in K \)), then no locations in that enclave can be read.

Rule Isset returns 1 if the contents of condition \( cnd \) is 0 (i.e., if \( cnd \) is not set), otherwise it evaluates to 0.

Rule Function requires that the mode annotation \( \mu \) on function \( \lambda^\mu.c \) equals the mode of the expression evaluation.

Figure 3 shows the inference rules for command execution. Many rules have the premise \( \mu \not\in K \), which collectively ensure that code in killed enclaves can not be executed. Rules Skip, Assign, Seq, If-Else, While-T, and While-F are standard. We write \( \tau[x \mapsto v] \) for the register file that maps \( x \) to \( v \) but otherwise is the same as \( \tau \). Similarly, memory \( m[l \mapsto v] \) maps \( l \) to \( v \) but otherwise is the same as \( m \).

The command call(e) evaluates expression \( e \) to a function and invokes it. The modes of callee and caller should match. This ensures that function calls cannot be used to amplify privilege, and the only way execution can transition modes is via an enclave(i, c) command.

Rule Update updates a memory location, and like Deref, ensures that an enclave’s memory locations can be accessed only by code within the enclave. This rule is used only for non-condition locations. Rule SetCnd is used to set conditions. Since this is a security relevant action, SetCnd produces event Mem(m’) in the trace where m’ is the new memory. These events are used in the definition of the semantic security conditions.

Rule Declassify declassifies expression \( e \) and assigns the result to variable \( x \). Operationally, it is similar to Assign but uses predicate hasNoVars(e) to enforce the syntactic restriction that expression \( e \) contains no variables: it may contain expressions built from values and memory locations (including conditions). Declassifications are security relevant events, and so a declassification event Decl(e, m) is emitted to the trace. Rule Output evaluates the expression \( e \) to a value \( v \), outputs \( v \) on channel \( \ell \), and adds events Mem(m) and Out(\( \ell, v \)) to the trace.

Rule Enclave executes enclave code. Note that enclaves can be entered only from normal mode (i.e., mode \( \mu \) in the conclusion must be \( N \)). This reflects the operation of Intel SGX-like mechanisms: execution of enclave code occurs only by non-enclave code jumping to a well-defined enclave entry point; execution of enclave code ends only by exiting the enclave, not by calling back to non-enclave code; code in one enclave can not directly execute code in another enclave.
### Figure 3. Large-step semantics for select IMPE commands

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Skip** | \( \mu \not\in K \)  
\[ \mu \vdash \langle \text{skip}, r, m, K \rangle \Downarrow r; m; K \triangleright \epsilon \] |
| **Assign** | \( \mu \vdash \langle e, r, m, K \rangle \Downarrow v \)  
\[ r' = r[x \mapsto v] \quad \mu \not\in K \]  
\[ \mu \vdash \langle x := e, r, m, K \rangle \Downarrow r'; m; K \triangleright \epsilon \] |
| **Update** | \( \mu \vdash \langle e_1, r, m, K \rangle \Downarrow l \)  
\( \delta(l) \in \{N, \mu\} \setminus K \)  
\( l \in \text{Loc} \setminus \text{Cond} \)  
\( m' = m[l \mapsto v] \)  
\[ \mu \vdash \langle e_1 \leftarrow e_2, r, m, K \rangle \Downarrow r; m'; K \triangleright \epsilon \] |
| **Output** | \( \mu \vdash \langle e, r, m, K \rangle \Downarrow v \)  
\( \ell \in \{L, H\} \)  
\( \mu \not\in K \)  
\[ \mu \vdash \langle \text{output } e \text{ to } \ell, r, m, K \rangle \Downarrow r; m; K \triangleright \text{Mem}(m') \cdot \text{Out}(\ell, v) \] |
| **Enclave** | \( E_i \vdash \langle e, r, m, K \rangle \Downarrow r'; m'; K' \triangleright t' \)  
\[ N \vdash \langle \text{enclave}(i, c), r, m, K \rangle \Downarrow r'; m'; K' \triangleright t' \] |
| **IF-ELSE** | \( \mu \vdash \langle e, r, m, K \rangle \Downarrow v \)  
\[ i = \begin{cases} 1 & \text{if } v \neq 0 \\ 2 & \text{otherwise} \end{cases} \]  
\[ \mu \vdash \langle c_1, r, m, K \rangle \Downarrow r'; m'; K' \triangleright t' \]  
\[ \mu \vdash \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle \Downarrow r'; m'; K' \triangleright t' \] |
| **WHILE** | \( \mu \vdash \langle \text{while } e, r, m, K \rangle \Downarrow t' \)  
\( v \neq 0 \)  
\[ \mu \vdash \langle c, r, m, K \rangle \Downarrow r'; m'; K' \triangleright t' \]  
\[ \mu \vdash \langle \text{while } e \text{ do } c, r', m', K' \rangle \Downarrow r''; m''; K'' \triangleright t'' \]  
\[ \mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \Downarrow r''; m''; K'' \triangleright t' \cdot t'' \]  
\[ \mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \Downarrow r; m; K \triangleright \epsilon \] |
| **SetCnd** | \( \delta(\text{cnd}) \in \{N, \mu\} \setminus K \)  
\( \text{cnd} \in \text{Cond} \)  
\( m' = m[\text{cnd} \mapsto 1] \)  
\( \mu \not\in K \)  
\[ \mu \vdash \langle \text{set(cnd)}, r, m, K \rangle \Downarrow r; m'; K \triangleright \text{Mem}(m') \] |
| **Call** | \( \mu \vdash \langle e, r, m, K \rangle \Downarrow \lambda \cdot c \)  
\( \mu \vdash \langle e, r, m, K \rangle \Downarrow r'; m'; K' \triangleright t' \)  
\[ \mu \vdash \langle \text{call}(e), r, m, K \rangle \Downarrow r'; m'; K' \triangleright t' \] |
| **Decl** | \( \mu \vdash \langle e, r, m, K \rangle \Downarrow v \)  
\( \mu \not\in K \)  
\[ \mu \vdash \langle \text{declasify}(e), r, m, K \rangle \Downarrow r'; m; K \triangleright \text{Decl}(e, m) \] |
| **Kill** | \( \mu \vdash \langle e, r, m, K \rangle \Downarrow v \)  
\( \mu \not\in K \)  
\[ \mu \vdash \langle \text{kill}(i), r, m, K \rangle \Downarrow r; m; K \cup \{E_i\} \triangleright \epsilon \] |

3. **Attacker Model and Security**

In this section we define security for the IMPE language for a variety of attackers. We consider a passive attacker that can only observe outputs on certain channels, an active attacker that can arbitrarily corrupt non-enclave computation, and an active attacker that can, under certain conditions, corrupt computation both outside and inside enclaves.

The definition of security is that at all times, an attacker knows no more than what the attacker is permitted to know. What the attacker is permitted to know is determined by the security policies on information, which conditions are set when, and what declassifications the program performs.

We model active attackers by allowing additional transitions in the operational semantics of IMPE. Thus, the definition of security is parameterized on variants of the operational semantics of IMPE.

The code uses two locations, password and guess, containing the password and user’s input respectively. Assume \( \delta(\text{password}) = E_1 \) and \( \delta(\text{guess}) = N \), i.e., password belongs to enclave \( E_1 \) and guess is not in an enclave. The program enters enclave \( E_1 \) checks if the password matches the guess by dereferencing the corresponding locations, sets variable status to the result, and exits the enclave. Variable status is then output on channel \( L \). Note that dereferencing password would fail if done outside enclave \( E_1 \).
We assume the only source of confidential information is the initial memory. A security specification \( \gamma \) maps locations to policies and indicates the policy to enforce on information in an initial memory. For example, if \( \gamma(l) = \ell_1 \land \ell_2 \) and \( m \) is the memory from which we start an execution, then we should enforce erasure policy \( \ell_1 \land \ell_2 \) on the data in \( m(l) \). We say that a security specification \( \gamma \) is well-formed if \( \forall l \in \text{Loc.} \gamma(l) \neq \top \) (since security level \( \top \) is for information in initial memory and \( \gamma \) is defined as:

\[
\ell'_{\ell} = \begin{cases} 
\text{Out}(\ell', v) \cdot [t']_{\ell} & \text{if } t = \text{Out}(\ell', v) \cdot t' \text{ and } \ell' \subseteq \ell \\
\{ t' \}_{\ell} & \text{if } t = \text{Out}(\ell', v) \cdot t' \text{ and } \ell' \nsubseteq \ell \\
\{ t' \}_{\ell} & \text{if } t = \alpha \cdot t' \land \alpha \neq \text{Out}(\ell', v) \\
\bot & \text{otherwise}
\end{cases}
\]

Given an execution of program \( c \), an attacker at level \( \ell \) observes some portion of the execution (i.e., some subsequence \( t_{\text{obs}} \)) of the trace produced during execution. The knowledge of the attacker is the set of initial memories for which execution of \( c \) could produce a trace \( t \) such that some subsequence of \( t \) looks the same to the attacker as \( t_{\text{obs}} \). That is, an attacker’s knowledge is the set of initial memories that the attacker believes are possible. Thus, the smaller the attacker’s knowledge, the more precise is the attacker’s knowledge.

We base our definition of attacker knowledge on that of Askarov et al. [7] by parametrizing it on the large-step semantics. That is, we will instantiate \( \downarrow_{\text{kind}} \) with different large-step semantics that represent different attackers. We assume that all initial configurations use a register file \( r_{\text{init}} \) that maps all variables to zero.

**Definition 1** (Attacker knowledge). Given program \( c \), security level \( \ell \), large-step semantics \( \downarrow_{\text{kind}} \), and trace \( t_{\text{obs}} \), attacker knowledge is defined as:

\[
k_{\ell}^{\text{kind}}(c, t_{\text{obs}}) = \{ m | N \vdash (c, r_{\text{init}}, m, \emptyset) \downarrow_{\text{kind}} r' \land m' \land K \triangleright t \\
\land \exists t_0, t_1, t_2. t = t_0 \cdot t_1 \cdot t_2 \land [t_{\text{obs}}]_{\ell} = [t_1]_{\ell} \}
\]

Consider the password authentication example from Section 2.3. Let \( c \) be the program, \( m_0 \) be the initial memory and \( t_{\text{obs}} = \text{Mem}(m_0) \cdot \text{Out}(L, 1) \) be the trace produced by the program executed with semantics \( \downarrow \). The knowledge of a passive attacker at security level \( L \) is the set of all initial memories such that the contents of locations password and guess are equal. More formally, \( k_L(c, t_{\text{obs}}) = \{ m' | m'(\text{password}) = m'(\text{guess}) \} \).

### 3.2 Security

The intuition for knowledge-based security conditions is that an attacker should know only what it is permitted to know. We thus define what an attacker is permitted to know.

We are concerned with attackers that may observe only a portion of a program’s execution. Thus, an attacker at level \( \ell \) that starts observing the execution after condition \( \text{cond} \) has been set should in general not be able to learn anything about information with erasure policy \( \ell_1 \land \ell_2 \) where \( \ell_2 \nsubseteq \ell \). However, an attacker is permitted to learn information that has already been declassified, including declassifications that occurred before the attacker started observing the execution.

**Permuted knowledge via erasure policies** Whether an attacker at level \( \ell \) is permitted to observe information with policy \( p \) depends on which conditions have been set. Let \( U \subseteq \text{Cond} \) be the currently unset conditions. We write \( \text{cur}(p, U) \) for the security level that should currently be enforced on information with policy \( p \). If \( p \) is an erasure policy \( \ell_1 \land \ell_2 \), then we should enforce security level \( \ell_1 \) if \( \text{cond} \in U \) and enforce \( \ell_2 \) if \( \text{cond} \notin U \). Formally:

\[
\text{cur}(p, U) = \begin{cases} 
\ell_1 & \text{if } p = \ell_1 \\
\ell_2 & \text{if } p = \ell_1 \land \ell_2 \text{ and } \text{cond} \in U \\
\ell_2 & \text{if } p = \ell_1 \land \ell_2 \text{ and } \text{cond} \notin U
\end{cases}
\]

Based on the current security level to enforce on information, we define equivalence classes of initial memories that an attacker at level \( \ell \) should not be allowed to distinguish. Intuitively, if initial memories \( m \) and \( m' \) are identical at every location \( l \) for which the current security level permits the attacker to learn information (i.e., \( \text{cur}(\gamma(l), U) \subseteq \ell \)), then the attacker should not be allowed to distinguish \( m \) and \( m' \).

**Definition 2** (Indistinguishable Memories). Given memory \( m \), security specification \( \gamma \), unset conditions \( U \), and security level \( \ell \), we define \( \text{ind}_{\ell}(m, \gamma, U) \) as:

\[
\{ m' | \forall l \in \text{Loc.} \text{cur}(\gamma(l), U) \subseteq \ell \implies m(l) = m'(l) \}
\]

Given an execution from initial memory \( m_0 \) where an attacker at level \( \ell \) starts observing the execution when \( U \) are the unset conditions, then the attacker should not learn whether the initial memory for the execution was \( m_0 \) or some memory in \( \text{ind}_{\ell}(m_0, \gamma, U) \). That is, the attacker’s knowledge should be a superset of \( \text{ind}_{\ell}(m_0, \gamma, U) \).

**Permuted knowledge via escape hatches** Declassifications permit an attacker to learn more information. Following Sabelfeld and Myers [30], we use escape hatches to characterize what information declassification commands \( x := \text{declassify}(e) \) reveal. An escape hatch is a computation over confidential information such that attackers are permitted to learn the result of the computation. In our setting, an escape hatch is an expression \( e \) evaluated against the initial memory. Recall that confidential information is input
to a program only via the initial memory. Thus, by evaluating escape hatch expression \( e \) against the initial memory, \( e \) describes a computation over confidential inputs that is permitted to be declassified.

We connect declassification events \( \text{Decl}(e, m) \) (where \( m \) is the current memory at the time of declassification, and expression \( e \) contains only operations over constants and memory locations) to escape hatches by requiring that the evaluation of \( e \) using \( m \) produces the same value as the evaluation of \( e \) using the initial memory. If so, the attacker is permitted to learn the result of evaluating \( e \). Otherwise we do not allow the declassification event to release any information. We capture this in the definition of escape-hatch indistinguishability below.

**Definition 3** (Escape-hatch indistinguishability). Given initial memory \( m_0 \), current memory \( m \), semantics \( \psi_{\text{kind}} \) and escape hatch \( e \), we define \( \text{Esc}_{\psi_{\text{kind}}}(m_0, m, e) \) as

\[
\{ m' | \exists \mu. (\mu \vdash e, r_{\text{init}}, m_0, \emptyset) \psi_{\text{kind}} v \land \\
(\mu \vdash e, r_{\text{init}}, m, \emptyset) \psi_{\text{kind}} v \\
\implies (\mu \vdash e, r_{\text{init}}, m', \emptyset) \psi_{\text{kind}} v \}
\]

Given semantics \( \psi_{\text{kind}} \), declassification event \( \text{Decl}(e, m) \), and initial memory \( m_0 \), \( \text{Esc}_{\psi_{\text{kind}}}(m_0, m, e) \) is equal to the set of all initial memories if expression \( e \) evaluates to different values in \( m \) and \( m_0 \) (i.e., the attacker should not learn any information from the declassification), and otherwise is equal to all initial memories \( m' \) such that \( e \) evaluates to the same value in \( m' \) as it does in \( m_0 \) (i.e., the attacker is permitted to learn the result of evaluating \( e \)).

**Security definition** We define \( [t]_{\text{mem}} = \{ m | \text{Mem}(m) \in t \} \) to be the set of memory events that occur in trace \( t \) and \( [t]_{\text{esc}} = \{ (e, m) | \text{Decl}(e, m) \in t \} \) to be the set of tuples corresponding to the declassification events in trace \( t \).

Suppose we have an execution from initial memory \( m_0 \) with specification \( \gamma \) that produces trace \( t \cdot t_{\text{obs}} \cdot t' \), where an attacker at level \( \ell \) observes \( t_{\text{obs}} \). Then the attacker is permitted to learn any information that a memory \( m'' \in [t_{\text{obs}}]_{\text{mem}} \) permits. That is, the intersection of the sets \( \text{Esc}_{\psi_{\text{kind}}}(m_0, m', e') \) for \( (e', m') \in [t \cdot t_{\text{obs}}]_{\text{esc}} \) describes what information the attacker is permitted to know based on the current security levels of information.

Moreover, the attacker is allowed to learn declassified information. The intersection of sets \( \text{Esc}_{\psi_{\text{kind}}}(m_0, m', e') \) for \( (e', m') \in [t \cdot t_{\text{obs}}]_{\text{esc}} \) describes what information the attacker is permitted to know based on declassifications that occurred before or during the attacker observation.

A program is secure if the attacker’s knowledge is indeed no more precise than the information the attacker is permitted to know. Definition 4 captures this intuition.

**Definition 4** (Security). Program \( c \) is secure at security level \( \ell \) for security specification \( \gamma \) and large-step semantics \( \psi_{\text{kind}} \) if for all initial memories \( m_0 \) and all executions

\[
N \vdash \delta (c, r_{\text{init}}, m_0, \emptyset) \psi_{\text{kind}} r; m; K \triangleright t \cdot t_{\text{obs}} \cdot t'
\]

where \( t_{\text{obs}} = \text{Mem}(m'') \cdot t'' \) for some memory \( m'' \) and trace \( t'' \), we have

\[
\forall \ell \in \{ \text{ind}_{\psi_{\text{kind}}}(c, t_{\text{obs}}) \}
\]

\[
\bigcap_{m' \in [t_{\text{obs}}]_{\text{mem}}} \bigcup_{e', m' \in (e', m') \in [t \cdot t_{\text{obs}}]_{\text{esc}}} \text{Esc}_{\psi_{\text{kind}}}(m_0, m', e')
\]

Note that this definition is termination- and progress-insensitive. We can modify the definition to be termination- and progress-sensitive, but this results in a more complicated definition that does not provide additional insight into the issues explored in this paper. We thus refrain from doing so.

Note that the definition quantifies over all possible observations \( t_{\text{obs}} \). The definition requires that the first event in the observed trace \( t_{\text{obs}} \) is a memory event to ensure we know the current security level to enforce on information as at the start of the attacker’s observation. This is without loss of generality, since every output event is immediately preceded by a memory event (see rule OUTPUT in Figure 3).

For example, let \( c \) be the password authentication program modified to set condition end on enclave exit.

\[
enclave(1, \text{status} := \text{password} = \text{guess}); \text{set}(\text{end}); \text{output status} to L
\]

The program is insecure for the specification \( \gamma \), where \( \gamma(\text{guess}) = L \cdot \text{end} \cdot \top \) and \( \gamma(\text{password}) = H \). Intuitively, for initial memory \( m_0 \) and \( t_{\text{obs}} = \text{Mem}(m_0[\text{end} \rightarrow 1]) \cdot \text{Out}(L, 1) \) produced by execution with semantics \( \psi \), then the lower bound \( \text{ind}_{L}(m_0, \gamma, \emptyset) \) on the knowledge of an attacker at security level \( L \) is the set of all memories. However, the attacker learns that password and guess are equal.

Suppose we now modify the program to include declassification:

\[
enclave(1, \text{status} := \text{declassify}(\text{password} = \text{guess}); \text{...}
\]

The declassification event induces a new lower bound: \( \{ m' | m'(\text{password}) = m'(\text{guess}) \} \) which is same as the attacker’s knowledge. The program is now secure for an attacker at security level \( L \).

### 3.3 Attackers

A passive attacker simply observes the execution of program and attempts to learn information about confidential input. By contrast, an active attacker can modify or influence the execution of a program. Active attackers represent many malicious behaviors, including attacks that can modify execution arbitrarily (e.g., by gaining control of the program counter or overwriting code) or modify some set of memory locations (e.g., by buffer overflows or by providing malicious input to a program).
We consider three attackers: (1) A passive attacker that can only observe output on the $L$ channel; (2) A non-enclave active attacker that can observe output on the $L$ channel and arbitrarily modify non-enclave code; and (3) An enclave active attacker that can observe output on the $L$ and $H$ channels, and can arbitrarily modify (enclave and non-enclave) code but only under certain conditions.

We use different operational semantics to represent the different attackers. The passive attacker corresponds to the semantics $\llbracket$ (Figure 3). That is, programs execute as written, but only under certain conditions. The converse does not necessarily hold. For example, the passive attacker can exploit a vulnerability in non-enclave code but is unable to exploit these vulnerabilities.

Inference rules for judgment $\mu \vdash \langle c, r, m, K \rangle \sqsubseteq_{E,chaos} r'; m'; K' \triangleright t'$ include all inference rules from Figure 5 (appropriately adapted) and the rule in Figure 4. This new rule allows command $c$ to change to an arbitrary command $c'$ provided all enclaves in $I$ are killed ($I \subseteq K$). Event $A(c')$ is emitted to the trace (and we modify $[t]_E$ to include events of the form $A(c')$).

Consider the following program that stores credit card information in an enclave, where $\gamma(c\text{card}) = H \triangleright \top$ (and $\gamma(I) = L$ for all other locations $l$) and $\delta(c\text{card}) = E_1$.

\begin{verbatim}
   enclave(1, output +c\text{card} to H; set(end)); kill(1)
\end{verbatim}

The program outputs the contents of $c\text{card}$ to the $H$ channel and sets condition $c\text{nd}$ in enclave $E_1$. It then exits the enclave $E_1$ and kills it. The program is secure at security level $H$ for specification $\gamma$ and semantics $\llbracket_{E_1,chaos}$, where $I = \{E_1\}$. This means that if an enclave active attacker modifies the program after $\text{kill}(1)$ has been executed, it is unable to learn anything about the contents of $c\text{card}$. Note that when $I = \emptyset$, the program is not secure for any subset of locations.

## 4. IMPE Type System

We introduce a security-type system [33] for IMPE that guarantees security, i.e., a well-typed program is secure against all the attackers described in Section 3.

Figure 6 shows the syntax of types. Base types $\sigma$ include integers, conditions, references, and functions. Recall that conditions are a subset of locations. We use type $\text{cond}^\mu$ for conditions (i.e., values in the set $\text{Cond}$). A reference type $\tau^\mu$ ref is a pointer to a memory location with contents of type $\tau$. Both condition types and reference types are annotated with mode $\mu$, indicating in which enclave, if any, the memory location resides. References also have a mutability annotation $rt \in \{\text{mut, immut}\}$, indicating whether the reference is mutable or immutable. We use immutable references to ensure that declassified expressions are indeed es-
cape hatches, i.e., that declassified expressions are not modified prior to declassification. All conditions are mutable. We explain function types \( \Gamma^+, K^-, U \overset{p}{\rightarrow} \Gamma^+, K^+ \) after explaining the type judgment.

A security type \( \tau = \sigma_p \) is a base type \( \sigma \) annotated with a security policy \( p \). Intuitively, data with type \( \sigma_p \) should have security policy \( p \) or a more restrictive policy enforced on it.

A type environment \( \Gamma \) maps variables to security types, and non-condition locations to pairs \( (\tau, rt) \) of a security type and immutability annotation, where \( \tau \) is the type of the location’s contents, and \( rt \) describes the location’s immutability. For simplicity, we assume that whether a condition is set is public information, and so for any \( \text{end} \in \text{Cond} \), the type of \( \text{end} \) is \( \text{cond}^\mu_{\text{end}} \) for some mode \( \mu \) where \( \delta(\text{end}) = \mu \). Thus, we exclude \( \text{Cond} \) from the domain of \( \Gamma \).

A type environment is well-typed for \( \delta \) if all locations containing confidential information belong to some enclave. Since security level \( \top \) is meant to indicate information that is too confidential to be stored on the machine, we also require that well-typed environments do not map any variable or location to a type \( \sigma_\top \). The following definition formally states the well-typedness of environment \( \Gamma \) for \( \delta \).

**Definition 5 (Well-Typed Environment).** A type environment \( \Gamma \) is well-typed for \( \delta \), denoted as \( \Gamma \vdash_\delta \Gamma \geq \text{ok} \), if

\[
\forall l \in \text{Loc} \setminus \text{Cond}. \quad \Gamma(l) = (\sigma_p, rt) \land p \not\subseteq L \implies \delta(l) \neq \top \land p \neq \top
\]

and

\[
\forall x \in \text{Vars}. \quad \Gamma(x) = \sigma_p \implies p \neq \top
\]

The IMP type system is flow-sensitive in that the type of variables may differ at different program points. Also, our type system tracks the set of killed enclaves to ensure that no code or data inside a killed enclave is accessed. To ensure that erasure policies are correctly enforced, our type system tracks the set of conditions that are definitely unset. The typing judgment for commands has the form

\[
\text{pc}, \mu, \Gamma, K, U \vdash_\delta c : \Gamma', K'
\]

where:

- \( \Gamma \) and \( \Gamma' \) are, respectively, the type environments immediately before and after execution of command \( c \);
- \( K \) and \( K' \) are, respectively, the set of killed enclaves immediately before and after execution of \( c \);
- \( U \) is the set of conditions that are known to be not set immediately before the execution of \( c \);
- \( \mu \) indicates whether \( c \) executes in normal mode (\( \mu = \top \)) or in an enclave (\( \mu = E_j \));
- \( \text{pc} \) is a policy representing an upper bound on the information that influences the decision to execute \( c \), and is also a lower bound on the side-effects of \( c \). This program counter policy \( [29, 38] \) is used to prevent implicit flows \( [14] \), i.e., information flows via the control decisions of a program.

- \( \delta \) is a function which indicates for each memory location which enclave, if any, it belongs to.

The type judgment for expressions is \( \mu, \Gamma \vdash_\delta e : \tau \), meaning that in mode \( \mu \) under type environment \( \Gamma \), expression \( e \) has type \( \tau \).

A function type \( \Gamma^+, K^-, U \overset{p}{\rightarrow} \Gamma^+, K^+ \) indicates the type environment \( \Gamma^- \) that must hold before the function is invoked, and the type environment \( \Gamma^+ \) that will hold immediately after function invocation. These environments may be partial functions, since the function may use only a subset of variables. Well-typedness of functions will ensure that \( \text{dom}(\Gamma^-) \subseteq \text{dom}(\Gamma^+) \). Kill set \( K^- \) is the set of killed enclaves the function expects at invocation, and \( K^+ \) is the set of killed enclaves after function invocation. Set \( U \) is the set of conditions that the function assumes are unset upon function invocation. Mode \( \mu \) is the mode in which the function was defined, and policy \( p \) is a lower bound on the side-effects of the function.

We define subtyping on security types based on the relative restrictiveness of security policies. Given policies \( p \) and \( q \), we say that \( q \) is at least as restrictive as \( p \), written \( p \leq q \), if policy \( q \) imposes at least as many restrictions on the use of data as policy \( p \). The relation \( \leq \) on policies forms a lattice. We write \( \uplus \) for the join operation. We overload the symbol \( \leq \) and write \( \sigma_1 \leq \sigma_2 \) when base type \( \sigma_1 \) is a subtype of base type \( \sigma_2 \), and write \( \tau_1 \leq \tau_2 \) when security type \( \tau_1 \) is a subtype of security type \( \tau_2 \). We lift subtyping to type environments and define \( \Gamma_1 \leq \Gamma_2 \) if and only if \( \text{dom}(\Gamma_1) = \text{dom}(\Gamma_2) \) and \( \forall y \in \text{dom}(\Gamma_1). \Gamma_1(y) \leq \Gamma_2(y) \). Function types are contravariant in the pre-environment, and the side-effect bound, covariant in the post-environment, and invariant otherwise. Inference rules for the subtyping (\( \leq \)) relation are presented in Appendix B.

Figure 7 shows typing rules for expressions. As is standard in security-type systems, constants (including integers, conditions, references, and function definitions) are given policy \( L \), the most permissive security policy.

Dereferencing an expression may reveal information about both which location is dereferenced and the contents of that location. Thus in rule T-Deref the result of a \( \ast e \) expression has a security policy that is at least as restrictive as the policy on the reference and the contents of the reference. The premise \( \mu' \neq \top \) \( \implies \mu = \mu' \) (in both T-Deref and T-Isunset) requires that locations in enclaves can be accessed only by code in the same enclave.

Most of the commands follow the standard security typing rules for an imperative language (including subsumption). The rules further ensure that killed enclaves are never accessed (premise \( \mu \not\in K \) in many rules) and that enclave locations are accessed only by code in the appropri-
For presentation purposes, these rules are non-algorithmic. They can be easily adapted to enable syntax-directed type-checking algorithms.

Rule T-OUTPUT ensures that the current security level enforced on both a value output to a channel, and the decision to perform the output, is permitted to be output \((\text{cur}(p, U) \sqcap \text{cur}(pc, U) \subseteq \ell)\).

Rule T-IF-ELSE is similar to T-IF-ELSE but is used when the branch condition tests whether a condition is unset. This allows the true branch to be type-checked under the assumption that condition \(\text{cond}\) is unset, which improves precision, of, for example, output commands.

Rule T-ENCLAVE ensures that command enclave\((i, c)\) can be executed only in non-enclave mode \(\mu = N\), and type checks \(c\) in mode \(E_i\) with an empty set of conditions that are assumed to be unset. This is to ensure that an attacker that can control non-enclave execution is unable to violate an assumption made by enclave code. Also, premise isVarLowContext\((\Gamma')\) ensures that at the end of the enclave code, all variables contain only information with policy \(L\). This ensures that at the end of execution of enclave code, there is no confidential information remaining in variables that could be leaked to an attacker.

Rule T-KILL requires that enclaves can only be killed by non-enclave code \((\mu = N)\). This reflects the operation of Intel’s SGX enclaves. Since killing an enclave may be detectable by a non-enclave attacker, we ensure that the decision to kill an enclave relies on only non-confidential information \((pc = L)\). Premise \(E_i \not\subseteq K\) ensures that an enclave is not killed more than once.

Rule T-UPDATE is mostly standard, but like T-DEREF and T-ISUNSET, requires that locations in enclaves can be accessed only by code in the same enclave.

Rule T-SETCNDCND checks that condition \(\text{cond}\) can be set only if it is not currently assumed to be unset, i.e., \(\text{cond} \not\subseteq U\).

Rule T-CALL ensures that the preconditions for calling the function are satisfied, namely that the kill set and unset conditions assumed by the function is equal to the current kill set and unset conditions, and that the assumptions of the function’s type environment are satisfied \((\forall y \in \text{dom}(\Gamma^\neg), \Gamma^\neg(y) \leq \Gamma(y))\). The program counter policy \(pc\) and the information revealed by which function to invoke \((q)\) must be no more restrictive than \(p\), the lower bound on the function’s side effects. The premise \(U \not\subseteq \emptyset \implies \mu \neq N\) prevents a non-enclave active attacker from directly invoking a function and violating the assumption on set \(U\). The type environment after the function call respects the function’s post-environment: \(\forall y \in \text{dom}(\Gamma^+), \Gamma^+(y) \leq \Gamma^+(y)\). Since \(\Gamma^\neg\) and \(\Gamma^+\) are partial, we require that the types of variables not in \(\text{dom}(\Gamma^\neg)\) (which is a superset of \(\text{dom}(\Gamma^+))\) remain unchanged: \(\forall y \in \text{dom}(\Gamma) \setminus \text{dom}(\Gamma^+)\), \(\Gamma(y) = \text{Gamma}(y)\). After the function invocation, the kill set is \(K^+\).

**Type Soundness** Program execution starts with a known initial register file \((\text{r}_{\text{init}})\) that maps all variables to constant zero. We say that type environment \(\Gamma\) corresponds to security specification \(\gamma\) if policies on locations agree with \(\gamma\) and \(\Gamma\) maps all variables to int\(_L\) (since \(r_{\text{init}}\) maps every variable...
Theorem 1. Let $\gamma$ be a well-formed security specification and $\Gamma$ be a type environment that corresponds to $\gamma$ and is well-typed for $\delta$. If $L, N, \Gamma, \emptyset, \emptyset \vdash c : \Gamma', K'$ then:

- $c$ is secure at security level $L$ for specification $\gamma$ and semantics $\delta$;

- $c$ is secure at security level $L$ for specification $\gamma$ and semantics $\delta$.

For all $I \subseteq \{E_1, E_2, \ldots\}$, define

$$\gamma'(l) = \begin{cases} 
\gamma(l) & \text{if } \delta(l) \in I \\
L & \text{otherwise} 
\end{cases}$$

Command $c$ is secure at security level $H$ for specification $\gamma'$ and semantics $\delta'_{E_1-chaos}$.

Note that for an enclave active attacker that can attack enclaves in set $I$ only after those enclaves have been killed, Theorem 1 states that command $c$ is secure for security specification $\gamma'$ derived from $\gamma$. Specification $\gamma'$ is the same as $\gamma$ for all locations placed in enclaves in $I$, but for all other locations does not enforce any security restrictions (i.e., $\gamma'(l) = L$ if $\delta(l) \notin I$). That is, we can protect information placed in enclaves in $I$ against an enclave active at-
\[ e ::= n \mid x \mid e_1 \oplus e_2 \mid l \mid *e \mid \text{isunset}(\text{cnd}) \mid \lambda.c \]
\[ v ::= \lambda.c \mid n \mid l \]
\[ c ::= \text{skip} \mid x ::= e \mid x ::= \text{declassify}(e) \mid e_1 \leftarrow e_2 \]
\[ \mid \text{output } e \text{ to } \ell \mid \text{call}(e) \mid \text{set}(\text{cnd}) \mid c_1; \ldots ; c_n \]
\[ \mid \text{if } e \text{ then } c_1 \text{ else } c_2 \mid \text{while } e \text{ do } c \]
\[ l \in \text{Loc} \quad \text{Cond} \subseteq \text{Loc} \quad \text{cnd} \in \text{Cond} \]
\[ \sigma ::= \text{int} \mid \text{cond} \mid \tau \text{ref}^r \mid G^*, U \overset{\text{L}}{\rightarrow} G^+ \]
\[ \mathbb{I} ::= \sigma_p \]
\[ rt \in \{\text{mut, immut}\} \]

Figure 9. IMPS syntax and types

The type system is a simplified version of the IMPE type system. Judgment \( pc, \mathcal{G}, U \vdash c: G' \) means that command \( c \) is well-typed, where \( \mathcal{G} \) and \( G' \) are the type environments immediately before and after execution of \( c \), program counter policy \( pc \) is an upper bound on the information that influences the decision to execute \( c \), and set \( U \) are conditions that are definitely unset.

Judgment \( \mathcal{G} \vdash e: \sigma_p \) means expression \( e \) has type \( \sigma_p \) under type environment \( \mathcal{G} \). All typing rules are straightforward adaptations of the IMPE rules and are given in Appendix C.

6. Translation

We provide a translation of IMPS programs to IMPE that automatically places code and locations into enclaves. Our translation is constraint-based: a type-directed algorithm produces a set of constraints, and any solution to the constraints provides a well-typed IMPE program. We consider various criteria for choosing one translation over another.

6.1 Constraint-Based Translation

The constraints place restrictions on where locations may be placed (i.e., on the function \( \delta \)), on kill sets, on mode annotations, and on which commands may be placed inside an enclave.

The constraints ensure that any location that contains confidential information (i.e., with a policy other than \( L \)) is placed in an enclave, and that subsequent use of these locations is consistent (i.e., accessed only by code in the same enclave). The constraints also ensure that confidential data cannot be accessed in non-enclave mode, and also that enclaves are killed appropriately (i.e., no enclave is accessed after it is killed, and enclaves are killed at most once).

The translation judgment for commands has the form

\[ pc, \mathcal{G}, U, c, G' \equiv \mu, \Gamma, K, \delta, c', \Gamma', K' \]

We ensure that if \( pc, \mathcal{G}, U \vdash c: G' \) for IMPS command \( c \), then \( c' \) is the translated IMPE command such that, provided the constraints are satisfied, \( pc, \mu, \Gamma, K, U \vdash_\delta c : \Gamma', K' \).

Instead of the translation judgment explicitly producing a set of constraints, for brevity we present inference rules for the judgment such that constraints are implied by premises that restrict modes, mode annotations, kill sets, etc.

The translation judgment for expressions has the form

\[ \mathcal{G}, e, \sigma_p \equiv \mu, \Gamma, \delta, c', \sigma_p \text{ where } e \text{ is an IMPS expression such that } \mathcal{G} \vdash e: \sigma_p \text{ holds and } c' \text{ is the translated IMPE expression } \]

such that, provided the constraints are satisfied, \( \mu, \Gamma \vdash_\delta c' : \sigma_p \text{ holds} \).

The judgment for translating base types is \( \sigma \equiv_\delta \sigma \). It states that an IMPS base type \( \sigma \) is translated to an IMPE base type \( \sigma \). It is parametrized by \( \delta \) to ensure that type environments for functions types are translated appropriately.

Figure 10 shows the type translation. In the rule for type environments, premise \( \forall l \in \text{dom}(\mathcal{G}). \mathcal{G}(l) = (\sigma_p, rt) \land p \not\leq L \implies \delta(l) \neq N \) ensures that all confidential locations...
 Enforcement of Network Invariant

They enforce the invariant that a location in enclave is accessed in the same mode by non-enclave code.

To follow the premises of the corresponding typing rules.

If the program contains confidential information, then the function should not be invoked at enclave exit, i.e., a variable contains confidential information when the enclave exits.

This is required to enforce typing rule T-ENCLAVE. Notice that an enclave exit after command $c_i$ does not necessarily mean that $\mu_{i+1} = N$. It may signal the start of a different enclave, hence we also state $\mu_i \neq \mu_{i+1}$ in the antecedent.

Rule TR-SEQ uses utility function processSeqOutput which inserts enclave and kill commands appropriately into the translation. Intuitively, enclave is introduced for a command $c'_j$ if there is a mode change. Command kill$(j)$ is inserted after command $c'_j$ if $j \in K'_{\mu'}$.

Pseudo code for processSeqOutput is presented in Appendix [2]

Rule TR-IF-ELSE requires that same sets of enclaves are killed in both the branches. Also, if variables contain confidential information on exit of either branch, then the outer mode should not be normal. Rule TR-IF-ISUNSET always places the command in an enclave to ensure that the premises of typing rule T-IF-ISUNSET are met. Rule TR-WHILE requires that no enclave is killed in the loop body. Rule TR-CALL requires that if set $U$ is non-empty, then the function is defined in an enclave.

Soundness of Translation

Successful translation of well-typed IMPs program produces a well-typed IMPE program.

\textbf{Theorem 2} (Soundness of Translation). Let $G$ be a well-typed IMPs environment and $\Gamma$ be an IMPE environment that is well-typed for $\delta$. For all commands $c \in$ IMPs, if $pc, G, U \vdash c : G'$ and $pc, G, K, c, G' \rightarrow \mu, \Gamma, U, \delta, c', \Gamma', K'$ then $pc, \mu, K, U \vdash_\delta c' : \Gamma', K'$

Given a well-typed IMPs program and environment $G$, if the translation is successful using an IMPE environment $\Gamma$ that is well-typed for $\delta$, then the translated IMPE program is also well-typed. Since a well-typed IMPE program is secure (Theorem [1], the translation thus guarantees security against all the attackers described earlier.

Note that well-typedness of the translated program is contingent on the success of translation. The only way that translation will fail is if predicate isVarLowContext($\Gamma'$) does not hold for $\Gamma'$ at enclave exit, i.e., a variable contains confidential information when the enclave exits. This is because the trivial solution of putting all code and data inside a single enclave will succeed provided there is no confidential information left in variables at the end of the program. One approach to ensure translation always succeeds is to add a semantics-

![Figure 10. Type translation rules](image-url)
preserving transformation that zeroes-out variables as soon as they are dead.

6.2 Constraint Solution and Optimization

The constraints used in the translation of IMPs programs to IMPE can be expressed as a Boolean SAT instance, assuming that the mode set \( \text{Mode} = \{\text{N}, \text{E}_1, \text{E}_2, \ldots\} \) is of a fixed finite size. Specifically, the constraints restrict modes of locations and code, and kill sets (which are sets of enclaves). All constraints generated during translation can be encoded straightforwardly in a SAT formula. For a program of size \( n \) with \( m \) locations, where \( |\text{Mode}| = k \), the size of SAT formula is \( O((n+m)^2 + nk) \).\(^3\)

There may be many possible translations of a given IMP program without any of them being clearly the “best” translation. Naively, we could try to place the entire program in a single enclave. However, even if successful, this is not always desirable for at least two reasons. First, an enclave may have size restrictions and a program can be too large to fit.\(^4\) Second, even if the program can fit inside an enclave, it may be desirable to have as little code as possible in enclaves, to reduce the trusted computing base (i.e., the code that must be assumed to be correct; security for a non-enclave active attacker assumes that enclave code does not contain exploitable vulnerabilities).

There are several possible criteria for comparing the quality of translations, including minimizing the code and data inside enclaves (which corresponds to minimizing the trusted computing base (TCB)), reducing the lifetime of confidential data by killing enclaves as soon as possible, or minimizing the performance penalty of enclaves.\(^5\)

We can cast our translation as a constraint optimization problem that optimizes an objective function that approximates TCB-size, lifetime of enclaves, performance penalty, or a combination of these.

A pseudo-Boolean function \( f : \{0, 1\}^n \rightarrow \mathbb{R} \) is a real-valued function of a finite number of 0-1 valued variables.\(^6\) A pseudo-Boolean constraint is an equality or inequality between pseudo-Boolean functions. Pseudo-Boolean optimization (PBO) optimizes a pseudo-Boolean function subject to pseudo-Boolean constraints. PBO is 0-1 multilinear integer programming and is NP-hard.\(^8\) We can encode the SAT formula for a translation as a pseudo-Boolean constraint and express TCB size and performance as pseudo-Boolean functions to be minimized.

We can compute the TCB cost by counting the number of non-sequence commands placed in enclaves.

Killing an enclave as soon as possible reduces the window of vulnerability. This can be achieved by maximizing the size of kill sets at all program points, which effectively kills enclaves as soon as possible. Moreover, we can facilitate killing enclaves as early as possible by using more enclaves, i.e., partitioning code and data into enclaves at fine granularity. This is also optimized by maximizing the size of kill sets. Note that to avoid spuriously putting public data into enclaves to increase the total number of enclaves that can be killed, we require that each killed enclave has at least some confidential data stored in it.

\(^3\) Intuitively, \( (n+m) \) mode variables, pairs of which are constrained to be either equal or different are generated, resulting in at most \( (n+m)^2 \) constraints. Additionally, \( nk \) kill set constraints (e.g., \( K_{i,j+1} = K_i' \cup K_i'' \) in TR-SEQ) are generated. Thus the size of the SAT formula is \( O((n+m)^2 + nk) \).

\(^4\) On some models, SGX enclaves have a maximum size of \( 2^{31} \) bits.\(^24\)

\(^5\) In Intel SGX, entering or exiting an enclave flushes all TLB entries.\(^24\)
Figure 12. Translation for commands
Enclave entry and exit is expensive and penalizes the run-time performance. Although we have not implemented it, we could approximate the run-time cost using a Control Flow Graph (CFG) and approximating how frequently execution enters and exits enclaves.

7. Comparison with SGX

Although there are several hardware-enforced enclave-like mechanisms, IMPE is mostly heavily influenced by SGX. We discuss how IMPE relates to SGX.

First, we assume that enclaves are isolated from each other: code in enclave $E_i$ can not access memory in enclave $E_j$ when $i \neq j$. SGX does enforce this via an access control mechanism, but uses a single encryption key to protect the contents of all enclaves. Some enclave mechanisms (such as TrustZone) do not provide multiple enclaves.

Second, we assume that once an enclave is killed, the contents of the enclave can never be recovered, thus providing forward secrecy. However, the current design of SGX bases access control decisions on the initial measurement of an enclave. That is, if another enclave is created that has the exact same initial contents as the killed enclave, a replay attack may be possible, whereby the new enclave decrypts memory pages from the killed enclave.

Third, our model assumes inputs to an execution are provided in the initial memory and output channels exist for security levels $L$ and $H$. Our model can be easily modified to use channels for input instead of the initial memory. Secure channels from an SGX enclave to remote parties can be straightforwardly implemented using cryptographic mechanisms. However, SGX currently provides little support for secure output to local devices and no support for secure local input, possibly making it unsuitable for, e.g., securely checking a locally-entered password. However, support for secure local I/O is emerging, such as TrustZone's Trusted User Interface [17]. This supports our modeling choice to allow the enclave to receive and send confidential information, which can represent (remote or local) secure I/O.

8. Evaluation

We implement six case studies (many inspired by related work [16, 34, 36]) to evaluate the expressiveness of security policies, and the translation from IMPs to IMPE. The translator and case studies are available online [19]. All case studies are implemented as (well-typed) IMPs programs which translate successfully to IMPE programs. Thus all case studies are secure against passive, enclave, and non-enclave active attackers.

We extend the calculi with strings, pairs, and arrays. The types of IMPE and IMPs are extended as follows.

$$
\sigma ::= \cdots \mid \text{string} \mid \sigma_1 \times \sigma_2 \mid \tau^{\mu} \mid rt \\
\tau ::= \cdots \mid \text{string} \mid \sigma_1 \times \sigma_2 \mid \tau \mid rt
$$

An array is a sequence of locations with the constraint that all elements of the array are in the same enclave (or all elements in no enclave). IMPE array type $\tau^{\mu} \mid rt$ indicates an array that contains values of type $\tau$, mode $\mu$ indicates in which enclave (if any) the array is placed and $rt$ indicates if the contents of array are mutable. The IMPs array type is similar except that there is no mode annotation. Types for strings and pairs are straightforward.

Password Authentication Recall the password authentication example (with declassification) from Section 3.2. Consider an IMPs version (i.e., without any enclave annotations). Translating it with our tool gives the following.

enclave(1, status := declassify(*password = *guess));
kill(1); set(end); output status to $L$

The translation assigns enclave $E_1$ to locations password and guess (i.e., translated locations have types $\text{int}_H \mid \text{ref}^{\text{immutable}}$ and guess : $\text{int}_L \mid \text{end} \times \top \mid \text{ref}^{\text{immutable}}$). The declassification is placed inside $E_1$ because it reads password and guess. The translation kills the enclave immediately after exiting the enclave. This is as early as possible, thus minimizing the window of vulnerability.

Private Browsing A private session of a web browser allows a user to browse the web with the assurance that the browsing history cannot be retrieved after the private session has ended. However, private browsing implementations are error prone, and many leak information from private sessions [11, 33]. We model a private browsing session where the user starts a private session, browses, then ends the session. The security requirement can be expressed as an erasure policy that states that all private browsing data (and data derived from it) should be erased when a condition marking the end of the session is set.

Since our calculi model input as the initial memory, we assume that the initial memory contains the user’s input to the private session (e.g., an array of URLs to visit). The user’s input has erasure policy $H \mid \text{end} \times \top$, where condition end is set at the end of the private session. During the private session, output is sent to channel $H$. Once the session ends, we model normal browsing by output to channel $L$.

Translation assigns enclave $E_1$ to all the locations containing the user’s input to the private session. It also places all code related to the private browsing session inside enclave $E_1$ and generates a kill instruction before resuming normal browsing.

Secure Calculator We implement a secure calculator that performs public operations on confidential data. This is a model of, for example, a tax computation, where well-known operations (the tax computation) are performed on confidential input (an individual’s financial information). The operations are chosen dynamically (i.e., public inputs specify which operations to perform). The result of the computation is output to channel $H$. The initial memory contains an array of operations to perform (with security policy
reduce each word in the document; a function takes a document as input and produces counts of the initial memory. contain several such documents. A map partial counts are then combined. Each document is modeled counts of each word in a document are first emitted and the frequencies, similar to a case study by Schuster et al. \[34\].

The translation places the confidential data in enclave \(E_1\) and the array of operations outside the enclave. To minimize the TCB, the translation places in the enclave each command that reads or writes the confidential stack, but leaves all other commands outside the enclave. For example:

while \((i < \text{numOps})\)
if \((\ast \text{ops}[i] = \text{"add"})\) then
    \(\text{stack}[\text{top} − 1] ← \ast \text{stack}[\text{top} − 1] + \ast \text{stack}[\text{top}];\)
else if \((\ast \text{ops}[i] = \text{"sub"})\) then
    ...
    \(\text{top} := \text{top} − 1;\)
output \(\ast \text{stack}[\text{top}]\) to \(H;\)
i := i + 1

The translation places the confidential data in enclave \(E_1\) and the array of operations outside the enclave. To minimize the TCB, the translation places in the enclave each command that reads or writes the confidential stack, but leaves all other commands outside the enclave. For example:

if \((\ast \text{ops}[i] = \text{"add"})\) then
    \(\text{enclave}(1, \text{stack}[\text{top} − 1] ← \ast \text{stack}[\text{top} − 1] + \ast \text{stack}[\text{top}]);\)

This reduces the amount of code in enclaves, but will likely result in poor performance, due to frequent enclave entries and exits. If this is a concern, the translation could use a different objective function that balances estimated performance with TCB size.

**Secure Map-Reduce** We model a word-count program that takes a set of private documents, and computes word frequencies, similar to a case study by Schuster et al. \[34\]. The program follows the map-reduce model, in which partial counts of each word in a document are first emitted and the partial counts are then combined. Each document is modeled as an array of confidential strings doc : \(\text{string}_H\) \(\text{mut},\) and the initial memory contains several such documents. A map function takes a document as input and produces counts of each word in the document; a reduce function takes as input a specific word, and sums the partial counts of the word. The output of the program \(\text{wordcount} : (\text{string} × \text{int})_H\) \(\text{mut}\) is an array of pairs of words and the frequency of that word.

The translation places the entire map and reduce functions inside an enclave, as well as all of the documents. That is, the entire computation is placed inside an enclave, as is the hand-coded map-reduce computation of Schuster et al. The enclave is killed after map-reduce computation.

**Secure Query Processing** We model query processing over confidential data, similar to the *Query Processing over Encrypted Database* case study by Sinha et al. \[36\]. Given a database table with public keys (e.g., employee names, in the column name) and confidential data (e.g., wage payments, in column wages), the query selects rows that match a given key, and sums the confidential data. The selection of rows uses only non-confidential data but the subsequent summing uses confidential data.

We model columns name and wages as arrays, with policies \(L\) and \(H\) respectively. Row selection chooses all indices of array name that are equal to key “alice”. Summing computes the sum of all wages corresponding to the selected indices.

The translation places array wages in enclave \(E_1\), but leaves array name outside of any enclave. The row selection computation is placed outside an enclave, and the summing operation is placed inside enclave \(E_1\). Our automated translation places the same data and computation in enclaves as the (manually coded) case study of Sinha et al.

**Secure Chat Client** We model a secure chat client, inspired by the case study of Askarov et al. \[7\]. Messages sent and received by the client are emitted to a log. When the user enters a “clear” command, all messages (including the log) should be erased. We model messages sent and received and commands entered by the user as data in the initial memory. We model logging as an update to location log. We give messages and the log the erasure policy \(L\) \(\text{clear}\) \(\top\), which states that the contents of log are erased when condition clear is set. The condition is set only when a “clear” command is issued. The translation places log in an enclave, as well as all code that updates the log.

**9. Related Work**

**Models for Secure Hardware Architecture and Compilation** Fournet and Planul \[16\] securely compile imperative programs into distributed programs using cryptography and hardware mechanisms (such as Trusted Platform Modules (TPM) and secure boot) to enforce noninterference for confidentiality and integrity. They emulate secure memory (that cannot be accessed by adversaries) and enforce control-flow restrictions on the distributed program. The compiled program is proven to be at least as secure as the source program: for every attack on the compiled program there is a corresponding attack on the source program, with the same information leakage. By contrast, we focus on expressive security policies (erasure and declassification) that go beyond noninterference. Their system doesn’t provide erasure guarantees. We target a single machine and use enclave mechanisms that directly provide secure memory (instead of emulating secure memory via cryptographic mechanisms). Both our work and theirs shield the programmer from the mechanisms used to enforce security. Although we do not focus on integrity guarantees in this work, we rely on enclaves to provide integrity guarantees on code running inside enclaves (cf. security against non-enclave active attackers). We believe that our target calculus IMPe can be extended to provide integrity guarantees about computation inside enclaves.

VC3 \[34\] enables distributed map-reduce computations in untrusted cloud environments while keeping code and data secret, using SGX enclaves to protect against adversaries that might control the entire software stack of the cloud provider’s infrastructure. We instead focus on provid-
ing confidentiality for general programs in the presence of an attacker controlling the entire software stack of a single system. In VC3, all data is confidential (i.e., equivalent to our policy $H$) and all map-reduce computation of a given node is placed inside a single enclave on that node. By contrast, we use expressive security policies (i.e., declassification and erasure) and infer enclave placement to optimize various objective functions. VC3 ensures that only address-taken variables are read and written. The region-self-integrity objective functions. VC3 ensures that only address-taken variables are read and written. The region-self-integrity mechanism prevents unintended disclosure of information due to low-level errors (e.g., buffer overflow). This can be used as a defense-in-depth mechanism in our work to reduce the possibility of an enclave active attacker exploiting vulnerabilities in enclave code.

Moat [35] models SGX using BoogiePL [13] and verifies the confidentiality of binary SGX programs in the presence of “havocing” adversaries capable of modifying non-enclave code. A havocing adversary is analogous to our non-enclave attacker, which can arbitrarily modify non-enclave code. Thus, ensuring confidentiality against a havocing adversary corresponds to security for a non-enclave active attacker. Our work also considers enclave active attackers, which are more powerful than havocing adversaries. Our work differs from Moat in shielding developers from low-level enclave-specific details.

Ironclad [22] provides verifiable remote equivalence: an application running on an untrusted server is indistinguishable from its high-level abstract state machine. Ironclad uses secure hardware (e.g., TPM) as the root of trust and to enable secure channels from verified software to remote clients. Our work could potentially be used in an Ironclad-like setting to reduce verification effort: enclave inference can be used to identify and minimize the security-critical parts of an application, which reduces the code that must be verified.

Sinha et al. [37] enforce confidentiality by placing an entire application inside an SGX enclave and restricting its communication with external memory through a narrow interface to a trusted library. They enforce Information Release Confinement, which ensures that the application satisfies a form of control-flow integrity and never directly accesses non-enclave memory. This work is complementary to ours, and could be used for defense-in-depth in our work, making it harder for an enclave active attacker to exploit vulnerabilities in enclave code.

Patrignani et al. [24] provide a fully-abstract secure compilation scheme for compiling strongly typed object-oriented languages to protected module architectures (PMAs) that offer memory isolation mechanisms and are similar to enclaves. Objects containing private methods are placed inside protected modules thus preventing a low-level attacker from bypassing encapsulation mechanisms. The compilation scheme is proven to preserve and reflect the encapsulation of the source program. Their low-level attacker is similar to the non-enclave active attacker in our model. Though we do not aim for full abstraction, our work provides a stronger information flow guarantee for applications with more expressive security requirements against different attackers.

None of the above works consider applications using multiple enclaves whereas our programming model supports multiple enclaves seamlessly.

**Language-based Information-Flow Control** Much work in language-based information-flow control is concerned with enforcing application-specific security guarantees [14, 25, 29, 38]. Our work extends these techniques to a setting where the underlying software stack is not trusted. That is, we consider strong low-level attackers that are capable of arbitrary corruption of some parts of a program.

**Information Erasure** A key emphasis in our work is the enforcement of information erasure using SGX-like mechanisms. Information erasure is related to data deletion, but requires that the observable behavior of a system reveals nothing about the deleted data, which may, for example, require tracking and deletion of data derived from the deleted data. Language-based information erasure was introduced by Chong and Myers [9], and several works present techniques for enforcing erasure (e.g., [7, 10, 23]). By contrast with these previous language-based approaches, we protect against more powerful lower-level attackers.

Other work uses language- and system-based techniques to ensure data deletion at the system- or architectural-level of abstraction. Chow et al. [11] enforce data deletion by analyzing the lifetime of sensitive data, and automatically zeroing out data in memory. Perlman [27] proposes a file system that uses cryptographic techniques to reliably delete files. These approaches may fail to remove derived data, and thus will not enforce information erasure. Lacuna [13] runs sensitive computations in a “private session” and can securely delete all session data at the end of the session (including data used to communicate with peripheral devices). Provided all sensitive information is contained within a private session, Lacuna can enforce both data deletion and information erasure.

**Acknowledgments**

This material is based upon work supported by the National Science Foundation under Grant No. 1054172.

**References**


Enclave Equivalence \( \simeq \)

Equivalence relation \( \simeq \) is used to characterize the ability of an active attacker. Intuitively, given commands \( c \) and \( c' \), we have \( c \simeq c' \) if \( c \) and \( c' \) have the same code in enclaves, but may differ arbitrarily on non-enclave code. We define \( \simeq \) using function \( \chi \) which syntactically extracts enclave code.

Definition 6 (Enclave Equivalence). Two IMP programs \( c_1 \) and \( c_2 \) are enclave equivalent, denoted \( c_1 \simeq c_2 \), iff

\[
\chi(c_1) = \chi(c_2)
\]

where

\[
\chi(\text{enclave}(j, c)) = \{(E_j, c)\}
\]

\[
\chi(\lambda E_j c) = \{(E_j, \lambda E_j c)\}
\]

\[
\chi(\lambda N c) = \chi(c)
\]

and all atomic expressions and commands return the empty set, e.g.,

\[
\chi(\text{skip}) = \emptyset
\]

\[
\chi(n) = \emptyset
\]

and all other expressions and commands recurse on sub-expressions and sub-commands, e.g.,

\[
\chi(c_1; \ldots; c_n) = \chi(c_1) \cup \ldots \cup \chi(c_n)
\]

\[
\chi(c_1 \oplus c_2) = \chi(c_1) \cup \chi(c_2)
\]

For example, given \( c_1 = \text{enclave}(1, \text{output} 42 \to L) \) and \( c_2 = \text{skip} \), we have \( \chi(c_1) = \chi(c_2) = \{(E_1, \text{output} 42 \to L)\} \). The programs \( c_1 \) and \( c_2 \) are thus enclave equivalent.

IMP Type System

Figure 13 defines the relabeling relation \( \preceq \) on policies.
Figure 15. IMPS typing rules for commands
### E. Proofs

We first prove the soundness of IMP type system, Theorem 1 in Section E.1 and then prove the soundness of translation, Theorem 2 in Section E.2.

#### E.1 Soundness of IMP Type System

The proof for Theorem 1 follows the technique of Pottier and Simonet [28]. The language IMP² extends IMP to include value pairs.

\[ v ::= \cdots | (v_1 \mid v_2) \]

The pair construct represents values that may arise in two different executions of a program. They are used to track how registers and memories differ in different executions of a program. Register (Memory) in IMP² is a function from variables (locations) to value pairs. We use \( (c, r, m, K) \bullet \) to denote IMP² configuration. It has the same meaning as the IMP configuration except that the register \( r \) and memory \( m \) now refer to IMP² register and memory functions.

We define the semantics of IMP² with a large step operational semantics denoted by \( \Downarrow \). The judgment for the evaluation of commands has the following form is similar to the large step defined in Section 2.3.

\[ \mu \vdash (c, r, m, K) \bullet \Downarrow_\text{com} \ r'; m'; K' \triangleright t' \bullet \]

Most of the rules are similar to the semantics defined in Figure 3. Rule SQ-SEQ is a straightforward adaptation of the rule SEQ. Rule SQ-If-Div states that if the conditional evaluates to pair value, then the final configuration is the result of merging the corresponding configurations on each projection. Figures 14 defines the merge operation on locations, registers, traces and kill sets. Similarly, rules SQ-While-Div and SQ-Call-Div state that if the expression evaluates to a pair value, then the final configuration is the result of merging the corresponding configurations on each projection.

\[
\begin{align*}
\text{SQ-SEQ} & \quad \forall i \in \{1 \ldots z\}, \mu \vdash (c_i, r_{i-1}, m_{i-1}, K_{i-1}) \bullet \Downarrow_\text{com} r_i; m_i; K_i \triangleright t_i \bullet \\
\text{SQ-If-Div} & \quad \mu \vdash (c, r, m, K) \bullet \Downarrow_\text{exp} (v_0 \mid v_1) \quad c_{\text{left}} = (v_0 == 1)?c_0 : c_1 \\
& \quad \mu \vdash (c_{\text{right}} = (v_1 == 1)?c_0 : c_1 \\
& \quad \mu \vdash (c_{\text{left}}, [r_1, m_1, [K_1]]) \downarrow r'_1; m'_1; K_1 \triangleright t'_1 \\
& \quad \mu \vdash (c_{\text{right}}, [r_2, m_2, [K_2]]) \downarrow r'_2; m'_2; K_2 \triangleright t'_2 \\
& \quad \hat{r} = \text{merge}(r_1', r_2') \\
& \quad \hat{m} = \text{merge}(m_1', m_2') \\
& \quad \hat{t} = \text{merge}(t_1', t_2') \\
& \quad K = \text{merge}(K_1, K_2) \\
\text{SQ-While-Div} & \quad \mu \vdash (e, r, m, K) \bullet \Downarrow_\text{com} (i \leftarrow c; \text{if } c \text{ then } c_0 \text{ else } c_1) \bullet \\
& \quad \mu \vdash (c_{\text{left}}, [r_1, m_1, [K_1]]) \downarrow r'_1; m'_1; K_1 \triangleright t'_1 \\
& \quad \mu \vdash (c_{\text{right}}, [r_2, m_2, [K_2]]) \downarrow r'_2; m'_2; K_2 \triangleright t'_2 \\
& \quad \hat{r} = \text{merge}(r_1', r_2') \\
& \quad \hat{m} = \text{merge}(m_1', m_2') \\
& \quad \hat{t} = \text{merge}(t_1', t_2') \\
& \quad K = \text{merge}(K_1, K_2) \\
\text{SQ-Call-Div} & \quad \mu \vdash (\text{call}(e), r, m, K) \bullet \Downarrow_\text{com} c_1; \text{call}(e) \bullet \\
& \quad \mu \vdash (c_1, [r_1, m_1, [K_1]]) \downarrow r'_1; m'_1; K_1 \triangleright t'_1 \\
& \quad \mu \vdash (c_2, [r_2, m_2, [K_2]]) \downarrow r'_2; m'_2; K_2 \triangleright t'_2 \\
& \quad \hat{r} = \text{merge}(r_1', r_2') \\
& \quad \hat{m} = \text{merge}(m_1', m_2') \\
& \quad \hat{t} = \text{merge}(t_1', t_2') \\
& \quad K = \text{merge}(K_1, K_2) \\
& \quad \mu \vdash (\text{call}(e), r, m, K) \bullet \Downarrow_\text{com} i; \text{call}(e) \bullet \\
& \quad \mu \vdash (c_1, [r_1, m_1, [K_1]]) \downarrow r'_1; m'_1; K_1 \triangleright t'_1 \\
& \quad \mu \vdash (c_2, [r_2, m_2, [K_2]]) \downarrow r'_2; m'_2; K_2 \triangleright t'_2 \\
& \quad \hat{r} = \text{merge}(r_1', r_2') \\
& \quad \hat{m} = \text{merge}(m_1', m_2') \\
& \quad \hat{t} = \text{merge}(t_1', t_2') \\
& \quad K = \text{merge}(K_1, K_2) \\
& \quad \mu \vdash (\text{call}(e), r, m, K) \bullet \Downarrow_\text{com} i; \text{call}(e) \bullet
\end{align*}
\]

Figure 17 defines the projection on pairs of locations, registers, traces and kill sets for \( i \in \{1, 2\} \). Recall that \( \alpha \) ranges over events.

For notation simplicity, we define the command projection of an IMP² trace to represent the changes made by the attacker to the program in \( i^{\text{th}} \) projection.

\[ [t]_{i, \text{cmd}} = [\langle [t]_i \rangle_{\text{cmd}}] \]
merge\((m_1, m_2, l) = \begin{cases} v & \text{if } m_1(l) = m_2(l) = v \\ (v_1 \mid v_2) & \text{if } m_i(l) = v_i \text{ and } v_1 \neq v_2 \end{cases}\)

merge\((m_1, m_2) = m \mid \forall l \in \text{Loc. } m(l) = \text{merge}(m_1, m_2, l)\)

merge\((r_1, r_2, x) = \begin{cases} v & \text{if } r_1(x) = r_2(x) = v \\ (v_1 \mid v_2) & \text{if } r_i(x) = v_i \text{ and } v_1 \neq v_2 \end{cases}\)

merge\((r_1, r_2) = r \mid \forall x \in \text{Vars. } r(x) = \text{merge}(r_1, r_2, x)\)

merge\((t_1, t_2) = \begin{cases} (\alpha_1 \mid \alpha_2) \cdot \text{merge}(t_1', t_2') & \text{if } t_i = \alpha_i \cdot t_i' \land \alpha_i \neq \epsilon \\ (\alpha_1 \mid \epsilon) \cdot \text{merge}(t_1', \epsilon) & \text{if } t_1 = \alpha_1 \cdot t_1' \land \alpha_2 = \epsilon \\ (\epsilon \mid \alpha_2) \cdot \text{merge}(\epsilon, t_2') & \text{if } t_2 = \alpha_2 \cdot t_2' \land \alpha_1 = \epsilon \\ \epsilon & \text{o.w} \end{cases}\)

merge\((K_1, K_2) = (K_1|K_2)\)

**Figure 16.** Definition of merge

\(\lfloor r \rfloor_i(x) = \begin{cases} v & \text{if } r(x) = v \\ v_i & \text{if } r(x) = (v_1\mid v_2) \end{cases}\)

\(\lfloor m \rfloor_i(x) = \begin{cases} v & \text{if } m(x) = v \\ v_i & \text{if } m(x) = (v_1\mid v_2) \end{cases}\)

\(\lfloor t \rfloor_i = \begin{cases} \text{Mem}(\lfloor m \rfloor_i \cdot \lfloor t' \rfloor_i) & \text{if } t = \text{Mem}(m) \cdot t' \\ \text{Decl}(e, \lfloor m \rfloor_i \cdot \lfloor t' \rfloor_i) & \text{if } t = \text{Decl}(e, m) \cdot t' \\ \text{Out}(\ell, \lfloor v \rfloor_i) \cdot \lfloor t' \rfloor_i & \text{if } t = \text{Out}(\ell, v) \cdot t' \\ A(c) \cdot \lfloor t' \rfloor_i & \text{if } t = A(c) \cdot t' \\ A(c_1 \simeq c_2) \cdot \lfloor t' \rfloor_i & \text{if } t = A(c_1 \simeq c_2) \cdot t' \\ \alpha_1 \cdot \lfloor t' \rfloor_i & \text{if } t = (\alpha_1 \mid \alpha_2) \cdot t' \\ \epsilon & \text{o.w} \end{cases}\)

\(\lfloor K \rfloor_i = K_i \text{ if } K = (K_1|K_2)\)

\(\text{protected}(p, S) = \begin{cases} \text{true} & \text{if } p = H \text{ or } \top \\ \text{true} & \text{if } p = L \land \ell_2 \text{ and } \text{cnd} \in S \\ \text{true} & \text{if } p = \ell_1 \land \ell_2 \text{ and } \ell_1 \leq L \\ \text{false} & \text{o.w} \end{cases}\)

**Figure 17.** Definition of projections
E.1.1 Adequacy

The language IMPE\(^2\) is adequate for reasoning about executions of two IMPE programs. We show that execution of IMPE\(^2\) program is sound, (large-step by a IMPE\(^2\) program corresponds to large-steps taken by its projections) and complete (given two IMPE executions, there exists an IMPE\(^2\) execution).  

Lemma 1 (IMPE\(^2\) is Sound). If \(\mu \vdash \langle c, r, m, K \rangle \) \(\downarrow^*\) \(r^*; m^*; K^* \triangleright t^* \), then \(\mu \vdash \delta \langle c, [r]_i, [m]_i, [K]_i \rangle \downarrow [r^*]_i; [m^*]_i; [K^*]_i \triangleright [t^*]_i \) for \(i \in \{1, 2\} \).

Proof Sketch. Proof is by induction on the derivation of \(\mu \vdash \langle c, r, m, K \rangle \) \(\downarrow^2\) \(r^*; m^*; K^* \triangleright t^* \).

Lemma 2 (IMPE\(^2\) is Complete). If \(\mu \vdash \delta \langle c, [r]_i, [m]_i, [K]_i \rangle \downarrow r^*_i; m^*_i; K^*_i \triangleright t^*_i \), then \(\exists \langle r^*, m^*, K^*, t^* \rangle \) such that \(\mu \vdash \langle c, r, m, K \rangle \) \(\downarrow^2\) \(r^*; m^*; K^* \triangleright t^* \) and prove that we can construct \(r^*, m^*, K^* \) and \(t^* \) such that \(\langle [r^*]_i, [m^*]_i, [K^*]_i \rangle = \langle r^*_i, m^*_i, K^*_i, t^*_i \rangle \) for \(i \in \{1, 2\} \).

Interesting cases are SQ-IF-DIV, SQ-WHILE-DIV and SQ-CALL-DIV. We give intuition for SQ-IF-DIV, the rest follow the same argument.

Given \(\mu \vdash \delta \langle e \rangle \) then \(c_1 \) else \(c_2, [r]_i, [m]_i, [K]_i \) \(\downarrow r^*_i; m^*_i; K^*_i \triangleright t^*_i \). Let

\[ r^* = \text{merge}(r^*_1, r^*_2) \]
\[ m^* = \text{merge}(m^*_1, m^*_2) \]
\[ t^* = \text{merge}(t^*_1, t^*_2) \]
\[ K^* = \text{merge}(K^*_1, K^*_2) \]

From the premise of SQ-IF-DIV, we thus have \(\mu \vdash \langle c, r, m, K \rangle \) \(\downarrow^2\) \(r^*; m^*; K^* \triangleright t^* \).

E.1.2 IMPE\(^2\) Type System

Let \(S\) be the set of conditions set during some observed trace \(t_{obs}, \mathcal{H}\) be the set of escape hatches in the observed trace and \(\hat{m}_0\) be the initial IMPE\(^2\) memory. The IMPE\(^2\) type system is parametrized by \(\delta, S, \mathcal{H}\) and \(\hat{m}_0\). The typing judgment for commands and expressions is shown below.

\[ pc, \mu, \Gamma, K, U \vdash_{\delta S \mathcal{H} \hat{m}_0} c : \Gamma', K' \]
\[ \mu, \Gamma \vdash_{\delta S \mathcal{H} \hat{m}_0} e : \sigma_p \]

The typing rules are similar to Figure\(^8\) with 2 extra rules for typing configurations shown in Figure\(^18\). Rule T-SQ-CONFIG says that a configuration \(\langle c, r, m, K \rangle\) is well-typed (or is ok) if:

- Command \(c\) is well-typed;  
- all conditions in set \(U\) are unset;  
- Security policy on any register mapped to a paired value is protected;  
- Security policy on any location (that does not belong to the set of conditions) mapped to a paired value is protected;  
- evaluation of an escape hatch with current memory results in a value that is same as evaluating it with initial memory;  
- Kill sets are same on both sides of the executions.

Rule T-SQ-VALUE says when a final configuration \(\langle r, m, K \rangle\) is well-typed (or is ok) and is similar to rule T-SQ-CONFIG.

Lemma\(^3\) proves that if an IMPE program is well-typed according to IMPE type system, then for also well-typed according to IMPE\(^2\) type system.

Lemma 3 (Type System). If \(L, N, \Gamma, 0, 0 \vdash_{\delta} c : \Gamma', K' \), then \(pc, \mu, \Gamma, K, U \vdash_{\delta S \mathcal{H} \hat{m}_0} c : \Gamma', K' \).

Proof. Proof is by straight forward induction on the derivation of the typing judgment \(\mu, \Gamma \vdash_{\delta} e : \sigma_p \).

Lemma 4 (Value Type Preservation). If \(\mu, \Gamma \vdash_{\delta S \mathcal{H} \hat{m}_0} e : \sigma_p \) and \(\mu \vdash_{\delta} \langle e, r, m, K \rangle \) \(\downarrow^2\) \(v \), then \(\mu, \Gamma \vdash_{\delta S \mathcal{H} \hat{m}_0} v : \sigma_p \).

Proof. Proof is by straight forward induction on the derivation of the typing judgment \(\mu, \Gamma \vdash_{\delta S \mathcal{H} \hat{m}_0} e : \sigma_p \).
The proof is by induction on the derivation of the large-step evaluation. Both the lemmas are used for proving Theorem 1.

Lemma 5 (IMPE⁴ Final Configuration Preservation). Let \( \Gamma \) be an environment that is well-typed for \( \delta, H \) be the set of escape hatches and \( m_0 \) be the initial IMPE⁴ memory such that \( l \in \{ \text{locations}(e) | e \in H \}, m_0(l) \neq (v_1 | v_2) \), i.e., not a pair value. If \( pc, \mu, \Gamma, U \vdash_{\deltaSH_{m_0}} \langle e, r, m, K \rangle : \Gamma', K' \bullet \text{ok} \) and \( \mu \vdash \langle e, r, m, K \rangle : \psi_{\text{exp}} v \) such that \( \mu \vdash (e, r, m, K) : \psi_{\text{exp}} v \) and \( r' = r[x \mapsto v] \). We have to prove that \( \Gamma' \vdash_{\deltaSH_{m_0}} \langle r', m', K' \rangle \bullet \text{ok} \).

Proof. The proof is by induction on the derivation of the large-step evaluation. For each case, we prove that the final configuration preserves the well-typedness of IMPE⁴ value configuration.

Case \textbf{SQ-SKIP}: Given \( pc, \mu, \Gamma, U \vdash_{\deltaSH_{m_0}} \langle \text{skip}, r, m, K \rangle : \Gamma', K' \bullet \text{ok} \) and \( \mu \vdash \langle \text{skip}, r, m, K \rangle : \psi_{\text{com}} r; m \). Configuration is not changed.

Case \textbf{SQ-ASSIGN}: Given \( pc, \mu, \Gamma, U \vdash_{\deltaSH_{m_0}} \langle x := e, r, m, K \rangle : \Gamma', K' \bullet \text{ok} \) and \( \mu \vdash \langle x := e, r, m, K \rangle : \psi_{\text{com}} r; m \). Let \( v = (v_1 | v_2) \). If \( \mu \vdash (e, r, m, K) : \psi_{\text{exp}} v \) such that \( v \neq (v_1 | v_2) \) (not a pair value). Hence proved.

Case \textbf{SQ-DECLASSIFY}: Given \( pc, \mu, \Gamma, U \vdash_{\deltaSH_{m_0}} \langle \text{declassify}(x)e, r, m, K \rangle : \Gamma', K' \bullet \text{ok} \) and \( \mu \vdash \langle \text{declassify}(x)e, r, m, K \rangle : \psi_{\text{com}} r; m \). Let \( v = (v_1 | v_2) \). If \( \mu \vdash (e, r, m, K) : \psi_{\text{exp}} v \) such that \( v \neq (v_1 | v_2) \) (not a pair value). Hence proved.

Case \textbf{SQ-UPDATE}: Given \( pc, \mu, \Gamma, U \vdash_{\deltaSH_{m_0}} \langle e_1 \leftarrow e_2, r, m, K \rangle : \Gamma', K' \bullet \text{ok} \) and \( \mu \vdash \langle e_1 \leftarrow e_2, r, m, K \rangle : \psi_{\text{com}} r; m \). Let \( v = (v_1 | v_2) \). If \( \mu \vdash (e, r, m, K) : \psi_{\text{exp}} v \) such that \( v \neq (v_1 | v_2) \) (not a pair value). Hence proved.

Case \textbf{SQ-OUTPUT}: Given \( pc, \mu, \Gamma, U \vdash_{\deltaSH_{m_0}} \langle \text{output} e \leftarrow \ell, r, m, K \rangle : \Gamma', K' \bullet \text{ok} \) and \( \mu \vdash \langle \text{output} e \leftarrow \ell, r, m, K \rangle : \psi_{\text{com}} r; m \). Let \( v = (v_1 | v_2) \). From the premise of T-SQ-CONFIG, we have \( \Gamma \vdash_{\deltaSH_{m_0}} \langle r, m, K \rangle \bullet \text{ok} \). Hence proved.

Case \textbf{SQ-SETCND}: Given \( pc, \mu, \Gamma, U \vdash_{\deltaSH_{m_0}} \langle \text{set}(cnd), r, m, K \rangle : \Gamma', K' \bullet \text{ok} \) and \( \mu \vdash \langle \text{set}(cnd), r, m, K \rangle : \psi_{\text{com}} r; m \). Let \( v = (v_1 | v_2) \). From the premise of T-SQ-CONFIG, we have \( \Gamma \vdash_{\deltaSH_{m_0}} \langle r, m, K \rangle \bullet \text{ok} \). Large-step evaluation does not modify register file, memory or killset. Hence proved.

Figure 18. Typing IMPE⁴ configurations
of T-SQ-CONFIG, we have \( \Gamma \vdash_{\text{SH}^\text{ini}} (r, m, K) \cdot \text{ok} \). Since \( m \) and \( m' \) do not differ (set(cnd) always sets cnd to a non-pair value), we have \( \Gamma \vdash_{\text{SH}^\text{ini}} \). 

**Case SQ-KILL:** Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^\text{ini}} (\text{kill}(i), r, m, K) : \Gamma', K' \cdot \text{ok} \) and \( N \vdash_2 (\text{kill}(i), r, m, K) \cdot \downarrow_2 \text{com} r; m; K \cup \{E_i\} \triangleright \cdot \). We have to prove that \( \Gamma \vdash_{\text{SH}^\text{ini}} \). From the premise of T-SQ-CONFIG, we have \( \Gamma \vdash_{\text{SH}^\text{ini}} (r, m, K) \cdot \text{ok} \). Since \( \{K_i\} = \{K\}_2 \), we therefore have \( \{K \cup \{E_i\}\}_1 = \{K \cup \{E_i\}\}_2 \). Hence proved.

**Case SQ-SEQ:** Given \( pc, N, \mu, U \vdash_{\text{SH}^\text{ini}} (c_1; \ldots; c_n, \lambda_0, m, K_0) : \Gamma, K' \cdot \text{ok} \) and \( N \vdash_1 (c_1; \ldots; c_n, \lambda_0, m, K_0) \). We have to prove that \( \Gamma, \mu \vdash_{\text{SH}^\text{ini}} \). From the premise of T-NSQ-CONFIG, we have \( \Gamma, \mu \vdash_{\text{SH}^\text{ini}} \{r, m, n, K\} \cdot \text{ok} \). From the premise of T-NSQ-CONFIG, we have \( \Gamma, \mu \vdash_{\text{SH}^\text{ini}} \{r, m, n, K\} \cdot \text{ok} \). From the premise of T-NSQ-CONFIG, we have \( \Gamma, \mu \vdash_{\text{SH}^\text{ini}} \{r, m, n, K\} \cdot \text{ok} \). Since the types of locations are well-typed for \( \delta \) then \( \Gamma \) is also well-typed for \( \delta \). Applying induction hypothesis, we thus have \( \mu, \Gamma \vdash_{\text{SH}^\text{ini}} \{r_1, m_1, K_1\} \cdot \text{ok} \). Since the types of locations are well-typed for \( \delta \) then \( \Gamma \) is also well-typed for \( \delta \). Applying induction hypothesis continuously, we thus have \( \mu, \Gamma \vdash_{\text{SH}^\text{ini}} \{r, m, n, K\} \cdot \text{ok} \).

**Case S-Q-ENCLAVE:** Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^\text{ini}} (\text{enclave}(i, c), r, m, K) : \Gamma', K' \cdot \text{ok} \) and \( N \vdash (\text{enclave}(i, c), r, m, K) \). We have to prove that \( \Gamma \vdash_{\text{SH}^\text{ini}} \{r', m', K\} \cdot \text{ok} \). From the premise of T-SQ-CONFIG, we have \( \Gamma \vdash_{\text{SH}^\text{ini}} \{r', m', K\} \cdot \text{ok} \). So, \( E_1 \vdash (c, r, m, K) \). From the premise of T-NSQ-CONFIG, we have \( \Gamma \vdash_{\text{SH}^\text{ini}} \{r, m, n, K\} \cdot \text{ok} \). From the premise of T-NSQ-CONFIG, we have \( \Gamma \vdash_{\text{SH}^\text{ini}} \{r, m, n, K\} \cdot \text{ok} \). Since \( \{K_i\} = \{K\}_2 \), we therefore have \( \{K \cup \{E_i\}\}_1 = \{K \cup \{E_i\}\}_2 \). Hence proved.

**Case S-Q-IF-ELSE:** Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^\text{ini}} (\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) : \Gamma', K' \cdot \text{ok} \) and \( N \vdash (\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) \). We have to prove that \( \Gamma \vdash_{\text{SH}^\text{ini}} \{r', m', K\} \cdot \text{ok} \). From the premise of T-SQ-CONFIG, we have \( \Gamma \vdash_{\text{SH}^\text{ini}} \{r', m', K\} \cdot \text{ok} \). So, \( E_1 \vdash (c, r, m, K) \). From the premise of T-NSQ-CONFIG, we have \( \Gamma, c, \mu, U \vdash_{\text{SH}^\text{ini}} \{c, r, m, K\} : \Gamma', K' \cdot \text{ok} \). Also, \( E_1 \vdash (c, r, m, K) \). From the premise of T-NSQ-CONFIG, we have \( \Gamma \vdash_{\text{SH}^\text{ini}} \{c, r, m, K\} \cdot \text{ok} \). Since \( \{K_i\} = \{K\}_2 \), we therefore have \( \{K \cup \{E_i\}\}_1 = \{K \cup \{E_i\}\}_2 \). Hence proved.
Case SQ-CALL-DIV: Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^{\text{new}}} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \, \text{o.k} \) and \( \mu \vdash \langle \text{call}(e), r, m, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{t} \).

We have to prove that \( \Gamma \vdash_{\text{SH}^{\text{new}}} \langle \hat{r}, \hat{m}, K \rangle \, \text{o.k} \).

From the initial configuration, we have \( \Gamma \vdash_{\text{SH}^{\text{new}}} \langle r, m, K \rangle \, \text{o.k} \) and \( \mu \vdash \langle r, m, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{t} \).

Let \( z \) be such that \( \hat{r}(z) = (v_1 | v_2) \). If \( r(z) = (v_1 | v_2) \) and \( \Gamma(z) = \sigma_y \), then from the premise of T-Sq-CONF, we already have \( \text{protected}(y, S) \). If \( r(z) \neq (v_1 | v_2) \), then from the well-typedness \( p, \mu, \Gamma, K', U \vdash_{\text{SH}^{\text{new}}} c : \Gamma', K' \), we have \( \text{protected}(p, S) \) and \( \text{protected}(y, S) \) (because an assignment is at least as restrictive as \( p \)). Similarly, let \( \hat{m}(l) = (v_1 | v_2) \) and \( \Gamma(l) = \sigma_y \).

Since the type of location is invariant throughout the program, from the initial configuration we have \( \text{protected}(y, S) \). A well-typed escape hatch has immutable locations and thus evaluates to the same initial value. From the function type, post killsets are same.

Hence proved.

Lemma 6 (IMPE Type Preservation). Let \( \Gamma \) be a well-formed typing context and \( pc, \mu, \Gamma, U \vdash_{\text{SH}^{\text{new}}} \langle c, r, m, K \rangle : \Gamma', \Gamma' \, \text{o.k} \).

If \( \mu' \vdash \langle c', r', m', K' \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{t} \) is an immediate (command) premise in the evaluation of \( \mu \vdash \langle c, r, m, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{t} \), then \( \exists \hat{p}, \Gamma, \hat{t}, U \), such that \( pc \leq \hat{pc} \), either \( U \leq U \) or \( \hat{pc} \leq \hat{pc} \).

Proof. The proof is by induction on the derivation of the large step \( \mu \vdash \langle c, r, m, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{t} \).

Case SQ-ENCLAVE: Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^{\text{new}}} \langle \text{enclave}(i, c), r, m, K \rangle : \Gamma', \Gamma' \, \text{o.k} \).

From the premises of T-Sq-CONF, we have \( \Gamma \vdash_{\text{SH}^{\text{new}}} \langle r, m, K \rangle \, \text{o.k} \) and \( pc, \Gamma, K, \emptyset \vdash_{\text{SH}^{\text{new}}} c : \Gamma, \Gamma' \).

Case SQ-IF: Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^{\text{new}}} \langle \text{if} \, \text{then} \, c_1 \, \text{else} \, c_2, r, m, K \rangle : \Gamma', \Gamma' \, \text{o.k} \).

From the premises of the IMPE large-step, we have \( \mu \vdash \langle c_1, r, m, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m} \).

Case SQ-WHILE: Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^{\text{new}}} \langle \text{while} \, \text{do} \, c, r, m, K \rangle : \Gamma', \Gamma' \, \text{o.k} \).

From the premises of the IMPE large-step, we have \( \mu \vdash \langle c, r, m, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m} \).

Case SQ-CALL: Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^{\text{new}}} \langle \text{call}(e), r, m, K \rangle : \Gamma', \Gamma' \, \text{o.k} \).

From the premises of the IMPE large-step, we have \( \mu \vdash \langle e, r, m, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m} \).

Case SQ-SEQ: Given \( pc, \mu, \Gamma, U \vdash_{\text{SH}^{\text{new}}} \langle c_1, r_0, m_0, K_0 \rangle : \Gamma_n, \Gamma_n \, \text{o.k} \).

From the premises of the IMPE large-step, we have \( \mu \vdash \langle c_1, r_1, m_1, K_1 \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m} \).

Hence proved.

Using Lemma 5 and Lemma 6, we prove the first part of Theorem 1.

Proof. Given \( L, \mu, \Gamma, K, \emptyset \vdash c : \Gamma', \Gamma' \).

Let \( m_1 \) be some initial memory for which \( N \vdash \langle c, r_{\text{init}}, m_1, K \rangle \cdot \Downarrow^2_{\text{com}} \hat{r}; \hat{m} \).

The attacker actually observes only low-events i.e., \( \{ t_{\text{obs}} \}_{L} \).

We need to show that

\[
\downarrow^k_{L}(c, t_{\text{obs}}) \geq M
\]
where

\[
M = \left( \bigcap_{m' \in [t_{obs}]} \text{mem} \right) \cap \left( e', m' \in [t_{obs}]_{exec} \right) \cap \text{ObsOverlap}(m_0, m', e')
\]

Let \( S \) be the set of conditions that are set at the beginning of \( t_{obs} \), i.e., \( S = \{ \text{cnd} \mid m'(\text{cnd}) = 0 \} \). If \( Q \setminus S \) is the set of conditions that are unset at some time during the observed trace. Also let \( H \) be the set of all escape hatches that are declassified till the last event of \( t_{obs} \). i.e. \( H = \{ e \mid (e, m) \in [t \cdot t_{obs}]_{exec} \} \).

Let \( m_2 \in M \). Also let \( N \vdash \delta \langle c, r_{init}, m_2, K \rangle \not\downarrow r'_{2}; m'_2; K'_2 \triangleright t_2 \). To ensure \( k_L^q(c, t_{obs}) \geq M \), we need to show that \( m_2 \in k_L^q(c, t_{obs}) \).

Note that \( m_1 \) and \( m_2 \) differ only in locations with policies that are protected by set \( S \). That is, for all locations \( l \in \text{Loc} \), if \( m_1(l) \neq m_2(l) \) then \( l = \sigma_p \implies \text{protected}(p, S) \).

Also note that \( m_1 \) and \( m_2 \) satisfy

\[
\forall e \in H, \mu \vdash \delta \langle c, r_{init}, m_1, K \rangle \not\downarrow v \iff \mu \vdash \delta \langle c, r, m_2, K \rangle \not\downarrow v
\]

We will construct an IMPE\(^2\) execution that represents the IMPE executions starting from \( m_0 \) and \( m_2 \). Type-preservation of IMPE\(^2\) (Lemma 5) will ensure that both executions produce the same observable trace, thus showing that \( m_2 \in k_L^q(c, t_{obs}) \).

Let IMPE\(^2\) memory \( m = \text{merge}(m_1, m_2) \). If \( \mu \vdash \langle c, r_{init}, m, K \rangle \not\triangleright \text{r}_2*; m_*; K \triangleright t_* \), by the adequacy of IMPE\(^2\) (Lemma 2), we have that the IMPE\(^2\) execution represents IMPE executions with \( m_1 \) and \( m_2 \) as initial memories.

Let \( t^* = t^*_{\text{pre}} \cdot t^*_{\text{obs}} \cdot t^*_{\text{post}} \) for some \( t_{\text{obs}} \) such that \( \{ t^*_{\text{obs}} \}_1 = t_{obs} \). Define observation overlapped by an IMPE\(^2\) trace \( t^* \) as:

\[
\text{obsOverlap}(t^*, t^*_{\text{pre}}, t^*_{\text{obs}}, t^*_{\text{post}}) = \begin{cases} 
\text{obsOverlap}(t^*, t^*_{\text{pre}}, t^*_{\text{obs}}, t^*_{\text{post}}) & \text{if } t^* \leq t^*_{\text{obs}} \\
 t^*_{\text{obs}} & \text{if } t^*_{\text{pre}} \cdot t^*_{\text{obs}} \leq t^* \leq t^*_{\text{post}} \\
 t^*_{\text{post}} & \text{if } t^* \leq t^*_{\text{pre}} \cdot t^*_{\text{obs}} \text{ and } t^*_{\text{pre}} \cdot t^*_{\text{obs}} \leq t^*_{\text{post}} 
\end{cases}
\]

Intuitively, \( \text{obsOverlap}(t^*, t^*_{\text{pre}}, t^*_{\text{obs}}, t^*_{\text{post}}) \) defines part of input trace \( t^* \) that overlaps with an observed trace \( t^*_{\text{obs}} \).

Since \( L, \mu, \Gamma, K, \emptyset \triangleright \gamma \text{ e : } \Gamma', K' \), we have \( L, \mu, \Gamma, K, \emptyset \triangleright \text{set}(\text{non-zero}) \text{ e : } \Gamma', K' \). Note that our initial configuration satisfies

\[
L, N, \Gamma, K, \emptyset \triangleright \gamma \text{ e : } \Gamma', K', \bullet \text{ok}
\]

Lemma 7 (Observational Equivalence is Preserved). Let \( S \) be the set of conditions that are set(non-zero) in some observed trace \( t_{\text{obs}} \). If \( pc, \mu, \Gamma, U \triangleright \gamma \text{ e : } \Gamma', K' \) \( \text{ok and } \mu \vdash \langle c, r, m, K \rangle \not\triangleright \text{r}_2*; m_*; K \triangleright t_* \), then

\[
[ \text{obsOverlap}(\delta, t^*_{\text{pre}}, t^*_{\text{obs}}, t^*_{\text{post}}) ]_1 \approx_L \text{obsOverlap}(\delta, t^*_{\text{pre}}, t^*_{\text{obs}}, t^*_{\text{post}}) ]_2
\]

**Proof.** The proof follows by induction on the derivation of \( \mu \vdash \langle c, r, m, K \rangle \not\triangleright \text{r}_2*; m_*; K \triangleright t_* \).

**Case Sq-Skip:** Emitted trace is empty.

**Case Sq-Assign:** Emitted trace is empty.

**Case Sq-Declassify:** Emitted trace does not include \textit{out} event.

**Case Sq-Update:** Emitted trace is empty.

**Case Sq-SetCnd:** Emitted trace does not include \textit{out} event.

**Case Sq-Output:** Given \( pc, \mu, \Gamma, U \triangleright \gamma \text{ e : } \Gamma', K' \) \( \text{ok and } \mu \vdash \langle c, r, m, K \rangle \not\triangleright \text{r}_2*; m_*; K \triangleright \text{Mem}(m) \cdot \text{Out}(\ell, v) \). Let \( \ell = \text{Mem}(m) \cdot \text{Out}(\ell, v) \). From the premise of T-Sq-CONFIG, we have \( pc, \mu, \Gamma, K, U \triangleright \gamma \) output \( e \) to \( \ell : \Gamma, K' \) and so \( \mu, \gamma \triangleright \gamma \text{ e : } \sigma_p \) and \( \text{cur}(p, U) \cup \text{cur}(pc, U) \subset \ell \).

**Case v = (v_1 \mid v_2):** We have \( \text{protected}(p, S) \) and so \( \ell \neq L \).

**Case v \neq (v_1 \mid v_2):** In this case \( \ell = \{L, H\} \).
In both the cases, we have
\[
|\text{obsOverlap}(\hat{t}, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverlap}(\hat{t}, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

**Case Sq-If-Else:** Given \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) : \Gamma', K'\hat{\cdot}ok\) and \(\mu \vdash (e, r, m, K) \downarrow v\) such that \(v\) is not a pair, applying induction hypothesis to the premises of SQ-IF-ELSE gives us
\[
|\text{obsOverlap}(\hat{t}, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

**Case Sq-While:** Given \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{while } e \text{ do } c, r, m, K) : \Gamma, K \cdot ok\) and \(\mu \vdash (e, r, m, K) \downarrow v\) such that \(v\) is not a pair, applying induction hypothesis to the premises of SQ-WHILE gives us
\[
|\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

From Lemma 6 we have \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{while } e \text{ do } c', r, m', K) : \Gamma, K \cdot ok\). Applying induction hypothesis to \(\mu \vdash (e, r, m, K) \downarrow v\) such that \(v\) is not a pair, we have \text{protected}(p, S)\). From the well-typedness, \(c_1\) and \(c_2\) do not emit any \textit{out} events to \(L\) channel. Hence
\[
|\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

**Case Sq-Call:** Given \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{call}(e), r, m, K) : \Gamma', K'\hat{\cdot}ok\) and \(\mu \vdash (\text{call}(e), r, m, K) \downarrow v\) such that \(v\) is not a pair, applying induction hypothesis to the premises of SQ-CALL gives us
\[
|\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

**Case Sq-If-Div:** Given \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) \downarrow \hat{\cdot}K'\hat{\cdot}\hat{\cdot}\). From the premises of T-SQ-CONFIG, we have \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) \downarrow v\) such that \(v\) is not a pair, we have \text{protected}(p, S)\). From the well-typedness, \(c_1\) and \(c_2\) do not emit any \textit{out} events to \(L\) channel. Hence
\[
|\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

**Case Sq-While-Div:** Given \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{while } e \text{ do } c, r, m, K) : \Gamma, K \cdot ok\) and \(\mu \vdash (e, r, m, K) \downarrow v\) such that \(v\) is not a pair, we have \text{protected}(p, S)\). From the well-typedness, \(c_1\) does not emit any \textit{out} events to \(L\) channel. Hence
\[
|\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

**Case Sq-Call-Div:** Given \(pc, \mu, \Gamma, U \vdash_{\text{SH}_\\text{Hrio}}(\text{call}(e), r, m, K) : \Gamma', K'\hat{\cdot}ok\) and \(\mu \vdash (\text{call}(e), r, m, K) \downarrow v\) such that \(v\) is not a pair, we have \text{protected}(p, S)\). From the well-typedness, \(c_1\) does not emit any \textit{out} events to \(L\) channel. Hence
\[
|\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}', t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

**Case Sq-Seq:** Given \(pc, \mu, \Gamma_0, U \vdash_{\text{SH}_\\text{Hrio}}(c_1 \ldots c_n : r_n, m_0, K_0) : \Gamma_n, K_n \cdot ok\) and \(\mu \vdash (c_1 \ldots c_n : r_n, m_0, K_0) \downarrow r_n ; m_n ; K_0 \vdash t_1 \ldots t_n\). From the premises of T-SQ-CONFIG, we have \(pc, \mu, \Gamma_0, U \vdash_{\text{SH}_\\text{Hrio}}(c_1 \ldots c_n : r_n, m_0, K_0) \downarrow v\) applying induction hypothesis to the premise, \(\mu \vdash (c_1 \vdots t_0, m_0, K_0) \downarrow v\) we have
\[
|\text{obsOverflow}(\hat{t}_1, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}_1, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

From Lemma 6 we have \(pc, \mu_1 , \Gamma_1, U \vdash_{\text{SH}_\\text{Hrio}}(c_2, r_1, m_1, K_1) : \Gamma_2, K_2 \cdot ok\). Applying induction hypothesis to the next premise, \(\mu \vdash (c_2, r_1, m_1, K_1) \downarrow v\) we have
\[
|\text{obsOverflow}(\hat{t}_2, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}_2, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]

Applying the inductive hypothesis continuously thus gives,
\[
|\text{obsOverflow}(\hat{t}_n, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_1| \approx_L |\text{obsOverflow}(\hat{t}_n, t_{\text{pre}}', t_{\text{obs}}', t_{\text{post}}')_2|
\]
Case Sq-Enclave: Given \( pc, p, \Gamma, U \vdash_{\delta} S_{\text{Hinio}} (\text{enclave}(i,c), r, m, K) : \Gamma', K' \oplus ok \) and \( N \vdash_{\delta} (\text{enclave}(i,c), r, m, K) \downarrow r' \); \( m' ; K' \triangleright t' \). From the premises of T-Sq-CONFIG, we have \( pc, p, \Gamma, K, U \vdash_{\delta} S_{\text{Hinio}} \text{enclave}(i,c) : \Gamma', K' \). From Lemma 6, we have \( pc, E_i, \Gamma, 0 \vdash_{\delta} S_{\text{Hinio}} (c, r, m, K) : \Gamma', K' \oplus ok \). Applying induction hypothesis to the premise \( E_i \vdash_{\delta} (c, r, m, K) \downarrow r' ; m' ; K' \triangleright t' \):

\[
[\text{obsOverlap}(t', t'_{\text{pre}}, t'_{\text{obs}}, t'_{\text{post}})]_1 \approx_L [\text{obsOverlap}(t', t'_{\text{pre}}, t'_{\text{obs}}, t'_{\text{post}})]_2
\]

Since we have \( L, N, \Gamma, 0 \vdash_{\delta} S_{\text{Hinio}} (c, r, m, 0) : \Gamma', K' \oplus ok \), applying Lemma 7 on \( \mu \vdash (c, r, m, K) \oplus \delta \) \( r'; m'; K' \triangleright t' \), we have

\[
[\text{obsOverlap}(t', t'_{\text{pre}}, t'_{\text{obs}}, t'_{\text{post}})]_1 \approx_L [\text{obsOverlap}(t', t'_{\text{pre}}, t'_{\text{obs}}, t'_{\text{post}})]_2
\]

Hence proved that \( m_2 \in k_L^2(c, t_{\text{obs}}) \).

We prove the second and third parts of Theorem 1 using similar approaches in Section E.1.3 and Section E.1.6.

E.1.3 Proofs for N-chaos Security

In this section we use a more permissive N-chaos type system and show that an IMPE program that is well-typed for the type system in Section 4 is also well-typed for N-chaos type system. Figure 19 presents the N-chaos type system. It relaxes the IMPE type system by unconstraining the commands running in normal mode. They can now read and write to memory locations with no restrictions on security policies. The new typing system relies on the guarantees provided by the operational semantics that a command running in normal mode does not access enclave memory. Typing rules for commands running in enclave mode are unchanged and are same as those presented in Figure 8.

Lemma 8 (Permissive Type System). If \( L, N, \Gamma, 0 \vdash_{\delta} c : \Gamma', K' \), then \( pc, p, \Gamma, K, U \vdash_{\delta \text{N}-\text{chaos}} c : \Gamma', K' \).

Proof Sketch. Proof is by straightforward induction on the derivation of the typing judgment \( \mu, \Gamma \vdash_{\delta} c : \sigma_p \).

E.1.4 IMPE\(^{2N-\text{chaos}}\) Adequacy

The language IMPE\(^{2N-\text{chaos}}\) is adequate for reasoning about executions of two IMPE programs. We show that the execution of IMPE\(^{2N-\text{chaos}}\) program using semantics \( \downarrow^2_{\text{N-chaos}} \) is sound (i.e., large-step taken by an IMPE\(^{2N-\text{chaos}}\) program corresponds to a large-step taken by either side of the execution) and complete (given two IMPE N-chaos executions, there exists an IMPE\(^{2N-\text{chaos}}\) execution).

Lemma 9 (IMPE\(^{2N-\text{chaos}}\) is Sound). If \( \mu \vdash (c, r, m, K) \oplus \downarrow^2_{\text{N-chaos}} r'; m'; K' \triangleright t' \), then \( \mu \vdash (c, r, m, K) \oplus \downarrow^2_{\text{N-chaos}} [r'; i]_j : [m']_j, [K']_j \triangleright [t']_j \) for \( i \in \{ 1, 2 \} \).

Proof Sketch. Proof is by induction on the derivation of \( \mu \vdash (c, r, m, K) \oplus \downarrow^2_{\text{com}} r'; m'; K' \triangleright t' \).

Lemma 10 (IMPE\(^{2N-\text{chaos}}\) is Complete). Let \( \mu \vdash (c, r, m, K) \oplus \downarrow^2_{\text{N-chaos}} r'; m'; K' \triangleright t' \) such that \( \downarrow^2_{\text{N-chaos}} t'_1 \) cmd = \( \downarrow^2_{\text{N-chaos}} t'_1 \) cmd. Then \( \exists (r^*, m^*, K^*, t^*) \), such that \( \mu \vdash (c, r, m, K) \oplus \downarrow^2_{\text{N-chaos}} r^*; m^*; K^* \triangleright t^* \) and \( \downarrow^2_{\text{N-chaos}} ([r^*], [m^*], [K^*], [t^*]) = ([r^*_i], [m^*_i], [K^*_i], [t^*_i]) \) for \( i \in \{ 1, 2 \} \).

Proof Sketch. Follows along the lines of proof of Lemma 2.

E.1.5 IMPE\(^{2N-\text{chaos}}\) N-chaos Type System

Let \( S \) be the set of conditions set during some observed trace \( t_{\text{obs}} \), \( H \) be the set of escape hatches till the observed trace and \( m_0 \) be the initial IMPE\(^{2N-\text{chaos}}\) memory. The IMPE\(^{2N-\text{chaos}}\) type system is parametrized by \( \delta, S, H \) and \( m_0 \). The typing judgment for commands and expressions is shown below.

\[
pc, \Gamma, U \vdash_{\delta} S_{\text{HinioN-chaos}} c : \Gamma', K'
\]

\[
\mu, \Gamma \vdash_{\delta} S_{\text{HinioN-chaos}} c : \sigma_p
\]

The typing rules are similar to Figure 19 with 2 extra rules for typing configurations shown in Figure 20.

Lemma 11 (Value Type Preservation). If \( \mu, \Gamma \vdash_{\delta} S_{\text{HinioN-chaos}} c : \sigma_p \) and \( \mu \vdash (c, r, m, K) \oplus \downarrow^2_{\text{N-chaos}} v \), then \( pc, \mu, \Gamma, K, U \vdash_{\delta} S_{\text{HinioN-chaos}} c : \Gamma', K' \).
Proof Sketch. Proof is by straightforward induction on the derivation of the typing judgment \( \mu, \Gamma \vdash_{\delta \text{N-ch}} e : \sigma_p \).

Lemma 12 (Protected Expression). Let \( \mu, \Gamma \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} (r, m, K) \) ok. If \( \mu, \Gamma \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} e : \sigma_p \) and \( \mu \vdash (c, r, m, K) \) \( \Downarrow^2 \text{N-ch} \) \( v \) such that \( v = (v_1 | v_2) \) for some values \( v_1 \) and \( v_2 \), then \( \text{protected}(p, S) \) and \( \mu \neq N \).

Proof Sketch. Proof is by straightforward induction on the derivation of the typing judgment \( \mu, \Gamma \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} e : \sigma_p \).

Lemma 13 (IMPE\textsuperscript{2N-ch} N-chaos Final Configuration Preservation). Let \( \Gamma \) be an environment well-typed for \( \delta, H \) be the set of escape hatches and \( \mu_0 \) be the initial IMPE\textsuperscript{2N-ch} memory such that \( l \in \{\text{locations}(e) | e \in H\} \), \( \mu_0(l) \neq (v_1 | v_2) \), i.e., not a pair value. If \( pc, \mu, \Gamma, U \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} (c, r, m, K) \) \( \Downarrow^2 \text{N-ch} \) \( r' ; m' ; K' \) \( \triangleright \) \( t' \bullet \), then \( \mu, \Gamma, U \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} (r', m', K') \) ok.

Proof. The proof is by induction on the derivation of the large step \( \mu \vdash (c, r, m, K) \) \( \Downarrow^2 \text{N-ch} \) \( r' ; m' ; K' \) \( \triangleright \) \( t' \bullet \). For each case, we prove that the final configuration preserves the well-typedness of IMPE\textsuperscript{2N-ch} value configuration.

Case NSQ-Skip: Given \( pc, \mu, \Gamma, U \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} \langle \text{skip}, r, m, K \rangle \) \( \Downarrow^2 \text{N-ch} \) \( r ; m ; K \triangleright \bullet \). Configuration is not changed.

Case NSQ-Assign: Given \( pc, \mu, \Gamma, U \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} \langle x := e, r, m, K \rangle \) \( \Downarrow^2 \text{N-ch} \) \( v \) and \( \mu \vdash (c, r, m, K) \) \( \Downarrow^2 \text{N-ch} \) \( r' ; m ; K' \) \( \triangleright \) \( t' \bullet \) such that \( \mu \vdash (c, r, m, K) \) \( \Downarrow^2 \text{N-ch} \) \( v \) and \( r' = r[x \mapsto v] \). We have to prove that \( \mu, \Gamma' \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} (r', m, K) \) ok. From the initial configuration, we have \( \mu, \Gamma, U \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} (r, m, K) \) ok. Register files \( r \) and \( r' \) differ only in variable \( x \). Let \( v = (v_1 | v_2) \). From the well-typedness, we have \( \mu, \Gamma, U \vdash_{\delta \text{SH} \mu_0 \text{N-ch}} e : \sigma_p \). Applying Lemma 12 we have \( \text{protected}(p, S) \) and \( \mu \neq N \). Since \( \Gamma' = \Gamma[x \mapsto \sigma_{p \cup q, S}] \), we have \( \text{protected}(pc \cup q, S) \). Hence proved.
Given \( pc, \mu, \Gamma, K, U : \delta_{\text{MemNoCh}} \) \( c : \Gamma', K' \)

\[ \forall e : \text{Var}, r(x) = (v_1 | v_2) \text{ and } \Gamma(x) = \sigma_p \rightarrow \text{protected}(p, S) \text{ and } \mu \neq N \]

\[ \forall l \in \text{Loc} \setminus \text{Cond}, m(l) = (v_1 | v_2) \text{ and } \Gamma(l) = (\sigma_p, rt) \rightarrow \text{protected}(p, S) \text{ and } \delta(l) \neq N \]

\[ \forall e \in \mathcal{H}, \mu \vdash \langle e, r_{\text{init}}, m_0, K \rangle : \downarrow^2_{\text{chaos}} v \rightarrow \mu \vdash \langle e, r, m, K \rangle : \downarrow^2_{\text{chaos}} v \]

\[ \left[ K \right]_1 = [K]_2 \]

\text{T-NSQ-CONFIG}

\[ pc, \mu, \Gamma, U : \delta_{\text{MemNoCh}} \langle c, r, m, K \rangle : \Gamma' \bullet ok \]

\[ \forall e : \text{Var}, r(x) = (v_1 | v_2) \text{ and } \Gamma(x) = \sigma_p \rightarrow \text{protected}(p, S) \text{ and } \mu \neq N \]

\[ \forall l \in \text{Loc} \setminus \text{Cond}, m(l) = (v_1 | v_2) \text{ and } \Gamma(l) = (\sigma_p, rt) \rightarrow \text{protected}(p, S) \text{ and } \delta(l) \neq N \]

\[ \forall e \in \mathcal{H}, \mu \vdash \langle e, r_{\text{init}}, m_0, K \rangle : \downarrow^2_{\text{chaos}} v \rightarrow \mu \vdash \langle e, r, m, K \rangle : \downarrow^2_{\text{chaos}} v \]

\[ \left[ K \right]_1 = [K]_2 \]

\text{T-NSQ-VALUE}

\[ \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m, K \rangle \bullet ok \]

\[ \text{Figure 20. } N\text{-chaos Typing IMPe}^{2N\text{-chaos}} \text{ configurations} \]

\textbf{Case NSQ-DECLASSIFY:} Given \( pc, \mu, \Gamma, U \vdash \delta_{\text{MemNoCh}} \langle \text{declassify}(x)e, r, m, K \rangle : \Gamma' \bullet ok \) and \( \mu \vdash \langle \text{declassify}(x)e, r, m, K \rangle : \downarrow^2_{\text{chaos}} r'; m \vdash e \bullet \) such that \( \mu \vdash \langle e, r, m, K \rangle : \downarrow^2_{\text{chaos}} v \) and \( m' = m[l \rightarrow v] \). Also expression e has no variables syntactically present (large-step has the premise hasNoVars(e)). We have to prove that \( \mu, \Gamma' \vdash \delta_{\text{MemNoCh}} \langle r', m, K \rangle \bullet ok \).

From the initial configuration, we have \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m, K \rangle \bullet ok \). Register files r and r’ differ only for variable x. Let \( v = (v_1 | v_2) \) for some \( v_1 \) and \( v_2 \). We have \( \Gamma' = \Gamma[x \rightarrow L] \). From the well-typedness, we have allLocImmutable(e). Thus \( e \in \mathcal{H} \) and so \( v \neq (v_1 | v_2) \) (not a pair value).

Hence proved.

\textbf{Case NSQ-UPDATE:} Given \( pc, \mu, \Gamma, U \vdash \delta_{\text{MemNoCh}} \langle e_1 \leftarrow e_2, r, m, K \rangle : \Gamma' \bullet ok \) and \( \mu \vdash \langle e_1 \leftarrow e_2, r, m, K \rangle : \downarrow^2_{\text{chaos}} r'; m \vdash e \bullet \) such that \( \mu \vdash \langle e_2, r, m, K \rangle : \downarrow^2_{\text{chaos}} v \) and \( m' = m[l \rightarrow v] \). We have to prove that \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m', K \rangle \bullet ok \).

From the premise of T-NSQ-CONFIG, we have \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m, K \rangle \bullet ok \), \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} e_1 : (\sigma^\mu_{\text{ref}}{^\Gamma})_q \) and \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} e_2 : \sigma' \) such that \( p' \cup q \cup p \leq p \).

\textbf{Case l (l1 | l2), v = (v1 | v2):} Applying Lemma [12] we have protected(p', S) and \( \mu \neq N \). So protected(p, S). Since \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} l : (\sigma^\mu_{\text{ref}}{^\Gamma})_L \), from the well-typedness of environment, we have \( \delta(l) = \mu' \neq N \). Hence \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m', K \rangle \bullet ok \).

\textbf{Case l = (l1 | l2), v = (v1 | v2):} Trivially \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m', K \rangle \bullet ok \).

\textbf{Case NSQ-OUTPUT:} Given \( pc, \mu, \Gamma, U \vdash \delta_{\text{MemNoCh}} \langle \text{output } e \rightarrow \ell, r, m, K \rangle : \Gamma' \bullet ok \) and \( \mu \vdash \langle \text{output } e \rightarrow \ell, r, m, K \rangle : \downarrow^2_{\text{chaos}} r; m \vdash \text{Mem}(m) \bullet \text{Out}(\ell, v) \bullet \) From the premise of T-NSQ-CONFIG, we have \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m, K \rangle \bullet ok \).

Large-step does not modify register file, memory or killset.

\textbf{Case NSQ-SETCN:} Given \( pc, \mu, \Gamma, U \vdash \delta_{\text{MemNoCh}} \langle \text{set}cnd, r, m, K \rangle : \Gamma' \bullet ok \) and \( \mu \vdash \langle \text{set}cnd, r, m, K \rangle : \downarrow^2_{\text{chaos}} r; m' ; K \vdash \text{Mem}(m') \bullet \) such that \( m' = m[c\text{nd} \rightarrow 1] \) We have to prove that \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m', K \rangle \bullet ok \). From the premise of T-NSQ-CONFIG, we have \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m, K \rangle \bullet ok \). Since \( m \) and \( m' \) do not differ (set(cnd) always sets cnd to a non-pair value), we have \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m', K \rangle \bullet ok \).

\textbf{Case NSQ-KILL:} Given \( pc, \mu, \Gamma, U \vdash \delta_{\text{MemNoCh}} \langle \text{kill}i, r, m, K \rangle : \Gamma' \bullet ok \) and \( N \vdash \langle \text{kill}i, r, m, K \rangle : \downarrow^2_{\text{chaos}} r; m; K \cup \{E_i\} \bullet \) We have to prove that \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m, K \cup \{E_i\} \rangle \bullet ok \). From the premise of T-NSQ-CONFIG, we have \( \mu, \Gamma \vdash \delta_{\text{MemNoCh}} \langle r, m, K \rangle \bullet ok \). Since \( [K]_1 = [K]_2 \), we therefore have \( [K \cup \{E_i\}]_1 = [K \cup \{E_i\}]_2 \). Hence proved.

\textbf{Case NSQ-SEQ:} Given \( pc, N, \Gamma, U \vdash \delta_{\text{MemNoCh}} \langle \ldots, c\text{nd}, r_0, m_0, K_0 \rangle : \Gamma' \bullet ok \) and \( N \vdash \langle \ldots, c\text{nd}, r_0, m_0, K_0 \rangle : \downarrow^2_{\text{chaos}} r_n; m_n; K_n \rangle \bullet n \) We have to prove that \( \mu, \Gamma_0 \vdash \delta_{\text{MemNoCh}} \langle r_n, m_n, K_0 \rangle \bullet ok \). From the premise of T-NSQ-CONFIG, we have \( \mu, \Gamma_0 \vdash \delta_{\text{MemNoCh}} \langle r_0, m_0, K_0 \rangle \bullet ok \) and \( pc, \mu, \Gamma_0, \Gamma_{i-1}, \Gamma_i \vdash \delta_{\text{MemNoCh}} c_i : \Gamma_i, K_i \) for \( i \in \{1 \ldots n\} \). Applying induction hypothesis, we thus have \( \mu, \Gamma_1 \vdash \delta_{\text{MemNoCh}} \langle r_1, m_1, K_1 \rangle \bullet ok \). Since the types of locations are fixed throughout the program, we have that if \( \Gamma_0 \) is well-typed for \( \delta \) then \( \Gamma_1 \) is also well-typed for \( \delta \). Applying induction hypothesis continuously, we thus have \( N, \Gamma_n \vdash \delta_{\text{MemNoCh}} \langle r_n, m_n, K_n \rangle \bullet ok \).
Case NSQ-ENCLAVE: Given \(pc, N, \Gamma, U \vdash_{\text{SHtnoNch}} \langle \text{enclave}(i, c), r, m, K \rangle \vdash \Gamma \bullet \text{ok} \) and \(N \vdash \langle \text{enclave}(i, c), r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). From the premise of T-NSQ-CONFIG, we have \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r, m, K \rangle \bullet \text{ok}\) and \(pc, E_i, \Gamma, K, \emptyset \vdash_{\text{SHtnoNch}} c : \Gamma' \vdash K'.\) So, \(pc, E_i, \Gamma, K, \emptyset \vdash_{\text{SHtnoNch}} (c, r, m, K) \vdash \Gamma \bullet \text{ok}.\) Also, \(E_i \vdash \langle c, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). Applying induction hypothesis, we thus have \(E_i, \Gamma \vdash_{\text{SHtnoNch}} \langle r', m', K' \rangle \bullet \text{ok}\). Hence \(N, \Gamma \vdash_{\text{SHtnoNch}} \langle r', m', K' \rangle \bullet \text{ok}\).

Case NSQ-IF-ELSE: Given \(pc, \mu, \Gamma, U \vdash_{\text{SHtnoNch}} (if \ e \ then \ c_1 \ else \ c_2, r, m, K) \vdash \Gamma \bullet \text{ok}\) and \(\mu \vdash \langle e \ then \ c_1 \ else \ c_2, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). From the premise of T-NSQ-CONFIG, we have \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r, m, K \rangle \bullet \text{ok}\) and \(pc, \mu, \Gamma, U \vdash_{\text{SHtnoNch}} (c_i, r, m, K) \vdash \Gamma \bullet \text{ok}\). Also, \(\mu \vdash \langle c_i, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). Applying induction hypothesis to the premise \(\mu \vdash \langle c_i, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\), we thus have \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r', m', K' \rangle \bullet \text{ok}\).

Case NSQ-WHILE: Given \(pc, \mu, \Gamma, U \vdash_{\text{SHtnoNch}} (while \ d \ e \ c, r, m, K) \vdash \Gamma \bullet \text{ok}\) and \(\mu \vdash \langle while \ d \ e \ c, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). From the premise of T-NSQ-CONFIG, we have \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r, m, K \rangle \bullet \text{ok}\) and \(pc, \mu, \Gamma, U \vdash_{\text{SHtnoNch}} (c, r, m, K) \vdash \Gamma \bullet \text{ok}\). Also, \(\mu \vdash \langle c, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). Applying induction hypothesis to the premise \(\mu \vdash \langle c, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\), we thus have \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r', m', K' \rangle \bullet \text{ok}\). From the well-typedness, we have \(K = K' = K''\).

Case NSQ-CALL: Given \(pc, \mu, \Gamma, U \vdash_{\text{SHtnoNch}} (call(e), r, m, K) \vdash \Gamma \bullet \text{ok}\) and \(\mu \vdash \langle call(e), r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). From the premise of T-NSQ-CONFIG, we have \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r, m, K \rangle \bullet \text{ok}\) and \(pc, \mu, \Gamma, K, U \vdash_{\text{SHtnoNch}} (e, r, m, K) \vdash \Gamma \bullet \text{ok}\). Also, \(\mu \vdash \langle e, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). Applying induction hypothesis to the premise \(\mu \vdash \langle e, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\), we thus have \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r', m', K' \rangle \bullet \text{ok}\). From the well-typedness, we have \(K = K' = K''\).

Case NSQ-IF-DIV: Given \(pc, \mu, \Gamma, U \vdash_{\text{SHtnoNch}} (if \ e \ then \ c_0 \ else \ c_1, r, m, K) \vdash \Gamma \bullet \text{ok}\) and \(\mu \vdash \langle if \ e \ then \ c_0 \ else \ c_1, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). From the initial configuration, we have \(pc, \mu, \Gamma, K, U \vdash_{\text{SHtnoNch}} c_0 : \Gamma', \mu, \Gamma, \emptyset : \text{int}_{p} \). From the premise of NSQ-IF-DIV, we have \(\mu \vdash \langle c, r, m, K \rangle \vdash \Gamma \bullet \text{ok}\). Let \(z \) be such that \(r(z) = (v_1 | v_2)\). If \(\Gamma(z) = \sigma_g\), then either \(\Gamma(z) = \sigma_g\) or there is an assignment to \(z\) in \(c_i\) for some \(i = \{0, 1\}\). If the former holds, then we already have \(\text{protected}(q, S)\). If the latter holds, then we have \(\text{protected}(q, S)\) (because an assignment is at least as restrictive as \(p_{e} \)).

Let \(m = (v_1 | v_2)\) and \(\Gamma(l) = \sigma_g\). Since the type of location is invariant throughout the program, from the initial configuration we have \(\text{protected}(q, S)\). A well-typed escape hatch has immutable locations and thus evaluates to the same initial value.

Since, both branches \(c_0\) and \(c_1\) have same killsets, we have \(K_1 = K_2\). So \([K_1] = [K_2]\). Hence \(\mu, \Gamma \vdash_{\text{SHtnoNch}} \langle r, m, K \rangle \vdash \Gamma \bullet \text{ok}\).
of NSQ-CALL-DIV, we have $\mu \vdash \langle e, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 (v_0 | v_1)$. So $\mu \neq N$, protected($q$, $S$) and since $q \leq p$, protected($p$, $S$) follows.

Let $z$ be such that $\bar{r}(z) = (v_1 | v_2)$. If $r(z) = (v_1 | v_2)$ and $\Gamma(z) = \sigma_y$, then from the premise of T-NSQ-CONF, we already have protected($y$, $S$). If $r(z) \neq (v_1 | v_2)$ i.e., not a pair value, and $\Gamma(z) = \sigma_y$, then from the well-typedness $p, \mu, \gamma, K, \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} = \Gamma^c, K^*$, we have protected($p$, $S$) and so protected($y$, $S$) (because an assignment is at least as restrictive as $p$). Similarly, let $m(l) = (v_1 | v_2)$ and $\Gamma(l) = \sigma_y$. Since the type of location is invariant throughout the program, from the initial configuration we have protected($y$, $S$). A well-typed escape hatch has immutable locations and thus evaluates to the same initial value. From the function type, post kills sets are same. So $|\ubar{\delta}^1| = |\ubar{\delta}^2|$. Hence $\mu, \Gamma \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (r_i, m, K) \bullet \text{ok}$.

Hence proved.

\[
\text{Lemma 14 (IMPE}_{2N_{\text{chaos}}}^N - \text{chaos Type Preservation). Let } \Gamma \text{ be a well-formed typing context and } \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c, r, m, K) : \Gamma' \bullet \text{ok. If } \mu \vdash \langle c', r', m', K' \rangle \bullet \Downarrow N_{\text{chaos}}^2 r'; m'; K' \triangleright t' \bullet \text{ is an immediate (command) premise in the evaluation of } \mu \vdash \langle c, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 r; m; K \triangleright t \bullet, \text{ then } \exists \bar{p}\mu, \Gamma, t', U, \text{ such that } p \leq \bar{p}\delta, \text{ either } U \subseteq \bar{U} \text{ or } \bar{U} = \emptyset \text{ and } \bar{p}c, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c', r', m', K') : \Gamma' \bullet \text{ok.}
\]

Proof. The proof is by induction on the derivation of the large step $\mu \vdash \langle c, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 r; m; K \triangleright t \bullet$. Since rules NSQ-ASSIGN, NSQ-SKIP, NSQ-UPDATE, NSQ-KILL, NSQ-OUTPUT, NSQ-SETCND, NSQ-IF-DIV, NSQ-WHILE-DIV and NSQ-CALL-DIV do not have IMPE$_{2N_{\text{chaos}}}^N$ command premises, the only relevant cases are NSQ-ENCLAVE, NSQ-IF-ELSE, NSQ-SEQUENCE, NSQ-ENCLAVE, NSQ-IF-ELSE, NSQ-SEQUENCE.

Case NSQ-ENCLAVE: Given $\mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (\text{enclave}(i, c, r, m, K) : \Gamma', K' \bullet \text{ok. From the premises of T-NSQ-CONF, we have } \mu, \Gamma \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c, r, m, K) \bullet \text{ok and } pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c, r, m, K) : \Gamma' \bullet \text{ok. From the premises of the IMPE}_{2N_{\text{chaos}}}^N \text{ large-step, we have } E_i \vdash \langle c, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 r; m; K \triangleright t' \bullet. \text{ Hence } \mu, \Gamma, \bar{U} \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c', r', m', K') : \Gamma' \bullet \text{ok.}
\]

Case NSQ-IF-ELSE: Given $pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (i \text{ then } c_1 \text{ else } c_2, r, m, K) : \Gamma' \bullet \text{ok. From the premises of the IMPE}_{2N_{\text{chaos}}}^N \text{ large-step, we have } \mu \vdash \langle c_i, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 r; m; K' \triangleright t \bullet \text{. From the premises of T-NSQ-CONF, we have } \mu, \Gamma \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c, r, m, K) \bullet \text{ok and } pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c_i, r, m, K) : \Gamma' \bullet \text{ok. Note that if } e = \text{isuset}(\text{end}), \text{ then we have } pc', \mu, \Gamma, U \cup \{\text{end}\} \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c_1, r, m, K) : \Gamma' \bullet \text{ok and } pc', \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c_2, r, m, K) : \Gamma' \bullet \text{ok.}
\]

Case NSQ-WHILE: Given $pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (\text{while } e \text{ do } c', r, m, K) : \Gamma, K \bullet \text{ok. From the premises of the IMPE}_{2N_{\text{chaos}}}^N \text{ large-step, we have } \mu \vdash \langle c', r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 r'; m'; K' \triangleright t' \bullet \text{ and } \mu \vdash \langle c, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 r; m; K \triangleright t \bullet. \text{ We thus have } K = K' = K'' \text{ and } pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c', r, m, K) : \Gamma \bullet \text{ok. Applying Lemma 13 to } pc', \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c', r, m, K) : \Gamma \bullet \text{ok, we have } \mu, \Gamma \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (r', m', K') \bullet \text{ok. Hence } pc', \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c', r', m', K') : \Gamma' \bullet \text{ok.}
\]

Case NSQ-CALL: Given $pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (\text{call}(e), r, m, K) : \Gamma', K' \bullet \text{ok. From the premises of the IMPE}_{2N_{\text{chaos}}}^N \text{ large-step, we have } \mu \vdash \langle e, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 \lambda e. c \text{ and } \mu \vdash \langle e, r, m, K \rangle \bullet \Downarrow N_{\text{chaos}}^2 r; m; K' \triangleright t' \bullet. \text{ From the premises of T-NSQ-CONF, we have } K = K', K' = K'' \text{ and } \Gamma = \Gamma'. \text{ Also we have } pc, \mu, \Gamma, K', \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c, r, m, K) : \Gamma' \bullet \text{ok. Hence } pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c, r, m, K) : \Gamma' \bullet \text{ok.}
\]

Case NSQ-SEQ: Given $pc, \mu, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c_1, \ldots, c_n, r_0, m_0, K_0) : \Gamma_n, K_n \bullet \text{ok. From the premises of the IMPE}_{2N_{\text{chaos}}}^N \text{ large-step, we have } \mu \vdash \langle c_i, r_{i-1}, m_{i-1}, K_{i-1} \rangle \bullet \Downarrow N_{\text{chaos}}^2 r; m; K_i \triangleright t \bullet. \text{ From the premises of T-NSQ-CONF, we have } \mu, \Gamma \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (r_0, m_0, K_0) \bullet \text{ok and } pc, \mu, \Gamma, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c_i, r, m, K) : \Gamma_i \bullet \text{ok. We already have } pc, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c_i, r_0, m_0, K_0) : \Gamma_1, K_1 \bullet \text{ok. Applying Lemma 13 we have } pc, \mu, \Gamma \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (r_{i-1}, m_{i-1}, K_{i-1}) \bullet \text{ok. Hence } pc, \Gamma, U \vdash \ubar{\delta}_{\delta} \chi_{\delta^{\delta}} (c_n, r_{n-1}, m_{n-1}, K_{n-1}) : \Gamma_n, K_n \bullet \text{ok.}
\]

Hence proved.

Using Lemma 13 and Lemma 14 we prove the second part of Theorem 1 for semantics $\Downarrow N_{\text{chaos}}$ and security specification 7.
Lemma 15

\[ k_L^{\mathcal{N}}((c, t_{\text{obs}})) \supseteq M \]

where

\[
M = \bigcap_{m' \in \{ t_{\text{obs}} \}_\text{mem}} \text{ind}_t(m_0, \gamma, \{ \text{cnd} \mid m'(\text{cnd}) = 0 \}) \\
\cap \left( (e', m') \in \{ t_{\text{obs}} \}_\text{exec} \right)
\]

Let \( S \) be the set of conditions that are set at the beginning of \( t_{\text{obs}} \), i.e., \( S = \{ \text{cnd} \mid m'(\text{cnd}) = 1 \} \). If \( Cond \) represents the set of all condition variables, then \( Cond \setminus S \) is the set of conditions that are unset at some time during the observed trace. Also let \( H \) be the set of all escape hatches that are declassified till the last event of \( t_{\text{obs}} \), i.e., \( H = \{ e \mid (e, m) \in \{ t \cdot t_{\text{obs}} \}_\text{exec} \} \).

Let \( m_2 \in M \). Also let \( N \vdash (c, r_{\text{init}}, m_2, K) \downarrow_{\mathcal{N}} t'_{\text{init}} ; m'_1 ; K' \triangleright t \cdot t_{\text{obs}} \cdot t' \) where \( t_{\text{obs}} = m' \cdot t'' \) for some memory \( m' \) and trace \( t'' \), and if \( t'' \) is not empty then the last element of \( t'' \) is an output event. Note that the attacker actually observes only low-events i.e. \([ t_{\text{obs}} ]_L \). We need to show that

\[
k_L^{\mathcal{N}}((c, t_{\text{obs}})) \supseteq M
\]

To ensure \( k_L^{\mathcal{N}}((c, t_{\text{obs}})) \supseteq M \), we need to show that \( m_2 \in k_L^{\mathcal{N}}((c, t_{\text{obs}})) \).

Note that \( m_1 \) and \( m_2 \) differ only in locations with policies that are protected by set \( S \). That is, for all locations \( l \in \text{Loc} \), if \( m_1(l) \neq m_2(l) \) then \( \Gamma(l) = \sigma_p \implies \text{protected}(p, S) \). Why? Suppose for some \( l \), s.t. \( \Gamma(l) = (\sigma_p, rt) \) let \( m_1(l) \neq m_2(l) \) and \( \neg\text{protected}(p, S) \). So, \( p = L \) or \( L \text{ and } K' \). Then for some \( m \in M \), we have \( m_1(l) = m_2(l) \). Since \( M \) is computed by the intersection of all such memories, every memory \( m'' \in M \) should satisfy \( m''(l) = m_1(l) \). This implies \( m_2(l) = m_1(l) \) which is a contradiction. Thus \( \text{protected}(p, S) \) must hold.

Also note that \( m_1 \) and \( m_2 \) satisfy

\[
\forall e \in H, \mu \vdash \langle c, r_{\text{init}}, m_1, K \rangle \downarrow v \iff \mu \vdash \langle c, r, m_2, K \rangle \downarrow v
\]

We will construct an \( \text{IMPE}^{\mathcal{N}} \) execution that represents the \( \text{IMPE} \) executions starting from \( m_0 \) and \( m_2 \). Type-preservation of \( \text{IMPE}^{\mathcal{N}} \) (Lemma 13) will ensure that both executions produce the same observable trace, thus showing that \( m_2 \in k_L^{\mathcal{N}}((c, t_{\text{obs}})) \).

Let \( \text{IMPE}^{\mathcal{N}} \) memory \( m = \text{merge}(m_1, m_2) \). If \( \mu \vdash \langle c, r_{\text{init}}, m, K \rangle \bullet \downarrow_{\mathcal{N}} s ; m' \bullet \) such that the attacker modifies the program in the same way in both the executions. By the adequacy of \( \text{IMPE}^{\mathcal{N}} \) (Lemma 10), we have that the \( \text{IMPE}^{\mathcal{N}} \) execution represents \( \text{IMPE} \) executions with \( m_1 \) and \( m_2 \) as initial memories.

Let \( t'' = t''_{\text{pre}} \cdot t''_{\text{obs}} \cdot t''_{\text{post}} \) for some \( t''_{\text{obs}} \) such that \( [t_{\text{obs}}]_1 = t_{\text{obs}} \). Define observation overlapped (same as the function defined in Section E.1.2 but repeated here for the ease of reference) by an \( \text{IMPE}^{\mathcal{E}} \) trace \( t'' \) as:

\[
\text{obsOverlap}(t'', t''_{\text{pre}}, t''_{\text{obs}}, t''_{\text{post}}) = \begin{cases} 
\epsilon & \text{if } t''_{\text{pre}} \leq t''_{\text{obs}} \\
t''_{\text{obs}} & \text{if } t''_{\text{pre}} \leq t''_{\text{obs}} \\
t''_{\text{obs}} & \text{if } t''_{\text{pre}} \leq t''_{\text{obs}} \\
t''_{\text{obs}} & \text{and } t''_{\text{pre}} \leq t''_{\text{obs}} \\
t''_{\text{obs}} & \text{and } t''_{\text{pre}} \leq t''_{\text{obs}}
\end{cases}
\]

Intuitively, \( \text{obsOverlap}(t'', t''_{\text{pre}}, t''_{\text{obs}}, t''_{\text{post}}) \) defines parts of input trace \( t'' \) that overlaps with an observed trace \( t''_{\text{obs}} \).

Since \( L, \mu, \Gamma, K, \emptyset \vdash_3 \langle c, r, m, K \rangle \triangleright \gamma \downarrow \text{pre} \cdot t''_{\text{obs}} \cdot t''_{\text{post}} \cdot t''_{\text{pre}} \), from Lemma 14, we have \( L, \mu, \Gamma, K, \emptyset \vdash_3 \gamma \downarrow \text{pre} \cdot t''_{\text{obs}} \cdot t''_{\text{post}} \cdot t''_{\text{pre}} \) and so \( L, \mu, \Gamma, K, \emptyset \vdash_3 \gamma \triangleright \emptyset \).

**Lemma 15 (Observational Equivalence is Preserved).** Let \( S \) be the set of conditions that are set (non-zero) in some observed trace \( t_{\text{obs}} \). If \( pc, \mu, \Gamma, U \vdash_3 \gamma \downarrow \text{pre} \cdot t''_{\text{obs}} \cdot t''_{\text{post}} \cdot t''_{\text{pre}} \cdot t''_{\text{obs}} \cdot t''_{\text{post}} \) then

\[
[ \text{obsOverlap}(t, t''_{\text{pre}}, t''_{\text{obs}}, t''_{\text{post}}) ]_1 \approx_L [ \text{obsOverlap}(t, t''_{\text{pre}}, t''_{\text{obs}}, t''_{\text{post}}) ]_2
\]

**Proof.** The proof follows by induction on the derivation of \( \mu \vdash \langle c, r, m, K \rangle \downarrow_{\mathcal{N}} t'' \).
Case NSq-Skip: Emitted trace is empty.
Case NSq-Assign: Emitted trace is empty.
Case NSq-Declassify: Emitted trace does not include output event.
Case NSq-Update: Emitted trace is empty.
Case NSq-SetCnd: Emitted trace does not include output event.

Case NSq-Output: Given $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle c, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash \langle output e \rangle \to \ell, r, m, K \bullet \frac{\delta}{\Delta_\text{chaos}} r; m; K \triangleright \text{Mem}(m) \cdot \text{Out}(\ell, v)$. Let $\ell = \text{Mem}(m) \cdot \text{Out}(\ell, v)$. From the premise of T-NSq-CONFIG, we have $pc, \mu, \Gamma, K', U \vdash output e \to \ell, \ell, K$ and so $\mu, \Gamma \vdash_{\delta \text{SHA}_N} e : \sigma_p$ and $\text{cur}(p, U) \sqcup \text{cur}(pc, U) \subseteq \ell$.

Case $v = (v_1 \mid v_2)$: We have protected $(p, S)$ and so $\ell \notin L$.
Case $v 

In the both the cases, we have

$$\text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}}) \approx_L \text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}})$$

Case NSq-If-Else: Given $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle \bullet \frac{\delta}{\Delta_\text{chaos}} r'; m''; K'' \triangleright t'' \bullet$. Let $\ell = t''$. Since $\mu \vdash_{\delta} (e, r, m, K) \downarrow v$ such that $v$ is not a pair, applying induction hypothesis to the premises of NSQ-IF-ELSE gives us

$$\text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}}) \approx_L \text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}})$$

From Lemma 14, we have $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle \text{while } e \text{ do } c, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash \langle \text{while } e \text{ do } c, r', m', K \rangle \bullet \frac{\delta}{\Delta_\text{chaos}} r''; m''; K'' \triangleright t'' \bullet$. Hence

$$\text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}}) \approx_L \text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}})$$

Case NSq-While: Given $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle \text{while } e \text{ do } c, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash \langle \text{while } e \text{ do } c, r', m', K \rangle \bullet \frac{\delta}{\Delta_\text{chaos}} r''; m''; K'' \triangleright t'' \bullet$. Since $\mu \vdash (e, r, m, K) \downarrow v$ such that $v$ is not a pair, applying induction hypothesis to the premise of NSQ-WHILE gives us

$$\text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}}) \approx_L \text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}})$$

Case NSq-Call: Given $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \bullet \frac{\delta}{\Delta_\text{chaos}} r'; m'; K' \triangleright t' \bullet$. Since $\mu \vdash (e, r, m, K) \downarrow v$ such that $v$ is not a pair, applying induction hypothesis to the premise of NSQ-CALL gives us

$$\text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}}) \approx_L \text{Overlap}(\hat{i}, t_{\text{pre}}, t_{\text{obs}}, t_{\text{post}})$$

Case NSq-If-Div: Given $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash (\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) \bullet \frac{\delta}{\Delta_\text{chaos}} r; m; K \triangleright c$. From the premises of T-NSQ-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_{\delta \text{SHA}_N} \langle c, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash (c, r, m, K) \downarrow v$ such that $v$ is a pair, we have protected $(p, S)$. From the well-typedness, neither $c_1$ nor $c_2$ do emit any out events to $L$ channel.

Case NSq-While-Div: Given $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle \text{while } e \text{ do } c, r, m, K \rangle : \Gamma, K \bullet ok$ and $\mu \vdash (\text{while } e \text{ do } c, r, m, K) \bullet \frac{\delta}{\Delta_\text{chaos}} r; m; K \triangleright c$. From the premises of T-NSQ-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_{\delta \text{SH}_N} \langle c, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash (c, r, m, K) \downarrow v$ such that $v$ is a pair, we have protected $(p, S)$.

Case NSq-If-Call: Given $pc, \mu, \Gamma, U \vdash_{\delta \text{SHA}_N} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash (\text{call}(e), r, m, K) \bullet \frac{\delta}{\Delta_\text{chaos}} r; m; K \triangleright c$. From the premises of T-NSQ-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_{\delta \text{SHA}_N} \langle c, r, m, K \rangle : \Gamma', K' \bullet ok$ and $\mu \vdash (c, r, m, K) \downarrow v$ such that $v$ is a pair, we have protected $(p, S)$.
Case NSq-Seq: Given \( pc, \mu, \Gamma_0, U \vdash_{\Delta}\text{SH}_{\text{N}\text{ch}} N\) \( \langle c_1; \ldots; c_n, r_0, m_0, K_0 \rangle : \Gamma_n, K_n \bullet \) \( ok \) and \( \mu \vdash \langle c_1; \ldots; c_n, r_0, m_0, K_0 \rangle \). From the premises of T-NSQ-\text{CONFIG}, we have \( pc, \mu, \Gamma_0, K_0, U \vdash_{\Delta}\text{SH}_{\text{N}\text{ch}} N\) \( c_1; \ldots; c_n \) : \( \Gamma_n, K_n \). Applying induction hypothesis to the premise, \( \mu \vdash \langle c_1, r_0, m_0, K_0 \rangle \bullet \). From Lemma \[14\] we have \( pc, \mu, \Gamma_1, U \vdash_{\Delta}\text{SH}_{\text{N}\text{ch}} N\) \( \langle c_2, r_1, m_1, K_1 \rangle : \Gamma_2, K_2 \bullet \). Applying inductive hypothesis to the next premise, \( \mu \vdash \langle c_2, r_1, m_1, K_1 \rangle \bullet \). From Lemma \[14\] we have \( pc, \mu, \Gamma_1, \emptyset \vdash_{\Delta}\text{SH}_{\text{N}\text{ch}} N\) \( \langle c, r, m, K \rangle : \Gamma', K' \bullet \). Applying induction hypothesis to the premise \( E_i \vdash \langle c, r, m, K \rangle \bullet \). From Lemma \[14\] we have \( pc, \mu, \Gamma_0, \emptyset \vdash_{\Delta}\text{SH}_{\text{N}\text{ch}} N\) \( \langle c, r_{\text{init}}, m, \emptyset \rangle : \Gamma' \bullet \). Hence proved that \( m_2 \in L \bullet_{\Delta} \langle c, t_{\text{obs}} \rangle \).

E.1.6 Proofs for \( E_1\text{-chaos} \) Security

In this section we use an even more permissive \( E_1\text{-chaos} \) type system and show that a IMPE program that is well-typed for the type system in Section 4 is also well-typed for \( E_1\text{-chaos} \) type system. Figure \[21\] presents the \( E_1\text{-chaos} \) type system. It further relaxes the \( N\text{-chaos} \) type system from Section E.1.3 by unconstraining the commands running both in the normal mode and killed enclave modes. They can now read and write to memory locations with no restrictions on security policies. The new typing system relies on the guarantees provided by the operational semantics that a command running in normal mode does not access enclave memory, and that a location from a killed enclave is inaccessible. Typing rules for commands running in enclave mode are unchanged and are same as those presented in Figure \[19\].

Lemma 16 (Permissive Type System 2). Let \( I \) be the set of enclaves killed. If \( L, N, \Gamma, \emptyset, \emptyset \vdash_{\Delta} c : \Gamma, K'\), then \( pc, \mu, \Gamma, K, U \vdash_{\Delta}\text{SH}_{\text{E}_1} c : \Gamma', K'\).

Proof Sketch. Proof is by straight forward induction on the derivation of the typing judgment \( \mu, \Gamma \vdash_{\Delta} c : \sigma_p \).

E.1.7 \text{IMPE}^{2E_1\text{-chaos}} Adequacy

The language \text{IMPE}^{2E_1\text{-chaos}} is adequate for reasoning about executions of two IMPE programs. We show that the execution of \text{IMPE}^{2E_1\text{-chaos}} program using semantics \( \bullet_{\Delta} \) is sound (i.e., large-step taken by a \text{IMPE}^{2E_1\text{-chaos}} program coresponds to a large-step taken by either side of the execution) and complete (given two \text{IMPE}^{2E_1\text{-chaos}} executions, there exists an \text{IMPE}^{2E_1\text{-chaos}} execution).
The definition differs from protected shown below. raised to IMP

$\text{EI-Skip-N}$

\[ pc, N, \Gamma, K, U \vdash_{\text{EI}} \text{skip} : \Gamma, K \]

$\text{EI-Assign}$

\[ \mu, \Gamma \vdash_{\text{EI}} e : \sigma_p \quad \mu \not\in I \]

\[ pc, \mu, \Gamma, K, U \vdash_{\text{EI}} x := e : \Gamma [x \mapsto \sigma_{pc,\mu}], K \]

$\text{EI-Output}$

\[ \mu, \mu, \Gamma, K, U \vdash_{\text{EI}} \text{output} e \to \ell : \Gamma, K \]

$\text{EI-SEQ}$

\[ \forall i \in \{1 \ldots n\}, pc, \mu, \Gamma_{i-1}, K_{i-1}, U \vdash_{\text{EI}} c_i : \Gamma_i, K_i \]

\[ pc, \mu, \Gamma_0, K_0, U \vdash_{\text{EI}} c_1; \ldots; c_n : \Gamma_n, K_n \]

$\text{EI-If-Isunset}$

\[ \mu, \Gamma \vdash_{\text{EI}} \text{isunset}(cnd) : \text{int}_L \]

\[ pc, \mu, \Gamma, K, U \vdash_{\text{EI}} c_1 : \Gamma', K_1 \]

\[ pc, \mu, \Gamma, K, U \vdash_{\text{EI}} c_2 : \Gamma', K_2 \]

\[ K' = K_1 \cup K_2 \quad \mu \not\in I \]

$\text{EI-If-Else}$

\[ \mu, \Gamma \vdash_{\text{EI}} e : \text{int}_P \]

\[ pc', N, \Gamma, K, U \vdash_{\text{EI}} c_1 : \Gamma', K_1 \]

\[ pc', N, \Gamma, K, U \vdash_{\text{EI}} c_2 : \Gamma', K_2 \]

\[ K' = K_1 \cup K_2 \quad \mu \not\in I \]

$\text{EI-While}$

\[ \mu, \Gamma \vdash_{\text{EI}} e : \text{int}_P \]

\[ pc, \mu, \Gamma, K, U \vdash_{\text{EI}} \text{while } e \text{ do } c : \Gamma, K \]

$\text{EI-Call}$

\[ \mu, \Gamma \vdash_{\text{EI}} e : (\Gamma', K', U \text{ API } \Gamma^+, K') \quad \mu \not\in I \]

\[ pc, \mu, \Gamma, K, U \vdash_{\text{EI}} \text{call}(e) : \Gamma_{\text{out}}, K^+ \]

Figure 21. $E_1$-chaos typing rules for IMPE

### E.1.8 IMPE$_{E_1}$-chaos $E_1$-chaos Type System

Let $S$ be the set of conditions set during some observed trace $t_{obs}$. $H$ be the set of escape hatches till the observed trace and $\hat{m}_0$ be the initial IMPE$_{E_1}$-chaos memory. A policy is now protected if it is either $\top$ or $\ell$ cond $\top$ s.t. $m\text{cond} = 1$. We define protected$_I(p, S)$ as follows:

$$
\text{protected}_I(p, S) = \begin{cases} 
\text{true} & \text{if } p = \top \\
\text{true} & \text{if } p = \ell \text{ cond } \top \text{ and } \text{cond} \in S \\
\text{false} & \text{otherwise}
\end{cases}
$$

The definition differs from protected$(p, S)$ defined earlier in that an erasure policy is protected if the confidentiality level is raised to $\top$ only (after some condition cond is set).

The IMPE$_{E_1}$-chaos type system is parametrized by $\delta$, $S$, $H$ and $\hat{m}_0$. The typing judgment for commands and expressions is shown below.

\[ pc, \mu, \Gamma, K, U \vdash_{\delta \text{SH} \hat{m}_0 \text{EI}} c : \Gamma', K' \]

\[ \mu, \Gamma \vdash_{\delta \text{SH} \hat{m}_0 \text{EI}} e : \sigma_p \]

The typing rules are shown in Figure 21 and ensure that commands running in enclaves that aren’t killed are well-typed according to IMPE$^+$ type system. Rules for typing configurations are shown in Figure 22 and are similar to T-NSQ-CONFIG and T-NSQ-VALUE.
Proof. The proof is by straightforward induction on the derivation of the large step µ.

\[ \forall \varphi \in \text{Vars}, (r, x) = (v_1 | v_2) \text{ and } \Gamma(x) = \sigma_p \implies \text{protected}_l(p, S) \text{ and } \delta \in I \]
\[ \forall \varphi \in \text{Loc} \setminus \text{Cond}, (l, m) = (v_1 | v_2) \text{ and } \delta(l) = (\sigma_p, rt) \implies \text{protected}_l(p, S) \text{ and } \delta \in I \]
\[ \forall \varphi \in \text{H}, \mu \vdash \langle e, r_{\text{init}}, m_0, K \rangle \bullet \psi_{E_{chaos}} v \implies \mu \vdash \langle e, r, m, K \rangle \bullet \psi_{E_{chaos}} v \]

\[
\begin{array}{c}
\text{T-ESQ-CONFIG} \\
\mu, \Gamma, U \vdash \delta_{SH_{\mu_0}E_{\mu}} (c, r, m, K) : \Gamma' \bullet \text{ok}
\end{array}
\]

\[
\begin{array}{c}
\text{T-ESQ-VALUE} \\
\Gamma \vdash \delta_{SH_{\mu_0}E_{\mu}} \langle r, m, K \rangle \bullet \text{ok}
\end{array}
\]

Lemma 19 (E_{chaos} Value Type Preservation). If \( \mu, \Gamma \vdash \delta_{SH_{\mu_0}E_{\mu}} e : \sigma_p \) and \( \mu \vdash \langle e, r, m, K \rangle \bullet \psi_{E_{chaos}} v \), then \( \mu, \Gamma \vdash \delta_{SH_{\mu_0}E_{\mu}} v : \sigma_p \).

Proof Sketch. The proof is by straightforward induction on the derivation of the typing judgment \( \mu, \Gamma \vdash \delta_{SH_{\mu_0}E_{\mu}} e : \sigma_p \).

Lemma 20 (E_{chaos} Protected Expression). Let \( \Gamma \vdash \delta_{SH_{\mu_0}E_{\mu}} \langle r, m, K \rangle \bullet \text{ok} \). If \( \mu, \Gamma \vdash \delta_{SH_{\mu_0}E_{\mu}} e : \sigma_p \) and \( \mu \vdash \langle e, r, m, K \rangle \bullet \psi_{E_{chaos}} v \), then \( \Gamma' \bullet \text{ok} \).

Proof Sketch. The proof is by straightforward induction on the derivation of the typing judgment \( \mu, \Gamma \vdash \delta_{SH_{\mu_0}E_{\mu}} e : \sigma_p \).

Lemma 21 (IMPE_{\mu_0}E_{\mu} E_{chaos} Final Configuration Preservation). Let \( I \) be the set of enclaves killed, \( \gamma \) be the security specification such that \( \gamma(l) = L \forall \delta(l) = I \) and \( \Gamma \) be an environment that corresponds to \( \gamma \) and is well-typed for \( \delta \). Also let \( H \) be the set of escape hatches and \( \hat{m}_0 \) be the initial \( \text{IMPE}_{\text{\mu_0}E_{\mu}} \) memory such that \( l \in \{ \text{locations}(e) \mid e \in H \} \), \( \hat{m}_0(l) \neq (v_1 | v_2) \), i.e., not a pair value. If \( pc, \mu, \Gamma, U \vdash \delta_{SH_{\mu_0}E_{\mu}} \langle c, r, m, K \rangle : \Gamma' \bullet \text{ok} \) and \( \mu \vdash \langle c, r, m, K \rangle \bullet \psi_{E_{chaos}} r; m' \), then \( \mu, \Gamma' \vdash \delta_{SH_{\mu_0}E_{\mu}} \langle r', m', K \rangle \bullet \text{ok} \).

Proof. The proof is by induction on the derivation of the large step \( \mu \vdash \langle c, r, m, K \rangle \bullet \psi_{E_{chaos}} r; m' \).
From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m, K \rangle \bullet \mathsf{ok}$, $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} e_1 : (\sigma_p^{\prime} \mathsf{ref}^{\mathsf{It}})_q$ and $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} e_2 : \sigma_p$ such that $p' \cup q \cup p \subseteq p$.

**Case** $l = (l_1 \| l_2), v = (v_1 \parallel v_2)$: Applying Lemma 20, we have protected$_I(p', S)$ and $\mu \in I$. So protected$_I(p, S)$.

Since $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} l : (\sigma_p^{\prime} \mathsf{ref}^{\mathsf{It}})_L$, from the well-typedness of environment, we have $d(l) = \mu' \in I$. Hence $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m', K \rangle \bullet \mathsf{ok}$.

**Case** $l \neq (l_1 \| l_2), v = (v_1 \parallel v_2)$: Same as above.

**Case** $l = (l_1 \| l_2), v \neq (v_1 \parallel v_2)$: Applying Lemma 20, we have protected$_I(q, S)$ and $\mu \in I$. So protected$_I(p, S)$.

Since $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} l : (\sigma_p^{\prime} \mathsf{ref}^{\mathsf{It}})_L$, from the well-typedness of environment, we have $d(l) = \mu' \in I$. Hence $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m', K \rangle \bullet \mathsf{ok}$.

**Case** $l \neq (l_1 \| l_2), v \neq (v_1 \parallel v_2)$: Trivially $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m', K \rangle \bullet \mathsf{ok}$.

**Case ESQ-OUTPUT**: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathsf{SHInoN}_{\mathsf{ch}}} \langle \text{output } e \to \ell, r, m, K \rangle : \Gamma' \bullet \mathsf{ok}$ and $\mu \vdash \langle \text{output } e \to \ell, r, m, K \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r; m': K \triangleright \mathsf{Mem}(m) \\bullet \mathsf{Out}(\ell, v)$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m, K \rangle \bullet \mathsf{ok}$.

Large-step does not modify register file, memory or killset.

**Case ESQ-SETCND**: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathsf{SHInoN}_{\mathsf{ch}}} \langle \text{set} \mathsf{nd}, r, m, K \rangle : \Gamma' \bullet \mathsf{ok}$ and $\mu \vdash \langle \text{set} \mathsf{nd}, r, m, K \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r; m': K \triangleright \mathsf{Mem}(m)$. So that $m' = m|\mathsf{cond} \to 1$. We have to prove that $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m', K \rangle \bullet \mathsf{ok}$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m, K \rangle \bullet \mathsf{ok}$. Since $m$ and $m'$ do not differ (set$\mathsf{nd}$ always sets $\mathsf{cond}$ to a non-pair value), we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m, K \rangle \bullet \mathsf{ok}$.

**Case ESQ-KILL**: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathsf{SHInoN}_{\mathsf{ch}}} \langle \text{kill}(i), r, m, K \rangle : \Gamma' \bullet \mathsf{ok}$ and $\mu \vdash \langle \text{kill}(i), r, m, K \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r; m': K \triangleright \mathsf{Mem}(m) \\bullet \mathsf{ok}$. We have to prove that $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m', K \rangle \bullet \mathsf{ok}$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m, K \rangle \bullet \mathsf{ok}$. Since $[K_1] = [K_2]$, we therefore have $[K \cup \{E_i\}]_1 = [K \cup \{E_i\}]_2$. Hence $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r, m, K \rangle \subseteq \mathsf{ok}$.

**Case ESQ-SEQ**: Given $pc, N, \mu, \Gamma, U \vdash_{\delta \mathsf{SHInoN}_{\mathsf{ch}}} \langle \text{enclave}(i, c, r, m, K) \rangle : \Gamma' \bullet \mathsf{ok}$ and $\mu \vdash \langle \text{enclave}(i, c, r, m, K) \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r'; m'; K' \triangleright t' \bullet \mathsf{ok}$. We have to prove that $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r', m', K' \rangle \bullet \mathsf{ok}$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle \mathsf{enclave}(i, c, r, m, K) \rangle \bullet \mathsf{ok}$.

**Case ESQ-IF-ELSE**: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathsf{SHInoE}_i} \langle \text{if} \mathsf{then} c_1 \text{else} c_2, r, m, K \rangle : \Gamma' \bullet \mathsf{ok}$ and $\mu \vdash \langle \text{if} \mathsf{then} c_1 \text{else} c_2, r, m, K \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r'; m'; K' \triangleright t' \bullet \mathsf{ok}$. We have to prove that $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r', m', K' \rangle \bullet \mathsf{ok}$.

From the premise of T-NSQ-CONFIG, we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle \mathsf{if} \mathsf{then} c_1 \text{else} c_2, r, m, K \rangle \bullet \mathsf{ok}$ and $\mu \vdash \langle \mathsf{if} \mathsf{then} c_1 \text{else} c_2, r, m, K \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r'; m'; K' \triangleright t' \bullet \mathsf{ok}$.

**Case ESQ-WHILE**: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathsf{SHInoN}_{\mathsf{ch}}} \langle \text{while } e \mathsf{do} c, r, m, K \rangle : \Gamma' \bullet \mathsf{ok}$ and $\mu \vdash \langle \text{while } e \mathsf{do} c, r, m, K \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r'; m'; K' \triangleright t' \bullet \mathsf{ok}$. We have to prove that $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r', m', K' \rangle \bullet \mathsf{ok}$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle \text{while } e \mathsf{do} c, r, m, K \rangle \bullet \mathsf{ok}$.

**Case ESQ-CALL**: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathsf{SHInoN}_{\mathsf{ch}}} \langle \text{call}(e), r, m, K \rangle : \Gamma' \bullet \mathsf{ok}$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \downarrow_{\mathsf{E}_i, \mathsf{chaos}} r'; m'; K' \triangleright t' \bullet \mathsf{ok}$. We have to prove that $\mu, \Gamma \vdash_{\delta \mathsf{SHInoE}_i} \langle r', m', K' \rangle \bullet \mathsf{ok}$.
From the premise of T-ESQ-CONFIG, we have \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle r, m, K \rangle \bullet ok \) and \( pc, \mu, \Gamma, K^+, U \vdash_{\deltaSHintokE_1} \text{call}(e) \) \( : \Gamma^+, K^+ \) such that \( \Gamma \leq \Gamma^+ \text{ and } K = K^, K^+ = K^+ \). From subsumption, \( p, \mu, \Gamma, U \vdash_{\deltaSHintokN-ch}_{\{c, r, m, K\}} : \Gamma \bullet ok \Gamma^k K^\prime \). Applying induction hypothesis to \( \mu \vdash \langle c, r, m, K \rangle \bullet \eta^2_{E_1-chaos} r^\prime; m'; K' \triangleright t' \bullet \), we thus have \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle r', m', K' \rangle \bullet ok \).

**Case ESQ-IF-DIV:** Given \( pc, \mu, \Gamma, U \vdash_{\deltaSHintokN-ch} \langle \text{if } e \text{ then } c_0 \text{ else } c_1, r, m, K \rangle : \Gamma' \bullet ok \) and \( \mu \vdash \langle \text{if } e \text{ then } c_0 \text{ else } c_1, r, m, K \rangle \bullet \eta^2_{E_1-chaos} \tilde{r}; \tilde{m}; K \triangleright \tilde{t} \bullet \). We have to prove that \( \mu, \Gamma' \vdash_{\deltaSHintokE_1} \langle \tilde{r}, \tilde{m}, K \rangle \bullet ok \).

From the initial configuration, we have \( pc', \mu, \Gamma, K, U \vdash_{\deltaSHintokE_1} c_2 : \Gamma', K' \) and \( \mu, \Gamma \vdash e : \text{int}_p \). From the premise of ESQ-IF-DIV, we have \( \mu \vdash \langle c, r, m, K \rangle \bullet \eta^2_{E_1-chaos} (v_0 | v_1) \). So \( \mu \in I, \text{protected}_I(p, S) \) and \( \text{protected}_I(pc', S) \).

Let \( z \) be such that \( r(z) = (v_1 | v_2) \). If \( (\Gamma(z) = \sigma_q) \), then either \( (\Gamma(z) = \sigma_q \text{ or there is an assignment to } z \text{ in } c_0 \text{ for some } i = \{0, 1\} \). If the former holds, then we already have \( \text{protected}_I(q, S) \). If the latter holds, then we have \( \text{protected}_I(q, S) \) (because an assignment is at least as restrictive as \( pc' \)).

Let \( m_l(l) = (v_1 | v_2) \) and \( \Gamma(l) = \sigma_q \). Since the type of location is invariant throughout the program, from the initial configuration we have \( \text{protected}_I(q, S) \). A well-typed escape hatch has immutable locations and thus evaluates to the same initial value. Since, both branches \( c_0 \) and \( c_1 \) have same killsets, we have \( K_1 = K_2 \). So \( [K_1] = [K_2] \). Hence \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle \tilde{r}, \tilde{m}, K \rangle \bullet ok \).

**Case ESQ-WHILE-DIV:** Given \( pc, \mu, \Gamma, U \vdash_{\deltaSHintokN-ch} \langle \text{while } e \text{ do } c, r, m, K \rangle \vdash \Gamma, K \bullet ok \) and \( \mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \bullet \eta^2_{E_1-chaos} \tilde{r}; \tilde{m}; K \triangleright \tilde{t} \bullet \). We have to prove that \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle \tilde{r}, \tilde{m}, K \rangle \bullet ok \).

From the initial configuration, we have \( pc', \mu, \Gamma, K, U \vdash_{\deltaSHintokE_1} c : \Gamma, K \) and \( \mu, \Gamma \vdash_{\deltaSHintokE_1} e : \text{int}_p \) for \( pc \leq \text{pc} \). From the premise of ESQ-WHILE-DIV, we have \( \mu \vdash \langle c, r, m, K \rangle \bullet \eta^2_{E_1-chaos} (v_0 | v_1) \). So \( \mu \in I, \text{protected}_I(p, S) \) and \( \text{protected}_I(pc', S) \).

Let \( z \) be such that \( r(z) = (v_1 | v_2) \). If \( r(z) = (v_1 | v_2) \) and \( \Gamma(z) = \sigma_q \), then from the premise of T-ESQ-CONFIG, we already have \( \text{protected}_I(q, S) \). If \( r \neq (v_1 | v_2) \), not a pair value, and \( \Gamma(z) = \sigma_q \), then from the well-typedness, \( pc', \mu, \Gamma, K, U \vdash_{\deltaSHintokE_1} c : \Gamma, K \), we have \( \text{protected}_I(pc', S) \) and \( \text{protected}_I(q, S) \) (because an assignment is at least as restrictive as \( pc' \)). Similarly, let \( m_l(l) = (v_1 | v_2) \) and \( \Gamma(l) = \sigma_q \). Since the type of location is invariant throughout the program, from the initial configuration we have \( \text{protected}_I(q, S) \). A well-typed escape hatch has immutable locations and thus evaluates to the same initial value. Killsets are unmodified. So \( [K_1] = [K_2] \). Hence \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle \tilde{r}, \tilde{m}, K \rangle \bullet ok \).

**Case ESQ-CALL-DIV:** Given \( pc, \mu, \Gamma, U \vdash_{\deltaSHintokN-ch} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \bullet ok \) and \( \mu \vdash \langle \text{call}(e), r, m, K \rangle \bullet \eta^2_{E_1-chaos} \tilde{r}; \tilde{m}; K \triangleright \tilde{t} \bullet \). We have to prove that \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle \tilde{r}, \tilde{m}, K \rangle \bullet ok \).

From the initial configuration, we have \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle r, m, K \rangle \bullet ok \) and \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle \text{call}(e), r, m, K \rangle \bullet \eta^2_{E_1-chaos} (v_0 | v_1) \). So \( \mu \in I, \text{protected}_I(p, S) \) and \( \text{protected}_I(q, S) \) follows.

Let \( z \) be such that \( r(z) = (v_1 | v_2) \). If \( r(z) = (v_1 | v_2) \) and \( \Gamma(z) = \sigma_q \), then from the premise of T-ESQ-CONFIG, we already have \( \text{protected}_I(y, S) \). If \( r \neq (v_1 | v_2) \), i.e., not a pair value, and \( \Gamma(z) = \sigma_q \), then from the well-typedness of \( pc', \mu, \Gamma', K', U \vdash_{\deltaSHintokE_1} c : \Gamma^+, K^+ \) such that \( K = K^, K^+ = K^+ \) and \( \Gamma = \Gamma^+, \Gamma^+ = \Gamma^+ \). From the premise of ESQ-CALL-DIV, we have \( \mu \vdash \langle c, r, m, K \rangle \bullet \eta^2_{E_1-chaos} (v_0 | v_1) \). So \( \mu \in I, \text{protected}_I(q, S) \) and since \( q \leq p \), \( \text{protected}_I(y, S) \) follows.

Thus, we have \( \mu, \Gamma \vdash_{\deltaSHintokE_1} \langle \tilde{r}, \tilde{m}, K \rangle \bullet ok \).

Hence proved.

**Lemma 22** (IMPE\(_{E_1-chaos}^2\) Type Preservation). Let \( I \) be the set of enclaves killed, \( \gamma \) be the security specification such that \( \gamma(l) = L \forall \delta(l) = l \) and \( \Gamma \) be an environment that corresponds to \( \gamma \) and is well-typed for \( \delta \). Also let \( H \) be the set of escape hatches and \( m_0 \) be the initial IMPE\(_{E_1-chaos}^N\) memory such that \( l \in \text{locations}(e) \) \( \implies e \in H \), \( m_0(l) \neq (v_1 | v_2) \), i.e., not a pair value and \( pc, \mu, \Gamma, U \vdash_{\deltaSHintokE_1} \langle c, r, m, K \rangle : \Gamma \bullet ok \). If \( \mu \vdash \langle c', r', m', K' \rangle \bullet \eta^2_{E_1-chaos} \tilde{r}; \tilde{m}; K \triangleright \tilde{t} \bullet \), then \( \exists \tilde{pc}, \Gamma, U, \text{protected}_I(p, S) \) follows.

Proof. The proof is by induction on the derivation of the large step \( \mu \vdash \langle c, r, m, K \rangle \bullet \eta^2_{E_1-chaos} r'; m'; K' \triangleright t' \bullet \). Since rules ESQ-ASSIGN, ESQ-SKIP, ESQ-UPDATE, ESQ-KILL, ESQ-OUTPUT, ESQ-SETCND, ESQ-IF-DIV, ESQ-WHILE-DIV and
ESQ-CALL-DIV do not have IMPE_{chaos}^2 command premises, the only relevant cases are ESQ-ENCLAVE, ESQ-IF, ESQ-WHILE, ESQ-SEQ, ESQ-CALL.

**Case ESQ-ENCLAVE:** Given \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle \text{enclave}(i, c), r, m, K \rangle : \Gamma' \bullet \text{ok} \). From the premises of T-SQ-CONFIG, we have \( \Gamma \vdash \delta E_{\text{chaos}} \langle r, m, K \rangle \bullet \text{ok} \) and \( pc, E_i, \Gamma, K, \emptyset \vdash \delta E_{\text{chaos}} \langle c : \Gamma', K' \rangle \). From the premises of the IMPE_{chaos}^2 large-step, we have \( E_i \vdash \langle c, r, m, K \rangle \vdash E_{\text{chaos}}^{2, c} ; m' ; K' \triangleright t' \bullet \). Hence \( pc, \emptyset, \Gamma, E_i \vdash \delta E_{\text{chaos}} \langle c, r, m, K \rangle : \Gamma' \bullet \text{ok} \).

**Case ESQ-IF-ELSE:** Given \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle : \Gamma' \bullet \text{ok} \). From the premises of the IMPE_{chaos}^2 large-step, we have \( \mu \vdash \langle e, r, m, K \rangle \vdash E_{\text{chaos}}^{2, c} ; m' ; K' \triangleright t' \bullet \). From the premises of T-SQ-CONFIG, we have \( \Gamma \vdash \delta E_{\text{chaos}} \langle c_i, r, m, K \rangle \bullet \text{ok} \) and \( pc', \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c_i, r, m, K \rangle : \Gamma', K' \) for \( i \in \{ 1, 2 \} \) and \( pc \leq pc' \). Hence \( pc', \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c_2, r, m, K \rangle : \Gamma' \bullet \text{ok} \).

Note that if \( e = \text{isunset}(\text{cmd}) \), then we have \( pc', \mu, \Gamma, U \cup \{ \text{cmd} \} \vdash \delta E_{\text{chaos}} \langle c, r, m, K \rangle : \Gamma' \bullet \text{ok} \) and \( pc', \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c_2, r, m, K \rangle : \Gamma' \bullet \text{ok} \).

**Case ESQ-WHILE:** Given \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle \text{while } e \text{ do } c', r, m, K \rangle : \Gamma' \bullet \text{ok} \). From the premises of the IMPE_{chaos}^2 large-step, we have \( \mu \vdash \langle e, r, m, K \rangle \vdash E_{\text{chaos}}^{2, c} ; m' ; K' \triangleright t' \bullet \) and \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c', r, m, K \rangle : \Gamma' \bullet \text{ok} \). Hence \( pc', \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c', r, m, K \rangle : \Gamma' \bullet \text{ok} \).

**Case ESQ-CALL:** Given \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \bullet \text{ok} \). From the premises of the IMPE_{chaos}^2 large-step, we have \( \mu \vdash \langle e, r, m, K \rangle \vdash E_{\text{chaos}}^{2, c} \lambda \cdot \mu \vdash \langle e, r, m, K \rangle \vdash E_{\text{chaos}}^{2, c} ; m' ; K' \triangleright t' \bullet \) and \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c', r, m, K \rangle : \Gamma', K' \bullet \text{ok} \). Hence \( pc', \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c', r, m, K \rangle : \Gamma', K' \bullet \text{ok} \).

**Case ESQ-SEQ:** Given \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c_1; \ldots ; c_n, r_0, m_0, K_0 \rangle : \Gamma_n, K_n \bullet \text{ok} \). From the premises of the IMPE_{chaos}^2 large-step, we have \( \mu \vdash \langle c_i, r_{i-1}, m_{i-1}, K_{i-1} \rangle \vdash E_{\text{chaos}}^{2, c} \lambda \cdot \mu \vdash \langle c_i, r_{i-1}, m_{i-1}, K_{i-1} \rangle \vdash E_{\text{chaos}}^{2, c} ; m' ; K' \triangleright t' \bullet \) and \( pc, \mu, \Gamma, U \vdash \delta E_{\text{chaos}} \langle c_i, r_{i-1}, m_{i-1}, K_{i-1} \rangle : \Gamma_i, K_i \) for \( i = 1, \ldots, n \).

We already have \( pc, U, \Gamma \vdash \delta E_{\text{chaos}} \langle c, r_0, m_0, K_0 \rangle \bullet \text{ok} \). Applying Lemma 21, we have \( \mu, \Gamma \vdash \delta E_{\text{chaos}} \langle r_1, m_1, K_1 \rangle \bullet \text{ok} \). Hence \( pc, U, \Gamma \vdash \delta E_{\text{chaos}} \langle c_2, r_1, m_1, K_1 \rangle : \Gamma_2, K_2 \bullet \text{ok} \). Repeatedly applying the above argument for \( n \) times, we thus have \( pc, U, \Gamma_{n-1}, \mu \vdash \delta E_{\text{chaos}} \langle c_n, r_{n-1}, m_{n-1}, K_{n-1} \rangle : \Gamma_n, K_n \bullet \text{ok} \).

Hence proved.

Using Lemma 21 and Lemma 22, we prove the final part of Theorem 1 for semantics \( E_{\text{chaos}}^{2, c} \) and specification \( \gamma' \).

**Proof.** Given \( L, \mu, \Gamma, K, \emptyset \vdash c : \Gamma', K' \). Let \( m_1 \) be some initial memory for which \( N \vdash c, r_{\text{init}}, m_1, K \vdash E_{\text{chaos}}^{2, c} \lambda m' ; r' ; m' ; K' \triangleright t' \), where \( t_{\text{obs}} \equiv m' \cdot t'' \) for some memory \( m' \) and trace \( t'' \), and if \( t'' \) is not empty then the last element of \( t'' \) is an output event. Note that the attacker actually observes only low-events i.e. \( |t_{\text{obs}}|_L \). We need to show that

\[
 k_L \vdash E_{\text{chaos}}^{2, c} (c, t_{\text{obs}}) > M
\]

where

\[
 M = \left( \bigcap_{m' \in \{ t_{\text{obs}} \}_{\text{mem}}} \text{ind}_t(m_0, \gamma', \{ cnd \mid m'(cnd) = 0 \}) \right) 
\]

\[
 \cap \left( \{ e' \mid m' \in \{ t_{\text{obs}} \}_{\text{exec}} \} \right)
\]

Let \( S \) be the set of conditions that are set at the beginning of \( t_{\text{obs}} \), i.e., \( S = \{ cnd \mid m'(cnd) = 1 \} \). If \( \text{Cond} \) represents the set of all condition variables, then \( \text{Cond} \setminus S \) is the set of conditions that are unset at some time during the observed trace. Also let \( \mathcal{H} \) be the set of all escape hatches that are declassified till the last event of \( t_{\text{obs}} \), i.e., \( \mathcal{H} = \{ e \mid (c, m) \in \{ t \cdot t_{\text{obs}} \}_{\text{exec}} \} \).

Let \( m_2 \in M \). Also let \( N \vdash c, r_{\text{init}}, m_2, K \vdash E_{\text{chaos}}^{2, c} ; m_2' ; K_2' \triangleright t_2 \). It thus follows that

\[
 [t_2]_{1, \text{cnd}} = [t_2]_{2, \text{cnd}}
\]
To ensure $k_L^{\mathcal{E}_1^{chaos}}(c, t_{obs}) \supseteq M$, we need to show that $m_2 \in k_L^{\mathcal{E}_1^{chaos}}(c, t_{obs})$.

Note that $m_1$ and $m_2$ differ only in locations with policies that are protected by set $S$. That is, for all locations $l \in Loc$, if $m_1(l) \neq m_2(l)$ then $\Gamma(l) = \sigma_p \implies protected(p, S)$. Why? Suppose for some $l$, s.t. $\Gamma(l) = (\sigma_p, r_t)$ let $m_1(l) \neq m_2(l)$ and $\neg protected(p, S)$. So, $p \in \ell$ or $\ell \notin S$. Thus, for some $m_j \in M$, we have $m_1(l) = m_j(l)$. Since $M$ is computed by the intersection of all such memories, every memory $m'' \in M$ should satisfy $m''(l) = m_1(l)$. This implies $m_2(l) = m_1(l)$ which is a contradiction. Thus $protected(p, S)$ must hold.

Also note that $m_1$ and $m_2$ satisfy

$$\forall e \in H, \mu \vdash_\delta \langle e, r_{init}, m_1, K \rangle \downarrow v \iff \mu \vdash_\delta \langle e, r, m_2, K \rangle \downarrow v$$

We will construct an IMPE execution that represents the IMPE executions starting from $m_1$ and $m_2$. Type-preservation of IMPE$^{\mathcal{E}_1^{chaos}}$ (Lemma 21) will ensure that both executions produce the same observable trace, thus showing that $m_2 \in k_L^{\mathcal{E}_1^{chaos}}(c, t_{obs})$.

Let IMPE$^{\mathcal{E}_1^{chaos}}$ memory $m = \text{merge}(m_1, m_2)$ and $\mu \vdash \langle c, r_{init}, m, K \rangle \Downarrow^2 \mathcal{E}_1^{chaos} r^*; m^*; K \triangleright t^*$ such that the attacker modifies the program in the same way in both the executions. By the adequacy of IMPE$^{\mathcal{E}_1^{chaos}}$ (Lemma 18), we have that the IMPE$^{\mathcal{E}_1^{chaos}}$ execution represents IMPE executions with $m_1$ and $m_2$ as initial memories.

Let $t^* = t^*_{pre} \cdot t^*_{obs} \cdot t^*_{post}$ for some $t^*_{obs}$ such that $[t^*_{obs}]_1 = t_{obs}$. Define observation overlapped (same as the function defined in Section E.1.3 but repeated here for the ease of reference) by an IMPE$^{\mathcal{E}_1^{chaos}}$ trace $t^*$ as:

$$\text{obsOverlap}(t^*, t^*_{pre}, t^*_{obs}, t^*_{post}) = \begin{cases} 
\epsilon & \text{if } t^* \leq_{lex} t^*_{pre} \\
 \{a\} & \text{if } t^*_{pre} \cdot t^*_{obs} \leq_{lex} t^* \\
 \{a\} & \text{if } t^* = t^*_{pre} \cdot t^*_{obs} \text{ and } t^* \leq t^*_{obs} \\
 \{a\} & \text{otherwise}
\end{cases}$$

Intuitively, $\text{obsOverlap}(t^*, t^*_{pre}, t^*_{obs}, t^*_{post})$ defines part of input trace $t^*$ that overlaps with an observed trace $t^*_{obs}$.

Since $L \cup M \cup \emptyset \vdash_\delta \mathcal{E}_1^{chaos} c : \Gamma', K'$, from Lemma 16 we have $L, \mu, \Gamma, K, \emptyset \vdash_\delta \mathcal{E}_1^{chaos} c : \Gamma', K'$ and so $L, \mu, \Gamma, K, \emptyset \vdash_\delta \mathcal{E}_1^{chaos} c : \Gamma', K'$. Note that our initial configuration satisfies:

$$L, N, \Gamma, \emptyset \vdash_\delta \mathcal{E}_1^{chaos} \langle c, r_{init}, m, \emptyset \rangle : \Gamma' \triangleright \Box$$

**Lemma 23** (Observational Equivalence is Preserved). Let $S$ be the set of conditions that are set(non-zero) in some observed trace $t_{obs}$. If $pc, \mu, \Gamma, U \vdash_\delta \mathcal{E}_1^{chaos} \langle c, r, m, K \rangle : \Gamma', K' \triangleright \Box$ and $\mu \vdash \langle c, r, m, K \rangle \Downarrow^2 \mathcal{E}_1^{chaos} \text{ let } c: \Gamma, K \triangleright \Box$, then

$$\text{obsOverlap}(\hat{t}, t^*_{pre}, t^*_{obs}, t^*_{post})_1 \approx_L \text{obsOverlap}(\hat{t}, t^*_{pre}, t^*_{obs}, t^*_{post})_2$$

Proof. The proof follows by induction on the derivation of $\mu \vdash \langle c, r, m, K \rangle \Downarrow^2 \mathcal{E}_1^{chaos} \text{ let } c: \Gamma, K \triangleright \Box$.

**Case ESq-Skip**: Emitted trace is empty.

**Case ESq-Assign**: Emitted trace is empty.

**Case ESq-Declasify**: Emitted trace does not include $out$ event.

**Case ESq-Update**: Emitted trace is empty.

**Case ESq-Kill**: Emitted trace is empty.

**Case ESq-SetCnd**: Emitted trace does not include $out$ event.

**Case ESq-Output**: Given $pc, \mu, \Gamma, U \vdash_\delta \mathcal{E}_1^{chaos} \langle c, r, m, K \rangle : \Gamma', K' \triangleright \Box$ and $\mu \vdash \langle \text{output } e \text{ to } \ell, r, m, K \rangle \Downarrow^2 \mathcal{E}_1^{chaos} r; m; K \triangleright \text{Mem}(m) \cdot \text{Out}(\ell, v)$. Let $\hat{t} = \text{Mem}(m) \cdot \text{Out}(\ell, v)$. From the premise of $\mathcal{T}$-ESq-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_\delta \text{output } e \text{ to } \ell, K$ and so $\mu, \Gamma \vdash_\delta \mathcal{E}_1^{chaos} e : \sigma_p$ and $\text{cur}(p, U) \sqcup \text{cur}(pc, U) \subseteq \ell$.

**Case $v = (v_1 | v_2)$**: We have protected($p, S$) and so $\ell \neq L$.

**Case $v \neq (v_1 | v_2)$**: In this case $\ell = \{L, H\}$.

In the both the cases, we have

$$\text{obsOverlap}(\hat{t}, t^*_{pre}, t^*_{obs}, t^*_{post})_1 \approx_L \text{obsOverlap}(\hat{t}, t^*_{pre}, t^*_{obs}, t^*_{post})_2$$

**Case ESq-If-Else**: Given $pc, \mu, \Gamma, U \vdash_\delta \mathcal{E}_1^{chaos} (\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) : \Gamma', K' \triangleright \Box$ and $\mu \vdash \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle \Downarrow^2 \mathcal{E}_1^{chaos} r; m'; K' \triangleright t^*$. Let $\hat{t} = t^*$. Since $\mu \vdash_\delta \langle c, r, m, K \rangle \Downarrow^2 v$ such that $v$ is not a pair, applying induction hypothesis to the premises of ESQ-IF-ELSE gives us

$$\text{obsOverlap}(\hat{t}, t^*_{pre}, t^*_{obs}, t^*_{post})_1 \approx_L \text{obsOverlap}(\hat{t}, t^*_{pre}, t^*_{obs}, t^*_{post})_2$$
Case ESq-While: Given $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (where $e \text{ do } c, r, m, K$) : $\Gamma, K \cdot \text{ok}$ and $\mu \vdash \langle e \text{ do } c, r, m, K \rangle \cdot \psi_{E_1}^{2}$ and $K \vdash v$. From the premises of T-ESq-CONFIG, we have $K = K' = K''$. Since $\mu \vdash \langle e, r, m, K \rangle \cdot \psi_{E_1}^{2}$ $v$ such that $v$ is not a pair, applying induction hypothesis to the premise of ESQ-WHILE gives us

$$\{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

From Lemma 22 we have $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (while $e \text{ do } c, r', m', K$) : $\Gamma, K \cdot \text{ok}$. Applying induction hypothesis to $\mu \vdash \langle e \text{ do } c, r', m', K \rangle \cdot \psi_{E_1}^{2}$ $r'; m'; K' \triangleright v'$. Hence

$$\{ \text{obsOverlap}(t'', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t'', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

Case ESq-Call: Given $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (call$(e), r, m, K$) : $\Gamma', K' \cdot \text{ok}$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \cdot \psi_{E_1}^{2}$ $v$ such that $v$ is a pair, we have protected$_{1}(p, S)$. From the well-typedness, neither $c_1$ nor $c_2$ do emit any out events to $L$ channel. Hence

$$\{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

Case ESq-If-Div: Given $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (if $e$ then $c_2 \text{ else } c_3, r, m, K$) : $\Gamma', K' \cdot \text{ok}$ and $\mu \vdash \langle \text{if } e \text{ then } c_2 \text{ else } c_3, r, m, K \rangle \cdot \psi_{E_1}^{2}$ $v$ such that $v$ is a pair, we have protected$_{1}(p, S)$. From the well-typedness, command $c$ does not emit any out events to $L$ channel. Hence

$$\{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

Case ESq-While-Div: Given $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (while $e \text{ do } c, r, m, K$) : $\Gamma, K \cdot \text{ok}$ and $\mu \vdash \langle e \text{ do } c, r, m, K \rangle \cdot \psi_{E_1}^{2}$ $v$ such that $v$ is a pair, we have protected$_{1}(p, S)$. From the well-typedness, command $c$ does not emit any out events to $L$ channel. Hence

$$\{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

Case ESq-Call-Div: Given $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (call$(e), r, m, K$) : $\Gamma', K' \cdot \text{ok}$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \cdot \psi_{E_1}^{2}$ $v$ such that $v$ is a pair, we have protected$_{1}(p, S)$. From the well-typedness, command $c$ does not emit any out events to $L$ channel. Hence

$$\{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t', t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

Case ESq-Seq: Given $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (c$; \ldots; c_n, r_0, m_0, K_0$) : $\Gamma_n, K_n \cdot \text{ok}$ and $\mu \vdash \langle c_1; \ldots; c_n, r_0, m_0, K_0 \rangle \cdot \psi_{E_1}^{2}$ $v$ such that $v$ is not a pair, applying induction hypothesis to the premise of ESQ-SEQ gives us

$$\{ \text{obsOverlap}(t, t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t, t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

From Lemma 22 we have $pc, \mu, \Gamma, U \vdash_{\delta_1} \varphi$ (c$; r_1, m_1, K_1$) : $\Gamma_2, K_2 \cdot \text{ok}$. Applying induction hypothesis to the next premise, $\mu \vdash \langle c_2, r_1, m_1, K_1 \rangle \cdot \psi_{E_1}^{2}$ $v$ such that $v$ is not a pair, applying induction hypothesis to the premise of ESQ-SEQ gives us

$$\{ \text{obsOverlap}(t, t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t, t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$

Applying the inductive hypothesis continuously thus gives,

$$\{ \text{obsOverlap}(t_n, t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{1} \approx_{L} \{ \text{obsOverlap}(t_n, t_{\text{pre}}^{*}, t_{\text{obs}}^{*}, t_{\text{post}}^{*}) \}_{2}$$
Case ESq-Enclave: Given $pc, \mu, \Gamma, U \vdash_{\deltaSHm0,N,ch} \langle enclave(i, c), r, m, K \rangle : \Gamma', K' \bullet ok$ and $N \vdash \langle enclave(i, c), r, m, K \rangle \bullet \frac{1}{2} E_{t\text{-\chaos}} r'^* ; m'^* ; K' \triangleright t'^* \bullet$. From the premises of T-ESQ-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_{\deltaSHm0,E^i} \langle enclave(i, c) \rangle : \Gamma', K'$. From Lemma 23, we have $pc, \Gamma, \emptyset \vdash_{\deltaSHm0,N,ch} \langle c, r, m, K \rangle : \Gamma', K' \bullet ok$. Applying induction hypothesis to the premise $E_i \vdash \langle c, r, m, K \rangle \bullet \frac{1}{2} E_{t\text{-\chaos}} r'^* ; m'^* ; K' \triangleright t'^*$,

$$\lfloor obsOverlap(t', t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*) \rfloor_1 \approx_L \lfloor obsOverlap(t', t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*) \rfloor_2$$

Since we have $L, N, \Gamma, \emptyset \vdash_{\deltaSHm0,N,ch} \langle c, r_{\text{init}}, m, \emptyset \rangle : \Gamma' \bullet ok$, applying Lemma 23 on $\mu \vdash \langle c, r_{\text{init}}, m, K \rangle \bullet \frac{1}{2} E_{t\text{-\chaos}} r'^* ; m'^* ; K' \triangleright t'^* \bullet$, we have

$$\lfloor obsOverlap(t', t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*) \rfloor_1 \approx_L \lfloor obsOverlap(t', t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*) \rfloor_2$$

Hence proved that $m_2 \in k_L(E_{t\text{-\chaos}}(c, t_{\text{obs}}))$.

E.2 Translation is Sound

Lemma 24. Let $G$ be an IMPS type environment that corresponds to $\gamma$ and is well-typed for $\delta$. Also let $pc, G, \emptyset \vdash c: G'$ and $c_{\text{sub}}$ is a sub-command of $c$. If $pc', G, U \vdash c_{\text{sub}}: G'$ such that $U \neq \emptyset$ then $\exists c', c_1, c_2, \text{cnd.}$ such that $c'$ is a sub-command of $c$ and $c_{\text{sub}}$ is a sub-command of $c_1$.

Proof. Given $pc, G, \emptyset \vdash c: G'$. It is easy to see that the only typing judgments that add to the set $U$ for the subcommands are T-FUNCTION and T-IF-ISUNSET. The remaining judgments T-ASSIGN, T-UPDATE, SEQ, T-IF-ELSE T-WHILE, T-SETCND, T-CALL and T-KILL do not change the set $U$ for their subcommands. Rule T-ENCLOSE nullifies the set $U$ for its subcommands. Also given $pc', G, U \vdash c_{\text{sub}}: G'$ such that $U \neq \emptyset$. This is possible only if $c_{\text{sub}}$ is a sub-command for some $\{ \text{if isunset(cnd)} \}$ then $c_1$ else $c_2, \lambda, c_1$.

Hence proved.

We now present the proof for Theorem 2.

Proof. The proof is by mutual induction on the translation derivation of expressions and commands.

1. For all expressions $e \in \text{IMPS}$, if $G \vdash e: \sigma_p$ and $G, e, \sigma_p \rightarrow \mu, \Gamma, e', \sigma_p$ then $\mu, \Gamma \vdash e': \sigma_p$.
2. For all commands $c \in \text{IMPS}$, if, $pc, G, U \vdash c: G'$ and $pc, G, c' \rightarrow \Gamma, \delta, e', \Gamma'$ then $pc, \mu, \Gamma, K, U \vdash_{\delta} c': \Gamma', K'$.

Case TR-INT: Given $G, n, \text{int}_p \rightarrow \mu, \Gamma, \delta, n, \text{int}_p$. From T-INT, we have $\mu, \Gamma \vdash_{\delta} n : \text{int}_p$.

Case TR-VAR: Given $G, x, \sigma_p \rightarrow \mu, \Gamma, \delta, x, \sigma_p$. Hence $\Gamma(x) = \sigma_p$. From T-VAR, we have $\mu, \Gamma \vdash_{\delta} x : \sigma_p$.

Case TR-LOC: Given $G, l, (\sigma_p, \text{ref}_t)^q \rightarrow \mu, \Gamma, \delta, l, (\sigma_{p'}^{\text{ref}_t})^q$. From the premises, $\Gamma(l) = \sigma_p$ and $\delta(l) = \mu'$. From T-LOC, we thus have $\mu, \Gamma \vdash_{\delta} l : (\sigma_{p'}^{\text{ref}_t})^q$.

Case TR-CND: Given $G, cnd, \text{cond}_p \rightarrow \mu, \Gamma, \delta, cnd, \text{cond}_p$. From premise, $\delta(cnd) = \mu'$. Since $\text{cnd} \in \text{Cond}$, from T-CND, we thus have $\mu, \Gamma \vdash_{\delta} \text{cond}_p : \text{cond}_p$.

Case TR-DREF: Given $G, \ast e, \sigma_{\text{pliq}} \rightarrow \mu, \Gamma, \delta, e', \sigma_{\text{pliq}}$. Applying induction hypothesis to the premise, we have $\mu, \Gamma \vdash_{\delta} e' : (\sigma_{p'}^{\text{ref}_t})^q$. Also, $\mu' \neq N \implies \mu = \mu'$. From T-DREF, we thus have $\mu, \Gamma \vdash_{\delta} \ast e : \sigma_{\text{pliq}}$.

Case TR-ISUNSET: Given $G, \text{isunset}(cnd), \text{int}_p \rightarrow \mu, \Gamma, \delta, \text{isunset}(cnd), \text{int}_p$. From the premises, $\delta(cnd) = \mu' \neq N \implies \mu = \mu'$. From T-ISUNSET, we thus have $\mu, \Gamma \vdash_{\delta} \text{isunset}(cnd) : \text{int}_p$.

Case TR-FUNCTION: Given $G, \lambda, c, (G^-, U \rightarrow^p G^*) \rightarrow \mu, \Gamma, \delta, \lambda^u, e', (\Gamma^-, K^-, U \rightarrow^p \Gamma^+, K^+)^q$. Since $G \vdash \lambda, c: G^-, U \rightarrow^p G^*$, we have $q = L$. Applying induction hypothesis to the premise, we have $p, \mu, \Gamma, K^-, U \vdash_{\delta} c : \Gamma^+, K^+$. Since, We also have $q = L$. From T-FUNCTION, we thus have $\mu, \Gamma \vdash_{\delta} \lambda^u, c : (\Gamma^-, K^-, U \rightarrow^p \Gamma^+, K^+)^L$.

Case TR-OP: Given $G, e_1 \oplus e_2, \sigma_{\text{pliq}} \rightarrow \mu, \Gamma, e', e_2, \sigma_{\text{pliq}}$. Applying induction hypothesis to the premises, we have $\mu, \Gamma \vdash_{\delta} e_1 : \text{int}_p$ and $\mu, \Gamma \vdash_{\delta} e_2 : \text{int}_p$. From T-OP, we thus have $\mu, \Gamma \vdash_{\delta} e_1 \oplus e_2 : \text{int}_p$.

Case TR-SKIP: Given $pc, G, U, \text{skip}, \rightarrow \mu, \Gamma, \delta, \text{skip}, \Gamma, K$. From T-SKIP, we thus have $pc, \mu, \Gamma, K, U \vdash_{\delta} \text{skip} : \Gamma, K$. 


Case TR-ASSIGN: Given \( pc, G, U, x := e, G[x \mapsto \sigma_{pc\cup \{\mu\}}] \vdash \mu, \Gamma, K, \delta, x := e', \Gamma[x \mapsto \sigma_{pc\cup \{\mu\}}], K \). From the well-typedness of IMPS expression \( e \), i.e. \( G \vdash e : \sigma_{pc} \), we have \( q \neq \top \). Applying induction hypothesis to the premise we have \( \mu, \Gamma \vdash e' \vdash : \sigma_{q} \). From the premises, \( (pc \cup q) \not\subseteq L \implies \mu \neq N, \mu \not\subseteq K \) and T-ASSIGN, we thus have \( \mu, \Gamma, K, U \vdash x := e' : \Gamma[x \mapsto \sigma_{pc\cup \{\mu\}}], K \).

Case TR-DECLASSIFY: Given \( L, G, U, x := \text{declasify}(e), G[x \mapsto \sigma_{L}] \vdash \mu, \Gamma, K, \delta, x := \text{declasify}(e'), \Gamma[x \mapsto \sigma_{L}], K \). From the well-typedness of IMPS expression \( e \), i.e. \( G \vdash e : \sigma_{L} \), we have \( q \neq \top \). Applying induction hypothesis to the premise we have \( \mu, \Gamma \vdash e' \vdash : \sigma_{q} \). From the premises, \( (pc \cup q) \not\subseteq L \implies \mu \neq N, \mu \not\subseteq K \) and T-DECLASSIFY, we thus have \( \mu, \Gamma, K, U \vdash x := \text{declasify}(e') : \Gamma[x \mapsto \sigma_{L}], K \).

Case TR-OUTPUT: Given \( pc, G, U, \) output \( e \) to \( e, G \), we have \( p \neq \top \). From the well-typedness of IMPS expression \( e \), i.e. \( G \vdash e : \sigma_{pc} \), we have \( (pc \cup q) \not\subseteq \top \) and T-OUTPUT, we thus have \( \mu, \Gamma, K, U \vdash output e' \vdash : \Gamma, K \).

Case TR-SETCOND: Given \( pc, G, U, \) set \( (cnd) \), \( G \vdash \mu, \Gamma, K, \delta, \) set \( (cnd) \), \( K \). From the well-typedness of IMPS command set(condvar), i.e. \( pc, G, U \vdash \) set \( (cnd) \) : \( G \), we have \( cnd \in \text{Cond} \setminus U \). From the premises and T-SETCOND, we thus have \( \mu, \Gamma, K, U \vdash \text{set}(cnd) : \Gamma, K \).

Case TR-UPDATE: Given \( pc, G, U, e_1 \leftarrow \delta, G \), \( \mu, \Gamma, K, \delta, e_1 \leftarrow e_2 \), \( G \), we have \( p, p', q \neq \top \). Applying induction hypothesis to the premises, we have \( \mu, \Gamma \vdash e_1 : (\sigma_{p'}^{\text{ref}^*}) \) and \( \mu, \Gamma \vdash e_2 : \sigma_{p'} \). From the remaining premises and T-UPDATE, we thus have \( \mu, \Gamma, K, U \vdash e_1 \leftarrow e_2 : \Gamma, K \).

Case TR-SEQ: Given \( pc, G_0, U, e_1 : \vdots : e_n, G_n \vdash \mu_0, \Gamma_0, K_0, \delta, e', \Gamma_n, K_{n+1} \). Applying induction hypothesis to the premises, we have \( \forall i \in \{1 : \ldots : n\}, pc, \mu_0, \Gamma_0, K_0, U \vdash e_i : \Gamma_i, K_i \).

Consider the case when processSeqOutput\((\mu_0, \Gamma_0, K_0, \delta, \nu, \mu, \Gamma, K, U) \) matches \((\mu_0, \mu_1, \mu_2, \mu_3) \) when \( (\mu_0, \mu_1, \mu_2, \mu_3) \) at some \( (\delta, \mu, \Gamma, K, U) \) in \( Cond \). From the well-typedness of \( \mu_0 \), \( \mu_1 \), \( \mu_2 \), \( \mu_3 \), \( \Gamma_0 \), \( \Gamma_1 \), \( \Gamma_2 \), we have \( \mu_0 \neq \top \). Applying induction hypothesis to the premises, we have \( \mu_0 \neq \top \). From the remaining premises and T-SEQ, we thus have \( \mu_0, \mu_1, \mu_2, \mu_3 \in Cond \setminus U \).

Case TR-IF-ELSE: Given \( pc, G, U, \) if \( e \) then \( c_1 \) else \( c_2 \), \( G \), \( \mu, \Gamma, K, \delta \), if \( e' \) then \( c_1' \) else \( c_2' \). Applying induction hypothesis to the premises, we have \( \mu, \Gamma \vdash e' \vdash : \int_{pc} \) and \( pc', \mu, \Gamma, K, U \vdash c_i : \Gamma'_i, K'_i \) for \( i = 1, 2 \). From the remaining premises and T-IF-ELSE, we thus have \( \mu, \Gamma, K, U \vdash e : \int_{pc} \) and \( pc', \mu, \Gamma, K, U \vdash c_i : \Gamma'_i, K'_i \) for \( i = 1, 2 \).

Case TR-IF-ISUNSET: Given \( pc, G, U, \) if isunset \( (cnd) \) then \( c_1 \) else \( c_2 \), \( \mu, \Gamma, K, \delta \), if unset \( (cnd) \) then \( c_1' \) else \( c_2' \). Applying induction hypothesis to the premises, we have \( \mu, \Gamma \vdash \text{isunset}(cnd) \vdash : \int_{pc} \) and \( pc', \mu, \Gamma, K, U \vdash c_i : \Gamma'_i, K'_i \) for \( i = 1, 2 \). From T-IF-ISUNSET, we thus have \( \mu, \Gamma, K, U \vdash e \) if isunset \( (cnd) \) then \( c_1 \) else \( c_2 : \Gamma'_i, K'_i \).

Case TR-WHILE: Given \( pc, G, U, \) while \( e \) do \( c, G \), \( \mu, \Gamma, K, \delta \), while \( e' \) do \( c', \Gamma, K \). Applying induction hypothesis to the premises, we have \( \mu, \Gamma \vdash e ' : \int_{pc} \) and \( pc', \mu, \Gamma, K, U \vdash c : \Gamma', K \). From the remaining premises and T-WHILE, we thus have \( \mu, \Gamma, K, U \vdash e : \int_{pc} \) and \( pc', \mu, \Gamma, K, U \vdash c : \Gamma', K \).

Case TR-CALL: Given \( pc, G, U, \) call \( e \), \( G \), \( \mu, \Gamma, K, \delta, \) call \( (e'), G \), \( \mu_0, \Gamma_0, K_0 \), \( \mu \vdash e : (\Gamma', K', U \vdash e : (\Gamma', K', \mu_0, \Gamma_0, K_0)) \). From the remaining premises and T-CALL, we thus have \( \mu, \Gamma, K, U \vdash e : (\Gamma', K', U \vdash e : (\Gamma', K', \mu_0, \Gamma_0, K_0)) \).

Case TR-SUB: Given \( pc_2, G_2, U, c, G_2 \), \( \mu, \Gamma, K, \delta, e', \Gamma_2, K \). Applying induction hypothesis to the premise, we have \( pc_1, \mu_1, \Gamma_1, K, U \vdash c : \Gamma_1', K' \). Also from translation of typing environment in Figure\( [\text{10}] \) we have \( \vdash \delta \Gamma_1 \) ok for \( i = 1, 2 \).

From the remaining premises and T-SUB, we thus have \( pc_2, \mu_2, \Gamma_2, K, U \vdash c : \Gamma_2', K' \).