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, 25]). 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 an 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...
We present IMP2. We show that a security-type system for
by implementing several simple models
of applications with application-specific security guarantees.

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 instruc-
tions 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 en-
sure 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 mecha-
nisms place the onus on the programmer to secure an appli-
cation by effectively decoupling the security-critical parts of
the application from the non-critical and/or untrusted parts
of the application. Hardening an application to carefully iso-rate the dependencies requires non-trivial effort.

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 en-
force expressive confidentiality policies (including era-
sure policies and delimited release policies) against sev-
eral attackers, including attackers that can arbitrarily cor-
rupt non-enclave code, and, under certain circumstances,
corrupt enclave code (Sections 3 and 4).

3. We present a translation from a non-enclave source lan-
guage 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 ap-
propriate placement of code and data into enclaves to en-
sure security guarantees against powerful low-level at-
tackers. The translation can be configured to optimize
various criteria, including reducing the size of the trusted
computing base, reducing the runtime performance im-
pact of using enclave mechanisms, or removing erased
data as soon as possible.

In addition, we validate the translation and the expres-
siveness 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 \( \mathcal{L} = \{L, H, T\} \) to express
confidentiality restrictions on information. Security level \( L \)
(“low security”) is for public information that anyone, in-
cluding 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 \( T \) is
for information so confidential that no-one is permitted to
learn it. Ideally, the system never contains information with
security level \( T \).

Let partial order \( \sqsubseteq \) be the smallest reflexive and transitive
relation such that \( L \subseteq H \) and \( H \subseteq T \). 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, informa-
tion needs to become more confidential.

Security policies describe how the security level of infor-
mation must change over time. A security level policy \( \ell \) sim-
ply means that information must be handled with security
level \( \ell \) at all times. An erasure policy \( \ell_1 \leftarrow cnd \wedge \ell_2 \) means that
initially information can be handled according to security
level \( \ell_1 \). However, when condition \( cnd \) is met, the informa-
tion 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, con-
ditions for erasure can be arbitrary state predicates. How-
ever, 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 respon-
sible 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 expres-
sive and simplifies specification and reasoning about erasure
policies.

We write \( P \) to denote the set of policies, and use metavari-
ables \( p, q \) 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 \( L \leftarrow end \wedge \ell \). The
policy says that the confidentiality level of password is
initially \( L \), and once end is set, it must be \( \ell \).
\[ e ::= n \mid x \mid e_1 \oplus e_2 \mid l \mid \ast e \mid \text{isunset}(\text{cnd}) \mid \lambda^\mu.c \]

\[ v ::= \lambda^\mu.c \mid n \mid l \]

\[ c ::= \text{skip} \mid x := e \mid x := \text{declassify}(e) \mid e_1 \leftarrow e_2 \mid \text{output } e \text{ to } \ell \mid \text{call}(e) \mid \text{set}(\text{cnd}) \mid \text{enclave}(i,c) \]

\[ l \in \text{Loc} \quad \text{cnd} \in \text{Cond} \quad \text{Cond} \subseteq \text{Loc} \]

\[ x \in \text{Vars} \quad i,n \in \mathbb{N} \]

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

**Figure 1. IMPE Syntax**

### 2.2 Syntax

IMPE 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 IMPE, 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 IMPE. 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 IMPE include integers, memory locations (including conditions), and first-class functions.

Commands in IMPE include standard imperative commands (\( \text{skip}, x := e, \text{if } e \text{ then } c_1 \text{ else } c_2, \text{ while } e \text{ do } c \)). 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 \( e_1 \) 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 \( \text{output } e \text{ to } \ell \) 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 5.2) 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 \( E_i,\ldots \) 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 \( (c,v,m,K) \) describes the current state of the system. Command \( c \) is the rest of the program to execute. Register file \( v \) 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 `δ(l) ∈ {N, µ} \ K` states that in normal mode (i.e., `µ = N`), only normal locations can be read; in enclave mode `E_i` (i.e., `µ = E_i`), both normal and enclave `E_i` locations may be read (i.e., `δ(l) ∈ {N, E_i}`). Locations from a different enclave cannot be read, and if an enclave has been killed (`E_i ∈ K`), then no locations in that enclave can be read.

Rule `IsUnset` 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 `µ` on function `λ^µ.c` equals the mode of the expression evaluation.

Figure 3 shows the inference rules for command execution. Many rules have the premise `µ /∈ 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 `r[x \mapsto v]` for the register file that maps `x` to `v` but otherwise is the same as `r`. 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 `ℓ`, and adds events `Mem(m)` and `Out(ℓ, v)` to the trace.

Rule `Enclave` executes enclave code. Note that enclaves can be entered only from normal mode (i.e., mode `µ` 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.
Rule `Kill` tears down enclave $E_i$ and adds it to the kill set. Once an enclave is killed, it is inactive and can no longer be used. Enclaves can be killed only in normal mode.

The following code illustrates how password authentication can be modeled in IMPE.

```
enclave(1, status := *password = *guess);
output status to L
```

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 $E_1$.

### 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.
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 \( \gamma(l) = \ell_1 \cap \ell_2 \) and \( m \) is the memory from which we start an execution, then we should enforce erasure policy \( \ell_1 \cap \ell_2 \) on the data in \( m(l) \). We say that a security specification \( \gamma \) is well-formed if \( \forall l \in \text{Loc}, \gamma(l) \neq T \) (since security level \( T \) is for information so confidential that it should not be on the machine).

### 3.1 Attacker Knowledge

We associate an attacker with a security level \( \ell \in \mathcal{L} \) and assume the attacker is able to observe outputs on any channel \( \ell' \) such that \( \ell' \subseteq \ell \). Given trace \( t \), \([t]_\ell\) is the output events that an attacker at level \( \ell \) can observe.

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

Given an execution of program \( c \), an attacker at level \( \ell \) observes some portion of the execution (i.e., some subsequence \( t_{obs} \) 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 \( t_{obs} \). 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. [27] 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 \( t_{obs} \), attacker knowledge is defined as:

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

Consider the password authentication example. Let \( c \) be the program, \( m_0 \) be the initial memory and \( t_{obs} = \text{Mem}(m_0) \cdot \text{Out}(L, 1) \) 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, \( k_L^{\Downarrow_{\text{kind}}}(c, t_{obs}) = \{ m' \mid m'(\text{password}) = m'(\text{guess}) \} \).

### 3.2 Security

The intuition for knowledge-based security conditions [5][7] 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 \( \ell_1 \cap \ell_2 \) 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.

**Permitted 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 \( \ell_1 \cap \ell_2 \), then we should enforce security level \( \ell_1 \) if \( \text{cond} \in U \) and enforce \( \ell_2 \) if \( \text{cond} \not\in U \). Formally:

\[
\text{cur}(p, U) = \begin{cases} 
\ell_1 & \text{if } p = \ell \\
\ell_2 & \text{if } p = \ell_1 \cap \ell_2 \text{ and } \text{cond} \in U \\
\ell & \text{if } p = \ell_1 \cap \ell_2 \text{ and } \text{cond} \not\in U
\end{cases}
\]

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., \( \text{cur}(\gamma(l), U) \sqsubseteq \ell \) ), 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:

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

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 \( \text{ind}_\ell(m_0, \gamma, U) \).

**Permitted knowledge via escape hatches** Deallocations 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 \( \text{Dec}(e, m) \) (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 \( e \), 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 \( \downarrow_{\text{kind}} \) and escape hatch \( e \), we define \( \text{Esc}_{\downarrow_{\text{kind}}}^{\downarrow_{\downarrow}}(m_0, m, e) \) as

\[
\{ m' \mid \exists \mu. \left( \mu \vdash_\delta \langle e, r_{\text{init}}, m_0, \emptyset \rangle \downarrow_{\text{kind}} v \land \mu \vdash_\delta \langle e, r_{\text{init}}, m, \emptyset \rangle \downarrow_{\text{kind}} v \right) \}
\]

Given semantics \( \downarrow_{\text{kind}} \), declassification event \( \text{Dec}(e, m) \), and initial memory \( m_0 \), \( \text{Esc}_{\downarrow_{\text{kind}}}^{\downarrow_{\downarrow}}(m_0, m, e) \) 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 \( [t]_{\text{mem}} = \{ m \mid \text{Mem}(m) \in t \} \) to be the set of memory events that occur in trace \( t \) and \( [t]_{\text{exec}} = \{ (e, m) \mid \text{Dec}(e, m) \in t \} \) 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 \( \text{Esc}_{\downarrow_{\text{kind}}}^{\downarrow_{\downarrow}}(m_0, m'', e) \) for \( (e', m') \in [t \cdot t_{\text{obs}}]_{\text{exec}} \) 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 \( \text{Esc}_{\downarrow_{\text{kind}}}^{\downarrow_{\downarrow}}(m_0, m', e') \) for \( (e', m') \in [t \cdot t_{\text{obs}}]_{\text{exec}} \) 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 \( \downarrow_{\text{kind}} \) if for all initial memories \( m_0 \) and all executions

\[
N \vdash_\delta \langle c, r_{\text{init}}, m_0, \emptyset \rangle \downarrow_{\text{kind}} r; m; K \triangleright t \cdot t_{\text{obs}} \cdot t'
\]

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

\[
\begin{align*}
R^\ell_\downarrow_{\downarrow_{\downarrow}}(c, t_{\text{obs}}) & \supseteq \\
\bigcap_{m' \in [t_{\text{obs}}]_{\text{mem}}} \bigcap_{(e', m') \in [t \cdot t_{\text{obs}}]_{\text{exec}}} \text{Esc}_{\downarrow_{\text{kind}}}^{\downarrow_{\downarrow}}(m_0, m', e')
\end{align*}
\]

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.

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

The program is insecure for the specification \( \gamma \), where \( \gamma(\text{guess}) = L \), 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 \( \downarrow \), 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:

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

The declassification event induces a new lower bound: \( \{ m' \mid m'(\text{password}) = m'(\text{guess}) \} \) 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).
The program is secure at level \( L \) change to command \( \vdash \). Consider the following program, where \( \delta \) the trace (and we modify \( \lfloor \) include all rules from Figure 3 (appropriately adapted) and the rule in Figure 4. This new rule allows command \( c \) to change to an arbitrary command \( c' \), so long as both programs have the same enclave code, expressed by relation \( c \equiv c' \) (defined in Appendix A). This corresponds to an attacker that can exploit a vulnerability in non-enclave code but is unable to corrupt code within enclaves. Since modifying the program is a security relevant action, an event \( A(c \equiv c') \) is emitted to the trace (and we modify \( \lfloor t \rfloor \) to include events of the form \( A(c \equiv c') \)).

If a program is secure for \( \downarrow \) then it is secure for \( \downarrow \). The converse does not necessarily hold. For example, consider the following program, where \( \delta(hi) = E_1 \) and \( \gamma(hi) = H \).

\[
c \equiv \text{enclave}(1, x := \ast hi); \text{output } 1 \text{ to } L
\]

The program is secure at level \( L \) for specification \( \gamma \) and semantics \( \downarrow \) but is insecure for semantics \( \downarrow \). Suppose the active attacker modifies the program to \( c' \equiv \text{enclave}(1, x := \ast hi); \text{output } x \text{ to } L \). Note that \( c \equiv c' \), since the code in enclaves for both \( c \) and \( c' \) is the same: \( \text{enclave}(1, x := \ast hi) \). Suppose we execute \( c' \) with an initial memory that maps \( hi \) to 42. The knowledge of an attacker observing output on channel \( L \) is \( \{ m' \mid m'(hi) = 42 \} \). However the permitted lower bound on attacker’s knowledge is the set of all initial memories (i.e., the attacker is not permitted to learn anything about the confidential data). So the program is not secure at level \( L \) for \( \gamma \) and \( \downarrow \).

**Enclave active attacker** Given a set of enclaves \( I \subseteq \{ E_1, E_2, \ldots \} \), relation \( \downarrow \) allows the attacker to arbitrarily change (enclave and non-enclave) code but only after all enclaves in \( I \) are killed. This corresponds to a setting where enclaves and non-enclave code all have exploitable vulnerabilities but the attacker does not immediately exploit these vulnerabilities.

Inference rules for judgment \( \vdash \langle c, r, m, K \rangle \) \( E_1 \)-chaos \( r' \); \( m' \) ; \( K' \triangleright t' \) include all inference rules from Figure 3 (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 \( \lfloor t \rfloor \) to include events of the form \( A(c') \)).

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

\[
\text{enclave}(1, \text{output } \ast \text{ccard to } H; \text{set(}\text{end})\}; \text{kill}(1)
\]

The program outputs the contents of ccard to the \( H \) channel and sets condition cond 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 \( \downarrow \), 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 ccard. 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 \([38]\) for IMPE that guarantees security, i.e., a well-typed program is secure against all the attackers described in Section 3.3.

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 \( \tau^\mu \) 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. Reference types 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 \( \Gamma^+, K', U \vdash_{\delta} \Gamma^+, K' + \) after explaining the type judgment.

A security type \( \tau = \tau_p \) is a base type \( \tau \) annotated with a security policy \( p \). Intuitively, data with type \( \tau_p \) 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 \( \text{cond}^\text{p} \), 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 \( \vdash_{\delta} \Gamma \text{ ok} \), if

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

and

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

The IMPE 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 (\( \mu = N \)) 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 \( \Gamma^+, K', U \vdash_{\delta} \Gamma^+, K' + \) 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 \( \cup \) 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 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 location which is dereferenced and the contents of that location. Thus in rule T-Deref the result of a +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 \( \mu' \neq N \implies \mu = \mu' \) (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-
easily adapted to enable syntax-directed type-checking algorithms.

This prevents non-enclave attackers from violating security policy.

A function and violating the assumption on set current kill set and unset conditions, and that the assumption that can control non-enclave execution is unable to violate an assumption made by enclave code. Also, premise isVarLowContext(Γ') 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 (µ = 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 ∉ 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-SETCND checks that condition con can be set only if it is not currently assumed to be unset, i.e., con ∉ 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 (∀y ∈ dom(Γ'), Γ(y) ≤ Γ'(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 ≠ ∅ ⇒ µ ≠ 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: ∀y ∈ dom(Γ'), Γ'(y) ≤ Γ_out(y). Since Γ− and Γ+ are partial, we require that the types of variables not in dom(Γ') (which is a superset of dom(Γ−)) remain unchanged: ∀y ∈ dom(Γ) \ dom(Γ'). Γ(y) = Γ_out(y).

After the function invocation, the kill set is K'.
Let \( \gamma \) be a well-formed security specification and \( \Gamma \) be a type environment that corresponds to \( \gamma \) and is well-typed for \( \delta \), the type system is sound. That is, a well-typed program is secure against all the attackers described in Section 3.3.

**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 \( \downarrow \); and
- \( c \) is secure at security level \( L \) for specification \( \gamma \) and semantics \( \downarrow_{N, \text{chaos}} \); and

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

**Command** \( c \) is secure at security level \( H \) for specification \( \gamma' \) and semantics \( \downarrow_{E_1, \text{chaos}} \).

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-
tacker characterized by semantics \( \downarrow_{E_{\text{chaos}}} \), but can not provide guarantees about information placed in other enclaves.

5. IMPs: A Non-enclave Calculus

Enclaves are a powerful mechanism, but management of enclaves may be error prone and distract the programmer from implementing correct functionality. We present a language IMPs that is similar to IMPE but removes all enclave-related commands and abstractions and thus allows the programmer to focus on functionality and high-level security requirements. In Section 6 we translate from IMPs to IMPE, automatically inferring appropriate enclaves.

The syntax for IMPs (Figure 9) is similar to IMPE, except that functions are not annotated with mode and commands `enclave(i, c)` and `kill(i)` are removed. An IMPs configuration is a triple \( \langle c, r, m \rangle \) where \( r \) and \( m \) are a register file and memory, respectively, as defined in Section 2.3.

The large-step semantic judgment for IMPs has the form \( \langle c, r, m \rangle \downarrow_s r', m' > t' \), meaning configuration \( \langle c, r, m \rangle \) executes and terminates with register file \( r' \) and memory \( m' \) and during execution produces trace \( t' \). The judgment for expression evaluation is \( \langle e, r, m \rangle \downarrow_s v \) and can be read as given register file \( r \) and memory \( m \), expression \( e \) evaluates to value \( v \). Inference rules for these judgments are straightforward, and similar to those of IMPE, although without any restrictions based on modes.

Types in IMPs (Figure 9) are similar to those of IMPE. We underline types and type metavariables to distinguish them from IMPE types. Unlike IMPE, conditions and references do not have mode annotations, and function types have neither mode nor kill set annotations. We use \( \mathcal{G} \) to denote type environments in IMPs. A type environment \( \mathcal{G} \) is well-typed if it does not map any location to type \( \sigma_T \). Similar to \( \Gamma \), we say that type environment \( \mathcal{G} \) corresponds to security specification \( \gamma \), if \( \mathcal{G} \) maps all variables to \( \text{int}\_\gamma \) and policies on locations agree with \( \gamma \).

The type system is a simplified version of the IMPE type system. Judgment \( pc, \mathcal{G}, U \vdash c: \mathcal{G}' \) means that command \( c \) is well-typed, where \( \mathcal{G} \) and \( \mathcal{G}' \) 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

\[
\text{pc}, \mathcal{G}, U, c, \mathcal{G}' \leadsto \mu, \Gamma, K, \delta, e', \Gamma', K'.
\]

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

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

\[
\mathcal{G}, e, \sigma_p \leadsto \mu, \Gamma, \delta, e', \sigma_p\text{ where } e \text{ is an IMPs expression such that } \mathcal{G} \vdash e : \sigma_p\text{ holds and } e' \text{ is the translated IMPE expression such that, provided the constraints are satisfied, } \mu, \Gamma \vdash_{\mathcal{G}} e' : \sigma_p\text{ holds.}
\]

The judgment for translating base types is \( \sigma \leadsto_{\delta} \sigma \). 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 \( \forall l \in \text{dom}(\mathcal{G}). \mathcal{G}(l) = (\sigma_p, \sigma) \land p \not\subseteq L \implies \delta(l) \neq N \) ensures that all confidential locations
have appropriate enclave assignments (even if these locations are not used by the program).

Figure 10 shows the translation for expressions. Translation for expressions proceeds by first translating the types. They enforce the invariant that a location in enclave $E_i$ is accessed in the same mode $E_i$. Rules TR-INT, TR-VAR, TR-LOC, TR-CND, and TR-OP are straightforward.

Rule TR-DEREF translates a dereference expression. The premise $\mu' \neq N \implies \mu = \mu'$ generates a conditional constraint such that if the dereferenced location is in an enclave ($\mu' \neq N$) then the expression is evaluated in the same enclave ($\mu = \mu'$). Similarly, rule TR-ISUNSET ensures that if a condition location is dereferenced, then the mode in which the expression is evaluated is appropriate.

Rule TR-FUNCT requires that if the post type environment $\Gamma^+$ has any variables with policies more restrictive than $L$ (isVarLowContext($\Gamma^+$)), then the function is defined in an enclave ($\mu \neq N$). Intuitively, any data left in variables at the end of the function invocation may be observable by the code that invoked the function. If that data includes confidential information, then the function should not be invoked by non-enclave code.

Figure 12 shows the inference rules for translating commands. Most of these rules are straightforward and closely follow the premises of the corresponding typing rules. Premise $\mu \notin K$ occurs in many of the rules, and ensures that code in killed enclaves cannot be executed.

Rule TR-SEQ drives the entire translation. Intuitively, given a sequence $c_1; \ldots; c_n$, it translates each sub-command $c_i$ by assigning them a different mode variable $\mu_i$. If the translation infers that $\mu_0 = N$ but $\mu_i \neq N$, then the translated sub-command $c_i'$ is placed inside an enclave. Variable $K_i$ is the kill set immediately before the execution of $c_i'$. $K_i'$ is the kill set immediately after the execution of $c_i'$, and $K_i''$ is the set of enclaves (if any) that can be safely killed after executing $c_i'$. Thus, we have that $K_i+1 = K_i' \cup K_i''$.

Constraint $K_i' \cap K_i'' = \emptyset$ ensures that an enclave is not killed more than once. Constraint $\mu_0 \neq N \implies (\mu_0 = \mu_i \land K_i'' = \emptyset)$ states that if sequence executes entirely in an enclave ($\mu_0 \neq N$) then all sub-commands are in the same enclave and no enclaves are killed. Constraint $\mu_i \neq N \land \mu_i = \mu_i+1 \implies K_i'' = \emptyset$ ensures that no enclave can be killed between sequences executing in same enclave.

Constraint $\mu_i \neq N \land (\mu_i \neq \mu_i+1 \land K_i'' \neq \emptyset) \implies$ isVarLowContext($\Gamma_i$) ensures that if execution exits an enclave (i.e., if command $c_i'$ executes in an enclave, but the sequence itself is not in an enclave) then no variables contain 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 $c_i'$ if there is a mode change. Command kill($j$) is inserted after command $c_i'$ if $j \in K_i''$. 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.

Theorem 2 (Soundness of Translation). Let $\mathcal{G}$ 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 $pc, \mathcal{G}, U \vdash c: \mathcal{G}'$ and $pc, \mathcal{G}, K, c, \mathcal{G} \Rightarrow \mu, \Gamma, U, \delta, c', \Gamma', K'$ then $pc, \mu, \Gamma, K, U \vdash \delta c': \Gamma', K'$

Given a well-typed IMPs program and environment $\mathcal{G}$, 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-
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 LMPE can be expressed as a Boolean SAT instance, assuming that the mode set Mode = \{N, E1, E2, \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 IMPs program without any of them being clearly the “best” translation. Naively, we could try to place the entire program and all locations 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.\(^7\) 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., \(K_{i+1} = K_i' \cup K_i''\) 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.\(^24\)
TR-Skip
\[ \begin{align*}
G & \rightsquigarrow^\text{typ}_3 \Gamma, \mu \notin K \\
\text{pc}, G, U, \text{skip}, G & \rightsquigarrow \mu, \Gamma, K, \delta, \text{skip}, \Gamma, K \\
\end{align*} \]

TR-Assign
\[ \begin{align*}
\forall \mu, \Gamma, \delta, e', \sigma_q \\
G & \rightsquigarrow^\text{typ}_3 \Gamma, e, \sigma_q \rightsquigarrow \mu, \Gamma, \delta, e', \sigma_q \\
(\text{pc} \cup \mu) & \not\subseteq L \implies \mu \neq N \quad \mu \notin K \\
\text{pc}, \text{G}, U, x & := e, G[x \mapsto \sigma_{\text{pc} \cup \mu}] \rightsquigarrow \mu, \Gamma, K, \delta, x := e', \Gamma, x \mapsto \sigma_{\text{pc} \cup \mu}, K \\
\end{align*} \]

TR-Declasify
\[ \begin{align*}
\forall \mu, \Gamma, \delta, e', \sigma_q \\
G & \rightsquigarrow^\text{typ}_3 \Gamma, e, \sigma_q \rightsquigarrow \mu, \Gamma, \delta, e', \sigma_q \\
(\text{pc} \cup \mu) & \not\subseteq L \implies \mu \neq N \quad \mu \notin K \\
L, G, U, x & := \text{declassify}(e), G[x \mapsto \sigma_{L}] \rightsquigarrow \mu, \Gamma, K, \delta, x := \text{declassify}(e'), \Gamma, x \mapsto \sigma_{L}, K \\
\end{align*} \]

TR-Output
\[ \begin{align*}
G, e, \sigma_p & \rightsquigarrow \mu, \Gamma, \delta, e', \sigma_p \\
G & \rightsquigarrow^\text{typ}_3 \Gamma, \mu \notin K \\
\text{pc}, G, U, \text{out} e & \rightsquigarrow \ell, G \rightsquigarrow \mu, \Gamma, K, \delta, \text{output e'} to \ell, K \\
\end{align*} \]

TR-Update
\[ \begin{align*}
G, e_1, \sigma_p & \rightsquigarrow \mu, \Gamma, \delta, e_1', \sigma_p \\
G, e_2, \sigma_p & \rightsquigarrow \mu, \Gamma, \delta, e_2', \sigma_p \\
G & \rightsquigarrow^\text{typ}_3 \Gamma, \mu' \neq N \implies \mu = \mu' \\
\text{pc}, G, U, e_1 & \leftarrow e_2, G \rightsquigarrow \mu, \Gamma, K, \delta, e_1' \leftarrow e_2', \Gamma, K \\
\end{align*} \]

TR-If-Else
\[ \begin{align*}
G & \rightsquigarrow^\text{typ}_3 \Gamma, G, e, \text{int}_p \rightsquigarrow \mu, \Gamma, \delta, e', \text{int}_p \\
\text{pc}', G, U, c_2, G' & \rightsquigarrow \mu, \Gamma, K, \delta, e_2', \Gamma', K' \\
\text{pc} \cup \mu & \subseteq \text{pc}' \\
\text{pc} & \text{pc}' \\
\text{(isVarLowContext}(\mu') & \vee \text{pc} \subseteq \text{pc}') \\
\text{pm} & \mu \neq N \\
\text{pc} & \text{pc}' \\
G & \rightsquigarrow \mu, \Gamma, K, \delta, e', \Gamma, K \\
\text{pc}, G, U, \text{if e then c}_1 & \text{else c}_2, G' \rightsquigarrow \mu, \Gamma, K, \delta, \text{if e' then c}_1' \text{else c}_2', \Gamma', K' \\
\end{align*} \]

TR-If-Isunset
\[ \begin{align*}
G & \rightsquigarrow^\text{typ}_3 \Gamma, G, \text{isunset}(\text{cnd}), \text{int}_L \rightsquigarrow \mu, \Gamma, \delta, \text{isunset}(\text{cnd}), \text{int}_L \\
\text{pc}, G, U & \cup \{\text{cnd}\}, c_1, G' \rightsquigarrow \mu, \Gamma, K, \delta, e_1', \Gamma', K' \\
\text{pc}, G, U, c_2, G & \rightsquigarrow \mu, \Gamma, K, \delta, e_2', \Gamma, K' \\
\mu & \subseteq \{N\} \cup K \\
\text{pc}, G, U, \text{if isunset}(\text{cnd}) & \text{then c}_1 \text{else c}_2 , G' \rightsquigarrow \mu, \Gamma, K, \delta, \text{if isunset}(\text{cnd}) \text{then c}_1' \text{else c}_2', \Gamma', K' \\
\end{align*} \]

TR-While
\[ \begin{align*}
G & \rightsquigarrow^\text{typ}_3 \Gamma, G, \text{isunset}(\text{cnd}), \text{int}_p \rightsquigarrow \mu, \Gamma, \delta, e', \text{int}_p \\
\text{pc}, G, U, c, G & \rightsquigarrow \mu, \Gamma, K, \delta, e', \Gamma, K \\
\text{pc} \cup \mu & \subseteq \text{pc}' \\
\text{pc} & \text{pc}' \\
\text{pm} & \mu \neq N \\
\text{pc} & \text{pc}' \\
G & \rightsquigarrow \mu, \Gamma, K, \delta, e', \Gamma, K \\
\text{pc}, G, U, \text{while e do c} & \text{else c}', G \rightsquigarrow \mu, \Gamma, K, \delta, \text{while e' do c}', \Gamma, K \\
\end{align*} \]

TR-Call
\[ \begin{align*}
G & \rightsquigarrow^\text{typ}_3 \Gamma, G, \text{call}(e), G_{\text{out}} \rightsquigarrow \mu, \Gamma, K, \delta, \text{call}(e'), G_{\text{out}}, K_{\text{out}} \\
\text{pc}, G, U, \text{call}(e), G_{\text{out}} & \rightsquigarrow \mu, \Gamma, K, \delta, \text{call}(e'), G_{\text{out}}, K_{\text{out}} \\
\end{align*} \]

TR-SetCnd
\[ \begin{align*}
\delta & \rightsquigarrow \text{cnd}(\mu') \Rightarrow \mu' \neq N \implies \mu = \mu' \\
\text{pc} & = L \\
\mu & \notin K \\
\end{align*} \]

TR-Seq
\[ \begin{align*}
G, G & \rightsquigarrow^\text{typ}_3 \Gamma, G, U \cup c_1 \cup \{\text{cnd}\}, c_1, G' \rightsquigarrow \mu, \Gamma, K, \delta, e_1, \Gamma', K' \\
\text{pc}, G, U, c_2, G' & \rightsquigarrow \mu, \Gamma, K, \delta, e_2, \Gamma, K' \\
\mu & \subseteq \{N\} \cup K \\
\text{pc}, G, U, \text{if isunset}(\text{cnd}) \text{then c}_1 \text{else c}_2 , G' \rightsquigarrow \mu, \Gamma, K, \delta, \text{if isunset}(\text{cnd}) \text{then c}_1' \text{else c}_2', \Gamma', K' \\
\end{align*} \]

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, IMP is most heavily influenced by SGX. We discuss how IMP relates to SGX.

First, we assume that enclaves are isolated from each other: code in enclave $E_i$ cannot 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 [7, 16, 34, 36]) to evaluate the expressiveness of security policies, and the translation from IMPs to IMP. The translator and case studies are available online [19]. All case studies are implemented as (well-typed) IMP programs which translate successfully to IMP 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 IMP and IMPs are extended as follows.

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

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

An array is a sequence of locations with the constraint that all elements of the array are in the same enclave (or all elements are in no enclave). IMP array type $\tau^\mu \parallel \tau^\nu$ indicates an array that contains values of type $\tau$, mode $\mu$ indicates in which enclave (if any) the array is placed and $\nu$ 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.

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

\[
\text{kill}(1); \text{set}(\text{end}); \text{output status to L}
\]

The translation assigns enclave $E_1$ to locations password and guess (i.e., translated locations have types $\text{imp}_{E_1} \text{ref}_{\text{immut}}$ and guess : $\text{imp}_{E_1} \text{end} \text{op}^{\tau^\mu} \text{ref}_{\text{immut}}$). 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 [1, 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 $H \text{\ref{end}op}^{\tau^\mu} \text{\ref{immut}}$, 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
the initial memory contains several such documents. A
map
doc
as an array of confidential strings
partial counts are then combined. Each document is modeled
The program follows the map-reduce model, in which partial
takes a set of private documents, and computes word fre-
performance with TCB size.
entries and exits. If this is a concern, the translation could
array of pairs of words and the frequency of that word. The
wordcount
a specific word, and sums the partial counts of the word. The

while (i < numOps)
if (+ops[i] = “add”) then
    stack[top - 1] <- stack[top] + stack[top];
else if (+ops[i] = “sub”) then
    ...
    top := top - 1;
output *stack[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 (+ops[i] = “add”) then
    enclave(1, stack[top - 1] <-
    *stack[top - 1] + *stack[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:stringH []immuat, 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 wordcount : (string × int)H []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 poli-
cies $L$ and $H$ respectively. Row selection chooses all indices
of array name that are equal to key “alice”. Summing com-
putes the sum of all wages corresponding to the selected in-
dices.

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 trans-
lation 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, in-
spired 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 mes-
ages and the log the erasure policy $L \rightarrow \top$, which states that
the contents of log are erased when condition clear is set. The condition is set only when a “clear” command is is-
formed. 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 Compila-
tion 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 con-
fidentiality 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 pro-
gram: 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 se-
curity policies (erasure and declassification) that go beyond
noninterference. Their system doesn’t provide erasure guar-
antees. We target a single machine and use enclave mecha-
nisms that directly provide secure memory (instead of emu-
lating secure memory via cryptographic mechanisms). Both
our work and theirs shield the programmer from the mecha-
nisms 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 en-
claves (cf. security against non-enclave active attackers). We
believe that our target calculus IMPlE can be extended to pro-
vide 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 adver-
saries 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 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. [20] 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


A. Enclave Equivalence $\simeq_{enc}$

Enclave relation $\simeq_{enc}$ is used to characterize the ability of an active attacker. Intuitively, given commands $c$ and $c'$, we have $c \simeq_{enc} c'$ 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 IMPs programs $c_1$ and $c_2$ are enclave equivalent, denoted $c_1 \simeq_{enc} c_2$, 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 $c_1 = \text{enclave}(1, \text{output } 42 \text{ to } L)$ and $c_2 = l \gets 1; \text{enclave}(1, \text{output } 42 \text{ to } L)$, we have $\chi(c_1) = \chi(c_2) = \{(E_1, \text{output } 42 \text{ to } L)\}$. The programs $c_1$ and $c_2$ are thus enclave equivalent.

B. IMPs Type System

Figure 13 defines the relabeling relation $\leq$ on policies.

\[
\begin{align*}
\ell_1 \subseteq \ell_2 & \quad \frac{p_1 \leq \ell_2}{\ell_1 \subseteq \ell_2} \\
\ell_1 \subseteq \ell_2 & \quad \frac{p_1 \leq \ell_2^{\text{end} \mathcal{A}} \ell_2'}{\ell_1^{\text{end} \mathcal{A}} \ell_1' \leq p_2} \\
\ell_1 \subseteq \ell_2 & \quad \frac{\ell_1^{\text{end} \mathcal{A}} \ell_1' \leq \ell_2^{\text{end} \mathcal{A}} \ell_2'}{\ell_1' \leq p_2} \\
\ell_1 \subseteq \ell_2 & \quad \frac{\ell_1^{\text{end} \mathcal{A}} \ell_1' \leq \ell_2^{\text{end} \mathcal{A}} \ell_2'}{\sigma \leq \sigma'} \\
\sigma \leq \sigma' & \quad \frac{p \leq q}{\sigma_p \leq \sigma_q} \\
\sigma_p \leq \sigma_q & \quad \frac{\sigma \leq \sigma}{\Gamma_1 \subseteq \Gamma_2, U \overset{\sigma_1}{\rightarrow^r} \Gamma_1, K \subseteq \Gamma_2, U \overset{\sigma_2}{\rightarrow^r} \Gamma_2, K^+}
\end{align*}
\]

**Figure 13.** Policy ordering and subtyping

\[
\begin{align*}
\text{ST-Int} & : \quad \frac{\Gamma \vdash n : \text{int}_L}{\Gamma \vdash c : \text{cond}_L} \\
\text{ST-Cnd} & : \quad \frac{\Gamma \vdash c : \text{cond}_L}{\Gamma \vdash \text{ wisdom } : \text{cnd}_L} \\
\text{ST-Var} & : \quad \frac{\Gamma \vdash \text{ ref } : \text{ref}_q}{\Gamma \vdash e : \text{ref}_q} \\
\text{ST-Loc} & : \quad \frac{\Gamma \vdash (\text{ref}_q)}{\Gamma \vdash (\text{ref}_q)'} \quad \text{ST-Deref} \quad \frac{\Gamma \vdash e : \text{ref}_q}{\Gamma \vdash \text{ref}_q} \\
\text{ST-Op} & : \quad \frac{\Gamma \vdash \text{cond}_L}{\Gamma \vdash \text{int}_L} \\
\text{ST-Isunset} \quad \frac{\Gamma \vdash \text{cond}_L}{\Gamma \vdash \text{int}_L} \\
\text{ST-Function} \quad \frac{\Gamma \vdash \lambda c : \text{ int}_L}{\Gamma \vdash \text{int}_L} \\
\end{align*}
\]

**Figure 14.** IMPs typing rules for expressions

C. IMPs Type System

Subtyping for IMPs types closely follows the subtyping of IMPe types. Figures 14 and 15 describe the type system.

D. Pseudo Code

Function processKill inserts $\text{kill}(j)$ whenever an enclave $E_j$ is killed and function processSeqOutput wraps the largest sequence of code with mode $E_j$ in enclave$(j, \ldots)$.)

\[
\begin{align*}
\text{processKill}(K) &= \\
&\text{match } K \text{ with } \\
&\{ k \cup K' \rightarrow \text{kill}(k), \text{processKill}(K') \} \\
&\emptyset \rightarrow ()
\end{align*}
\]

\[
\begin{align*}
\text{processSeqOutput}(c'_{1:2}, \mu_0, \mu_{1:2}, \bar{K}_{1:2}) &= \\
&\text{match } (\mu_0, \mu_{1:2}, \bar{K}_{1:2}) \text{ with } \\
&\{ \mu', (\mu' \ldots \mu'), (\emptyset \ldots \emptyset) \rightarrow c'_{1:2} \} \\
&\{ N, (N, \mu_{2:2}), (K', \bar{K}_{2:2}) \rightarrow \}
\end{align*}
\]
<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
</table>
| **ST-Skip** | $G(x) = \sigma_q$ $\vdash e: \sigma_p$
| **ST-Assign** | $\text{pc}, G, U \vdash \text{skip: } G'$
| **ST-Declassify** | $G(x) = \sigma_q$ $\vdash e: \sigma_p$ $p \neq \top$
| **ST-Update** | $G' \vdash e_1: (\sigma_p \text{ ref}^t)_q$ $G' \vdash e_2: \sigma_{p'}$
| **ST-Seq** | $\forall i \in \{1 \ldots n\}$, $\text{pc}, G_{i-1}, U \vdash c_i: G_i$
| **ST-SetCnd** | $G, U \vdash \text{set(cnd): } G'$
| **ST-If-Isunset** | $G \vdash \text{isunset(cnd): } \text{int}_p$
| **ST-If-Else** | $G', U \vdash c_1: G'$ $G', U \vdash c_2: G''$
| **ST-Sub** | $\text{pc}_1, G_1, U_1 \vdash c: G'_1$ $\text{pc}_2 \leq \text{pc}_1$
| **ST-While** | $G', U \vdash \text{while e do c: } G''$
| **ST-Call** | $G \vdash e: (G^*, U,p,G^*)_q$

**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 \( (c, r, m, K) \) 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.

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

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. Figure 16 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.

**SQ-SEQ**

\[ \forall i \in \{1 \ldots z\}, \mu \vdash (c_i, r_{i-1}, m_{i-1}, K_{i-1}) \Downarrow \Downarrow \text{com} \quad r_i; m_i; K_i \triangleright t_i \]

**SQ-IF-DIV**

\[ \mu \vdash (c, r, m, K) \Downarrow \Downarrow \text{com} \quad (v_0 \mid v_1) \quad c_{\text{leq}} = (v_0 == 1)?c_0 : c_1 \quad c_{\text{right}} = (v_1 == 1)?c_0 : c_1 \\
\mu \vdash (c_{\text{leq}}, [r]_1, [m]_1, [K]_1) \Downarrow r_1'; m_1'; K_1 \triangleright t_1' \quad \mu \vdash (c_{\text{right}}, [r]_2, [m]_2, [K]_2) \Downarrow r_2'; m_2'; K_2 \triangleright t_2' \\
\hat{r} = \text{merge}(r_1', r_2') \quad \hat{m} = \text{merge}(m_1', m_2') \quad \hat{t} = \text{merge}(t_1', t_2') \quad \hat{K} = \text{merge}(K_1, K_2) \]

**SQ-WHILE-DIV**

\[ \mu \vdash (e, r, m, K) \Downarrow \Downarrow \text{com} \quad (v_0 \mid v_1) \quad c_{\text{leq}} = (v_0 == 1)?\text{skip} : c \quad c_{\text{right}} = (v_1 == 1)?c : \text{skip} \\
\mu \vdash (c_{\text{leq}}, [r]_1, [m]_1, [K]_1) \Downarrow r_1'; m_1'; K_1 \triangleright t_1' \quad \mu \vdash (c_{\text{right}}, [r]_2, [m]_2, [K]_2) \Downarrow r_2'; m_2'; K_2 \triangleright t_2' \\
\hat{r} = \text{merge}(r_1', r_2') \quad \hat{m} = \text{merge}(m_1', m_2') \quad \hat{t} = \text{merge}(t_1', t_2') \quad \hat{K} = \text{merge}(K_1, K_2) \]

**SQ-CALL-DIV**

\[ \mu \vdash (\text{call}(e), r, m, K) \Downarrow \Downarrow \text{com} \quad (\lambda^\alpha.c_1 \mid \lambda^\beta.c_2) \\
\mu \vdash (c_1, [r]_1, [m]_1, [K]_1) \Downarrow r_1'; m_1'; K_1 \triangleright t_1' \quad \mu \vdash (c_2, [r]_2, [m]_2, [K]_2) \Downarrow r_2'; m_2'; K_2 \triangleright t_2' \\
\hat{r} = \text{merge}(r_1', r_2') \quad \hat{m} = \text{merge}(m_1', m_2') \quad \hat{t} = \text{merge}(t_1', t_2') \quad \hat{K} = \text{merge}(K_1, K_2) \]

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 \( i^{th} \) projection.

\[ [t]_{i,\text{cmd}} = ([t]_i)_{\text{cmd}} \]
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\(t_1, t_2\) = \[
\begin{cases}
  (\alpha_1 \mid \alpha_2) \cdot \text{merge}(t'_1, t'_2) & \text{if } t_i = \alpha_i \cdot t'_i \land \\
  (\alpha_1 \mid \epsilon) \cdot \text{merge}(t'_1, \epsilon) & \text{if } t_1 = \alpha_1 \cdot t'_1 \land \alpha_2 = \epsilon \land \\
  (\epsilon \mid \alpha_2) \cdot \text{merge}(\epsilon, t'_2) & \text{if } t_2 = \alpha_2 \cdot t'_2 \land \alpha_1 = \epsilon \land \\
  \epsilon & \text{o.w}
\end{cases}
\]
merge\(K_1, K_2\) = \(K_1\mid K_2\)

**Figure 16.** Definition of merge

\[
[r]_i(x) = \begin{cases}
  v & \text{if } r(x) = v \\
  v_i & \text{if } r(x) = (v_1|v_2)
\end{cases}
\]
\[
[m]_i(x) = \begin{cases}
  v & \text{if } m(x) = v \\
  v_i & \text{if } m(x) = (v_1|v_2)
\end{cases}
\]
\[
[t]_i = \begin{cases}
  \text{Mem}([m]_i \cdot [t']_i) & \text{if } t = \text{Mem}(m) \cdot t' \land \\
  \text{Decl}(e, [m]_i \cdot [t']_i) & \text{if } t = \text{Decl}(e, m) \cdot t' \land \\
  \text{Out}(\ell, [v]_i \cdot [t']_i) & \text{if } t = \text{Out}(\ell, v) \cdot t' \land \\
  A(c) \cdot [t']_i & \text{if } t = A(c) \cdot t' \land \\
  A(c_1 \approx c_2) \cdot [t']_i & \text{if } t = A(c_1 \approx c_2) \cdot t' \land \\
  \alpha_i \cdot [t']_i & \text{if } t = (\alpha_1 \mid \alpha_2) \cdot t' \land \\
  \epsilon & \text{o.w}
\end{cases}
\]
\[
[K]_i = K_i \text{ if } K = (K_1\mid K_2)
\]

**Figure 17.** Definition of projections

\[
\text{protected}(p, S) = \begin{cases}
  \text{true} & \text{if } p = H \text{ or } \top \\
  \text{true} & \text{if } p = L \text{ and } \ell_2 \text{ and } \text{cnd} \in S \\
  \text{true} & \text{if } p = \ell_1 \text{ and } \ell_1 \not\leq L \\
  \text{false} & \text{o.w}
\end{cases}
\]
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 $\mu \vdash \langle c, r, m, K \rangle \bullet \downarrow_{com}^2 r^*; m^*; K^* \triangleright t^* \bullet$, 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 $\mu \vdash \langle c, r, m, K \rangle \bullet \downarrow_{com}^2 r^*; m^*; K^* \triangleright t^* \bullet$. \hfill $\Box$

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 $\mu \vdash \langle c, r, m, K \rangle \bullet \downarrow_{com}^2 r^*; m^*; K^* \triangleright t^* \bullet$ and $(\langle r^* \rangle, \langle m^* \rangle, \langle K^* \rangle, \langle t^* \rangle) = \langle r^*_i, m^*_i, K^*_i, t^*_i \rangle$ for $i \in \{1, 2\}$.

Proof Sketch. We use induction on the derivation of $\mu \vdash \delta \langle c, [r]_i, [m]_i, [K]_i \rangle \downarrow r^*_i; m^*_i; K^*_i \triangleright t^*_i$ and prove that we can construct $r^*, m^*, K^*$ and $t^*$ such that $(\langle r^* \rangle, \langle m^* \rangle, \langle K^* \rangle, \langle t^* \rangle) = \langle r^*_i, m^*_i, K^*_i, t^*_i \rangle$ 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 $\mu \vdash \delta \langle e \ if \ then \ c_1 \ else \ c_2, [r]_i, [m]_i, [K]_i \rangle \downarrow r^*_i; m^*_i; K^*_i \triangleright t^*_i$. 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 $\mu \vdash \langle c, r, m, K \rangle \bullet \downarrow_{com}^2 r^*; m^*; K^* \triangleright t^* \bullet$. \hfill $\Box$

E.1.2 IMPE$^2$ Type System
Let $\mathcal{S}$ be the set of conditions setting 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 $\delta, \mathcal{S}, \mathcal{H}$ and $\hat{m}_0$. The typing judgment for commands and expressions is shown below.

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

$$\mu, \Gamma \vdash_{\delta \mathcal{S} \mathcal{H} \hat{m}_0} e : \sigma_p$$

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 $L, N, \Gamma, \emptyset, \emptyset \vdash_{\delta} c : \Gamma', K'$, then $pc, \mu, \Gamma, K, U \vdash_{\delta \mathcal{S} \mathcal{H} \hat{m}_0} c : \Gamma', K'$.

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

Lemma 4 states that for well-typed expressions, evaluation preserves types.

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

Proof. Proof is by straight forward induction on the derivation of the typing judgment $\mu, \Gamma \vdash_{\delta \mathcal{S} \mathcal{H} \hat{m}_0} e : \sigma_p$. \hfill $\Box$
Lemma 5 (IMPE^2 Final Configuration Preservation). Let $\Gamma$ be an environment that is well-typed for $\delta$, $\mathcal{H}$ be the set of escape hatches and $\bar{m}_0$ be the initial IMPE^2 memory such that $l \in \{ \text{locations}(e) \mid e \in \mathcal{H} \}$, $\bar{m}_0(l) \neq (v_1, v_2)$, i.e., not a pair value. If $pc, \mu, \Gamma, U \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle e, r, m, K \rangle : \Gamma', K' \Rightarrow \cdot \Rightarrow \cdot$, then $\Gamma \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle r', m', K' \rangle \Rightarrow \cdot$.

Proof. The proof is by induction on the derivation of the large-step $\mu \vdash \langle e, r, m, K \rangle \cdot \cdot \cdot \Rightarrow \cdot$ for each case. For example, the final configuration preserves the well-typedness of IMPE^2 value configuration.

Case SQ-Skip: Given $pc, \mu, \Gamma, U \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle \text{skip}, r, m, K \rangle : \Gamma', K' \Rightarrow \cdot \Rightarrow \cdot$ and $\mu \vdash \langle \text{skip}, r, m, K \rangle \cdot \cdot \cdot \Rightarrow \cdot \Rightarrow \cdot$. Configuration is not changed.

Case SQ-Assign: Given $pc, \mu, \Gamma, U \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle x := e, r, m, K \rangle : \Gamma', K' \Rightarrow \cdot \Rightarrow \cdot$ and $\mu \vdash \langle x := e, r, m, K \rangle \cdot \cdot \cdot \Rightarrow \cdot \Rightarrow \cdot$ such that $\mu \vdash \langle e, r, m, K \rangle \cdot \cdot \cdot \Rightarrow \cdot \Rightarrow \cdot$. Register files $r$ and $r'$ differ only in variable $x$. Let $v = (v_1, v_2)$. If $\mu \vdash_{\delta, \mathcal{H}, \bar{m}_0} e : \sigma_p$, we have $\text{protected}(p, \sigma_p)$. $\Gamma' = \Gamma[x \rightarrow \sigma_p]$. Hence proved.

Case SQ-Declassify: Given $pc, \mu, \Gamma, U \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle \text{declassify}(x)e, r, m, K \rangle : \Gamma', K' \Rightarrow \cdot \Rightarrow \cdot$ and $\mu \vdash \langle \text{declassify}(x)e, r, m, K \rangle \cdot \cdot \cdot \Rightarrow \cdot \Rightarrow \cdot$. Expressions $e$ has no variables syntactically present (large-step hasNoVars($e$)). We have to prove that $\Gamma' \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle r', m, K \rangle \Rightarrow \cdot$.

Case SQ-Update: Given $pc, \mu, \Gamma, U \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle e_1 \leftarrow e_2, r, m, K \rangle : \Gamma', K' \Rightarrow \cdot \Rightarrow \cdot$ and $\mu \vdash \langle e_1 \leftarrow e_2, r, m, K \rangle \cdot \cdot \cdot \Rightarrow \cdot \Rightarrow \cdot$. Let $v = (v_1, v_2)$ for some $v_1$ and $v_2$. If $\mu \vdash_{\delta, \mathcal{H}, \bar{m}_0} e : \sigma_p$, we have $\text{protected}(p, \sigma_p)$. $\Gamma' = \Gamma[x \rightarrow \sigma_p]$. From the well-typedness, we have allLocImmutable($\ell$). Thus $e \in \mathcal{H}$ and so $v = (v_1, v_2)$ (not a pair value). Hence proved.

Case SQ-SetCND: Given $pc, \mu, \Gamma, U \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle \text{set}(cnd), r, m, K \rangle : \Gamma', K' \Rightarrow \cdot \Rightarrow \cdot$ and $\mu \vdash \langle \text{set}(cnd), r, m, K \rangle \cdot \cdot \cdot \Rightarrow \cdot \Rightarrow \cdot$ from the premise of T-SQ-CONFIG, we have $\Gamma \vdash_{\delta, \mathcal{H}, \bar{m}_0} \langle r, m', K \rangle \Rightarrow \cdot$. Large-step does not modify register file, memory or killset. Hence proved.
of T-Sq-CONFIG, we have $\Gamma \vdash_{SH} \ (q, m, K \cdot ok)$. Since $m$ and $m'$ do not differ (set(cnd) always sets cnd to a non-
Case SQ-CALL-DIV: Given $pc, \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \circ \mu$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \cdot \uparrow^2_{\text{com}} \hat{\tau}; \hat{m}; \hat{K} \triangleright \hat{\mu}$.

We have to prove that $\Gamma \vdash_{\Delta \Theta \land \Theta} \langle \hat{r}, \hat{m}, K \rangle \circ \hat{\mu}$.

From the initial configuration, we have $\Gamma \vdash_{\Delta \Theta \land \Theta} \langle r, m, K \rangle \circ \mu$, $\mu, \Gamma \vdash_{\Delta \Theta \land \Theta} e : (\Gamma', K', U \to \Gamma^+ \circ \mu) \circ \theta$ and so $p, \mu, \Gamma, K, U \vdash_{\Delta \Theta \land \Theta} c : \Gamma', K^+ \circ \theta$. From the premise of SQ-CALL-DIV, we have $\mu \vdash \langle e, r, m, K \rangle \cdot \uparrow^2_{\text{com}} (v_1 | v_2)$. So protected$(q, S)$ and since $q \leq p$, protected$(p, S)$ follows.

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-CONFIG, 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 of $p, \mu, \Gamma, K, U \vdash_{\Delta \Theta \land \Theta} c : \Gamma^+ \circ \mu$, we have protected$(p, S)$ and so protected$(y, S)$ (because an assignment is aleast 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 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. So $[\hat{K}]_1 = [\hat{K}]_2$. Hence proved.

\[
\Box
\]

Lemma 6 (IMPE Type Preservation). Let $\Gamma$ be a well-formed typing context and $pc, \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle c, r, m, K \rangle : \Gamma', K' \circ \mu$. If $\mu' \vdash \langle c', r', m', K' \rangle \cdot \uparrow^2_{\text{com}} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{\mu}$, then $\exists \hat{pc}, \hat{\Gamma}', \hat{U}, \text{such that} \quad pc \leq \hat{pc}$, either $U \leq \hat{U}$ or $U = 0$ and $\hat{pc}, \hat{\Gamma}', \hat{U}, \mu' \vdash_{\Delta \Theta \land \Theta} \langle c', r', m', K' \rangle : \Gamma', K' \circ \mu$.

Proof. The proof is by induction on the derivation of the large step $\mu \vdash \langle c, r, m, K \rangle \cdot \uparrow^2_{\text{com}} \hat{r}; \hat{m}; K' \triangleright \hat{\mu}$. Since rules SQ-ASSIGN, SQ-SKIP, SQ-UPDATE, SQ-KILL, SQ-OUTPUT, SQ-SETCND, SQ-IF-DIV, SQ-WHILE-DIV and SQ-CALL-DIV do not have IMPE command premises, the only relevant cases are SQ-ENCLUDE, SQ-IF, SQ-WHILE, SQ-SEQ, SQ-CALL.

Case SQ-ENCLUDE: Given $pc, \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle \text{enclude}(i, t), r, m, K \rangle : \Gamma', K' \circ \mu$. From the premises of T-Sq-CONFIG, we have $\Gamma \vdash_{\Delta \Theta \land \Theta} \langle r, m, K \rangle \circ \mu$ and $pc, \mu, \Gamma, K, \emptyset \vdash_{\Delta \Theta \land \Theta} e : \Gamma', K' \circ \mu$. From the premises of the IMPE large-step, we have $E_i \vdash \langle c, r, m, K \rangle \cdot \uparrow^2_{\text{com}} \hat{r}; \hat{m}; K' \triangleright \hat{\mu}$. Hence $pc, \emptyset, \Gamma, E_i \vdash_{\Delta \Theta \land \Theta} \langle c, r, m, K \rangle : \Gamma', K' \circ \mu$.

Case SQ-IF: Given $pc, \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle \text{if} e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle : \Gamma', K' \circ \mu$. From the premises of the IMPE large-step, we have $\mu \vdash \langle c_1, r, m, K \rangle \cdot \uparrow^2_{\text{com}} \hat{r}; \hat{m}; K' \triangleright \hat{\mu}$. From the premises of the T-Sq-CONFIG, we have $\Gamma \vdash_{\Delta \Theta \land \Theta} \langle r, m, K \rangle \circ \mu$ and $pc', \mu, \Gamma, K, U \vdash_{\Delta \Theta \land \Theta} c_i : \Gamma', K' \circ \mu$ for $i = \{1, 2\}$, $pc \leq pc'$.

Note that if $e = \text{isnset}(\text{cond})$, then we have $pc', \mu, \Gamma, U \cup \{\text{cond}\} \vdash_{\Delta \Theta \land \Theta} \langle c_i, r, m, K \rangle : \Gamma', K' \circ \mu$ and $pc', \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle c_2, r, m, K \rangle : \Gamma', K' \circ \mu$.

Case SQ-WHILE: Given $pc, \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle \text{while } e \text{ do } c', r, m, K \rangle : \Gamma', K' \circ \mu$. From the premises of the IMPE large-step, we have $\mu \vdash \langle c', r, m, K \rangle \cdot \uparrow^2_{\text{com}} \hat{r}; \hat{m}; K' \triangleright \hat{\mu}$ and $\mu \vdash \langle \text{while } e \text{ do } c', r', m', K' \rangle \cdot \uparrow^2_{\text{com}} \hat{r}; \hat{m}; K'' \triangleright t' \mu$.

From the premises of T-Sq-CONFIG, we have $\Gamma \vdash_{\Delta \Theta \land \Theta} \langle r, m, K \rangle \circ \mu$ and $pc', \mu, \Gamma, K, U \vdash_{\Delta \Theta \land \Theta} c' : \Gamma', K' \circ \mu$ for $pc \leq pc'$. We thus have $K = K' = K''$ and $pc', \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle c', r, m, K \rangle : \Gamma', K' \circ \mu$. Applying Lemma 5 to $pc', \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle c', r, m, K \rangle : \Gamma', K' \circ \mu$.

Case SQ-CALL: Given $pc, \mu, \Gamma, U \vdash_{\Delta \Theta \land \Theta} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \circ \mu$. From the premises of the IMPE large-step, we have $\mu \vdash \langle e, r, m, K \rangle \cdot \uparrow^2_{\text{com}} \hat{\tau}; \hat{m}; K' \triangleright \hat{\mu}$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \cdot \uparrow^2_{\text{com}} \hat{r}; \hat{m}; K' \triangleright t' \mu$.

From the premises of T-Sq-CONFIG, we have $\Gamma \vdash_{\Delta \Theta \land \Theta} \langle r, m, K \rangle \circ \mu$ and $pc, \mu, \Gamma, K, U \vdash_{\Delta \Theta \land \Theta} c : \Gamma', K' \circ \mu$ for $i = \{1, \ldots, n\}$.

We already have $pc, U, \Gamma, 0, \mu \vdash_{\Delta \Theta \land \Theta} \langle c_1, r_0, m_0, K_0 \rangle : \Gamma_1, K_1 \circ \mu$. Applying Lemma 5 we have $\Gamma \vdash_{\Delta \Theta \land \Theta} \langle r_1, m_1, K_1 \rangle \circ \mu$.

Hence $pc, U, \Gamma, 1, \mu \vdash_{\Delta \Theta \land \Theta} \langle c_2, r_1, m_1, K_1 \rangle : \Gamma_2, K_2 \circ \mu$. Repeatedly applying the above argument for $n$ times, we thus have $pc, U, \Gamma, n, \mu \vdash_{\Delta \Theta \land \Theta} \langle c, r_n, m_n, K_n \rangle : \Gamma_n, K_n \circ \mu$.

Hence proved.

\[
\Box
\]

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

Proof. Given $L, \mu, \Gamma, K, \emptyset \vdash c : \Gamma', K'$. Let $m_1$ be some initial memory for which $N \vdash \langle c, r_{\text{init}}, m_1, K \rangle \downarrow r_1; m_1; K' \triangleright t \cdot t_{\text{obs}} \cdot t'$ 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

$k^\Psi_L(c, t_{\text{obs}}) \geq M$
where

\[ M = \left( \bigcap_{m' \in \{ t_{obs} \}_{m \in m}} \text{ind}_t(m_0, \gamma, \{ \text{cnd} \mid m'(\text{cnd}) = 0 \}) \right. \]
\[ \left. \bigcap_{(e', m') \in \{ t_{obs} \}_{m \in m}} \text{Esc}_0^{\text{cond}}(m_0, m', e') \right) \]

Let \( S \) be the set of conditions that are set at the beginning of \( t_{obs} \), i.e., \( S = \{ \text{cnd} \mid m'(\text{cnd}) = 1 \} \). If \( Q \) represents the set of all condition variables, then \( Q \backslash S \) 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. \( H = \{ e \mid (e, m) \in [t \cdot t_{obs}]_{\text{exec}} \} \).

Let \( m_2 \in M \). Also let \( N \models \delta \langle c, r_{\text{inst}}, m_2, K \rangle \Downarrow r_2'; m_2'; K_2' \triangleright t_2 \). To ensure \( k_\text{L}(c, t_{obs}) \supseteq M \), we need to show that \( m_2 \in k_\text{L}(c, t_{obs}) \).

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 \( \Gamma(l) = \sigma_p \Rightarrow \text{protected}(p, S) \). 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 \( L \text{cnd}\neq t_2 \text{ s.t. cnd} \in S \). Then 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

\[ \forall e \in H, \mu \models \delta \langle c, r_{\text{inst}}, m_1, K \rangle \Downarrow v \iff \mu \models \delta \langle c, r, m_2, K \rangle \Downarrow v \]

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 \( m_2 \in k_\text{L}(c, t_{obs}) \).

Let IMPE\(^2\) memory \( m = \text{merge}(m_1, m_2) \). If \( \mu \models \langle c, r_{\text{inst}}, m, K \rangle \models_\text{com} \forall_v r^*: m^*; K \triangleright t^* \bullet \), 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:

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

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 \( L, \mu, \Gamma, K, \emptyset \models_\text{H} c : \Gamma', K' \), we have \( L, \mu, \Gamma, K, \emptyset \models_\text{H} \forall_v \Gamma', K' \). Note that our initial configuration satisfies

\[ L, N, \Gamma, \emptyset \models_\text{H} \langle c, r_{\text{inst}}, m, \emptyset \rangle : \Gamma', K', \bullet_0 \]

**Lemma 7** (Observational Equivalence is Preserved). Let \( S \) be the set of conditions that are set(non-zero) in some observed trace \( t_{obs} \). If \( pc, \mu, \Gamma, U \models_\text{H} \langle c, r, m, K \rangle : \Gamma', K' \bullet_0 \text{ and } \mu \models \langle c, r, m, K \rangle \models_\text{com} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{\bullet} \), then

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

**Proof.** The proof follows by induction on the derivation of \( \mu \models \langle c, r, m, K \rangle \models_\text{com} \hat{r}; \hat{m}; \hat{K} \triangleright \hat{\bullet} \).

**Case Sq-Skip:** Emitted trace is empty.
**Case Sq-Assign:** Emitted trace is empty.
**Case Sq-Declassify:** Emitted trace does not include out event.
**Case Sq-Update:** Emitted trace is empty.
**Case Sq-Kill:** Emitted trace is empty.
**Case Sq-SetCnd:** Emitted trace does not include out event.
**Case Sq-Output:** Given \( pc, \mu, \Gamma, U \models_\text{H} \langle c, r, m, K \rangle : \Gamma', K' \bullet_0 \text{ and } \mu \models \langle c, r, m, K \rangle \models_\text{com} \hat{r}; \hat{m}; \hat{K} \triangleright \text{Mem}(m) \cdot \text{Out}(\ell, v) \bullet_0 \). Let \( \hat{t} = \text{Mem}(m) \cdot \text{Out}(\ell, v) \). From the premise of T-Sq-CONFIG, we have \( pc, \mu, \Gamma, K, U \models_\text{H} \) output \( e \) to \( \ell \), and so \( \mu, \Gamma \models_\text{H} e : \sigma_p \) and \( \text{cur}(p, U) \cup \text{cur}(pc, U) \subseteq \ell \).

**Case v = (v_1 | v_2):** We have \( \text{protected}(p, S) \) 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

\[ \text{Case Sq-If-Else: Given } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (if } e \text{ then } c_1 \text{ else } c_2, r, m, K) : \Gamma', K' \cdot \text{ok} \text{ and } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-IF-ELSE gives us} \]

\[ \text{Case Sq-While: Given } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (while } e \text{ do } c, r', m', K') : \Gamma, K \cdot \text{ok} \text{ and } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-WHILE gives us} \]

\[ \text{Case Sq-Seq: Given } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-SEQ gives us} \]

\[ \text{Case Sq-Call-Div: Given } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (call(e), r, m, K) : } \Gamma, K' \cdot \text{ok} \text{ and } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-CALL gives us} \]

\[ \text{Case Sq-While-Div: Given } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (while } e \text{ do } c, r, m, K) : \Gamma, K \cdot \text{ok} \text{ and } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-WHILE gives us} \]

\[ \text{From Lemma } 6 \text{ we have } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (call(e), r, m, K) : } \Gamma, K \cdot \text{ok}. \text{ Applying induction hypothesis to } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-CALL gives us} \]

\[ \text{Hence} \]

\[ \text{Case Sq-If-Div: Given } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (if } e \text{ then } c_1 \text{ else } c_2, r, m, K) : \Gamma', K' \cdot \text{ok} \text{ and } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-IF-DIV gives us} \]

\[ \text{Case Sq-While-Div: Given } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (while } e \text{ do } c, r, m, K) : \Gamma, K \cdot \text{ok} \text{ and } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-WHILE gives us} \]

\[ \text{Case Sq-Seq: Given } \text{pc, } \mu, \Gamma, U \vdash \text{RUN}_{\text{seq}} \text{ (call(e), r, m, K) : } \Gamma, K' \cdot \text{ok} \text{ and } \mu \vdash \langle e, r, m, K \rangle \Downarrow v \text{ such that } v \text{ is not a pair, applying induction hypothesis to the premises of SQ-SEQ gives us} \]

\[ \text{Applying the inductive hypothesis continuously thus gives,} \]
Case Sq-Enclave: Given $pc, \mu, \Gamma, U \vdash_{\deltaSH_{\text{eni}}} \langle \text{enclave}(i, c), r, m, K \rangle : \Gamma', K' \cdot \text{ok}$ and $N \vdash_{\delta} \langle \text{enclave}(i, c), r, m, K \rangle \Downarrow r'; m'; K' \triangleright t'$. From the premises of T-Sq-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_{\deltaSH_{\text{eni}}} \langle \text{enclave}(i, c), r, m, K \rangle : \Gamma', K'$. From Lemma 6 we have $pc, E_i, \Gamma, \emptyset \vdash_{\deltaSH_{\text{eni}}} \langle c, r, m, K \rangle : \Gamma', K' \cdot \text{ok}$. Applying induction hypothesis to the premise $E_i \vdash_{\delta} \langle c, r, m, K \rangle \Downarrow r'; m'; K' \triangleright t'$

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

Since we have $L, N, \Gamma, \emptyset \vdash_{\deltaSH_{\text{eni}}} \langle c, r, m, \emptyset \rangle : \Gamma', K'$, applying Lemma 7 on $\mu \vdash c, r, m, K \cdot \text{ok}$, we have

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

Hence proved that $m_2 \in k^2_{L}(c, t_{\text{obs}})$. □

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 $L, N, \Gamma, \emptyset, \emptyset \vdash_{\delta} c : \Gamma', K'$, then $pc, \mu, \Gamma, K, U \vdash_{\deltaN_{\text{cha}}} c : \Gamma', K'$.

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$^{2N}$-chaos Adequacy

The language IMPE$^{2N}$-chaos is adequate for reasoning about executions of two IMPE programs. We show that the execution of IMPE$^{2N}$-chaos program using semantics $\Downarrow_{\text{chaos}}^2$ is sound (i.e., large-step taken by an IMPE$^{2N}$-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$^{2N}$-chaos execution).

Lemma 9 (IMPE$^{2N}$-chaos is Sound). If $\mu \vdash c, r, m, K \cdot \Downarrow_{\text{chaos}}^2 r^*; m^*; K^* \triangleright t^*$, then $\mu \vdash_{\delta} \langle c, r, m, K \rangle \Downarrow_{\text{chaos}}^2 [r^*]; [m^*]; [K^*] \triangleright [t^*]$ for $i \in \{1, 2\}$.

Proof Sketch. Proof is by induction on the derivation of $\mu \vdash c, r, m, K \cdot \Downarrow_{\text{chaos}}^2 r^*; m^*; K^* \triangleright t^*$. □

Lemma 10 (IMPE$^{2N}$-chaos is Complete). Let $\mu \vdash_{\delta} \langle c, r, m, K \rangle \Downarrow_{\text{chaos}}^2 [r^*]; [m^*]; [K^*] \triangleright [t^*]$ such that $\lcmd_{\text{chaos}} = [t^*]_{2, \cmd}$ Then $\exists (r^*, m^*, K^*, t^*)$ such that $\mu \vdash \langle c, r, m, K \rangle \cdot \Downarrow_{\text{chaos}}^2 r^*; m^*; K^* \triangleright t^*$ and $\langle [r^*]; [m^*]; [K^*]; [t^*] \rangle = \langle r^*_i; m^*_i; K^*_i; t^*_i \rangle$ for $i \in \{1, 2\}$.

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

E.1.5 IMPE$^{2N}$-chaos N-chaos Type System

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

$$pc, \mu, \Gamma, K, U \vdash_{\deltaSH_{\text{eni}}} c : \Gamma', K'$$

$$\mu, \Gamma \vdash_{\deltaSH_{\text{eni}}} c : \sigma_p$$

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 $\mu \vdash_{\deltaSH_{\text{eni}}} c : \sigma_p$ and $\mu \vdash c, r, m, K \cdot \Downarrow_{\text{chaos}}^2 v$, then $pc, \mu, \Gamma, K, U \vdash_{\deltaSH_{\text{eni}}} c : \Gamma', K'$. □
Proof Sketch. Proof is by straightforward induction on the derivation of the typing judgment \( \mu, \Gamma \vdash_{\delta \text{NS}^{N=\text{chaos}}} e : \sigma_p \).

Lemma 12 (Protected Expression). Let \( \mu, \Gamma \vdash_{\delta \text{NS}^{N=\text{chaos}}} (r, m, K) \cdot \text{ok} \). If \( \mu, \Gamma \vdash_{\delta \text{NS}^{N=\text{chaos}}} e : \sigma_p \) and \( \mu \vdash \langle e, r, m, K \rangle \cdot \downarrow_2 \text{chaos} \) 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 \( \mu, \Gamma \vdash_{\delta \text{NS}^{N=\text{chaos}}} e : \sigma_p \).

Lemma 13 (IMPE\textsuperscript{2N-chaos} N-chaos Final Configuration Preservation). Let \( \Gamma \) be an environment well-typed for \( \delta \), \( \mathcal{H} \) be the set of escape hatches and \( m_0 \) be the initial IMPE\textsuperscript{2N-chaos} memory such that \( l \in \{ \text{locations}(e) \mid e \in \mathcal{H} \} \), \( m_0(l) \neq (v_1 \mid v_2) \), i.e., not a pair value. If \( pc, \mu, \Gamma, U \vdash_{\delta \text{NS}^{N=\text{chaos}}} \langle c, r, m, K \rangle \cdot \text{ok} \) and \( \mu \vdash \langle c, r, m, K \rangle \cdot \downarrow_2 \text{chaos} \) for some values \( r' \) and \( m' \) and \( K' > t' \), then \( \mu, \Gamma \vdash_{\delta \text{NS}^{N=\text{chaos}}} \langle c, r, m, K \rangle \cdot \text{ok} \).

Proof. The proof is by induction on the derivation of the large step \( \mu \vdash \langle c, r, m, K \rangle \cdot \downarrow_2 \text{chaos} \) for some values \( r' \) and \( m' \). For each case, we prove that the final configuration preserves the well-typedness of IMPE\textsuperscript{2N-chaos} value configuration.

Case NSq-Skip: Given \( pc, \mu, \Gamma, U \vdash_{\delta \text{NS}^{N=\text{chaos}}} \langle \text{skip}, r, m, K \rangle : \Gamma' \cdot \text{ok} \) and \( \mu \vdash \langle \text{skip}, r, m, K \rangle \cdot \downarrow_2 \text{chaos} \) for some values \( r, m, K > c \). Configuration is not changed.

Case NSq-Assign: Given \( pc, \mu, \Gamma, U \vdash_{\delta \text{NS}^{N=\text{chaos}}} \langle x := e, r, m, K \rangle : \Gamma' \cdot \text{ok} \) and \( \mu \vdash \langle x := e, r, m, K \rangle \cdot \downarrow_2 \text{chaos} \) for some values \( r' = r \mid x \). We have to prove that \( \mu, \Gamma' \vdash_{\delta \text{NS}^{N=\text{chaos}}} \langle r', m, K \rangle \cdot \text{ok} \). From the initial configuration, we have \( \mu, \Gamma \vdash_{\delta \text{NS}^{N=\text{chaos}}} \langle x := e, r, m, K \rangle \cdot \text{ok} \). Register files \( r \) and \( r' \) differ only in variable \( x \). Let \( v = (v_1 \mid v_2) \). From the well-typedness, we have \( \mu, \Gamma \vdash_{\delta \text{NS}^{N=\text{chaos}}} e : \sigma_p \). 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.
∀ end ∈ U, m(cnd) = 0  
∀ x ∈ Vars, r(x) = (v1,v2) and Γ(x) = σp, r = (σp, rt)  
∀ l ∈ Loc \ Cond, m(l) = (v1,v2) and Γ(l) = (σp,rt)  
∀ e ∈ H, μ ⊢ (e,r, m,K) • 3vN-chaos v  

T-NSQ-CONFIG 

pc,μ,Γ, U ⊢ δSHinN-e (c,r,m,K) : Γ′•ok 
∀ x ∈ Vars, r(x) = (v1,v2) and Γ(x) = σp, r = (σp, rt) 
∀ l ∈ Loc \ Cond, m(l) = (v1,v2) and Γ(l) = (σp,rt)  
∀ e ∈ H, μ ⊢ (e,r, m,K) • 3vN-chaos v  

T-NSQ-VALUE 

μ,Γ ⊢ δSHinN-e (r,m,K) • ok

Figure 20. N-chaos Typing IMPe2N-chaos configurations

Case NSQ-DECLASSIFY: Given pc,μ,Γ, U ⊢ δSHinN-e (declassify(x),e,r,m,K) : Γ′•ok and μ ⊢ (declassify(x),e,r,m,K) • 3vN-chaos r′; m ; K • e such that μ ⊢ (e,r,m,K) • 3vN-chaos v and r′ = r[x → v]. Also expression e has no variables syntactically present (large-step has the premise hasNoVars(e)). We have to prove that μ, Γ′ ⊢ δSHinN-e (e, r, m, K) • ok.

From the initial configuration, we have μ, Γ ⊢ δSHinN-e (e, r, m, K) • ok. Register files r and r′ differ only for variable x. Let v = (v1, v2) for some v1 and v2. We have Γ′ = Γ[x → L]. From the well-typedness, we have allLocImmutable(e). Thus e ∈ H and so v ̸= (v1 | v2) (not a pair value).

Hence proved.

Case NSQ-UPDATE: Given pc,μ,Γ, U ⊢ δSHinN-e (e1 ← e2, r, m, K) : Γ′•ok and μ ⊢ (e1 ← e2, r, m, K) • 3vN-chaos r; m ; K • e such that μ ⊢ (e1,r,m,K) • 3vN-chaos v and m′ = m[l → v]. We have to prove that μ, Γ ⊢ δSHinN-e (e, r, m, K) • ok.

From the premise of T-NSQ-CONFIG, we have μ, Γ ⊢ δSHinN-e (e, r, m, K) • ok, μ, Γ ⊢ δSHinN-e e1 : (σp, refT) and μ, Γ ⊢ δSHinN-e e2 : σp′ such that p′ ⊵ q ∪ p ≤ p.

Case l = (l1 | l2): Applying Lemma 12, we have protected(p′, S) and μ ̸= N. So protected(p, S). Since μ, Γ ⊢ δSHinN-e l : (σp, refT) from the well-typedness of environment, we have δ(l) = μ′ ̸= N. Hence μ, Γ ⊢ δSHinN-e (r,m′,K) • ok.

Case l = (l1 | l2), v = (v1, v2): Same as above.

Case l = (l1 | l2), v ̸= (v1, v2): Applying Lemma 12, we have protected(q, S) and μ ̸= N. So protected(p, S). Since μ, Γ ⊢ δSHinN-e l : (σp, refT) from the well-typedness of environment, we have δ(l) = μ′ ̸= N. Hence μ, Γ ⊢ δSHinN-e (r,m′,K) • ok.

Case l = (l1 | l2), v = (v1, v2): Trivially μ, Γ ⊢ δSHinN-e (r, m′, K) • ok.

Case NSQ-OUTPUT: Given pc,μ,Γ, U ⊢ δSHinN-e (output e to l, r, m, K) : Γ′•ok and μ ⊢ (output e to l, r, m, K) • 3vN-chaos r; m ; K ⊢ Mem(m) • Out(e, v) from the premise of T-NSQ-CONFIG, we have μ, Γ ⊢ δSHinN-e (r, m, K) • ok.

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

Case NSQ-SETCND: Given pc,μ,Γ, U ⊢ δSHinN-e (set(cnd), r, m, K) : Γ′•ok and μ ⊢ (set(cnd), r, m, K) • 3vN-chaos r; m ; K ⊢ Mem(m′) • such that m′ = m[cnd → 1] We have to prove that μ, Γ ⊢ δSHinN-e (r, m′, K) • ok. From the premise of T-NSQ-CONFIG, we have μ, Γ ⊢ δSHinN-e (r, m, K) • ok. Since m and m′ do not differ (set(cnd) always sets cnd to a non-pair value), we have μ, Γ ⊢ δSHinN-e (r, m′, K) • ok.

Case NSQ-KILL: Given pc,μ,Γ, U ⊢ δSHinN-e (kill(i), r, m, K) : Γ′•ok and N ⊢ (kill(i), r, m, K) • 3vN-chaos r; m ; K ⊢ Mem(i) • We have to prove that μ, Γ ⊢ δSHinN-e (r, m, K) • ok. From the premise of T-NSQ-CONFIG, we have μ, Γ ⊢ δSHinN-e (r, m, K) • ok. Since [K]1 = [K]2, we therefore have [K ∪ {E}1]1 = [K ∪ {E}1]2. Hence proved.

Case NSQ-SEQ: Given pc,N,Γ, U ⊢ δSHinN-e (ε1;...;εn,r0,m0,K0) : Γ•ok and N ⊢ (ε1;...;εn,r0,m0,K0) • 3vN-chaos r; m; n ; K ⊢ Mem(i) • We have to prove that N, Γ ⊢ δSHinN-e (r, m, K) • ok. From the premise of T-NSQ-CONFIG, we have μ, Γ ⊢ δSHinN-e (r0,m0,K0) • ok and pc,μ,Γi−1, Ki−1, U ⊢ δSHinN-e (εi;...;εn,r0,m0,K0) • ok. Since the types of locations are fixed throughout the program, we have that if Γ0 is well-typed for δ then Γ1 is also well-typed for δ. Applying induction hypothesis, we thus have μ, Γ1 ⊢ δSHinN-e (r1,m1,K1) • ok. Since the types of locations are fixed throughout the program, we have that if Γ0 is well-typed for δ then Γ1 is also well-typed for δ. Applying induction hypothesis continuously, we thus have N, Γn ⊢ δSHinN-e (rn,mn,Kn) • ok.
Case NSQ-ENCLOSE: Given \( pc, N, \Gamma, U \vdash_{\delta SH_{\|N\|}} \langle \text{enclave}(i, c), r, m, K \rangle : \Gamma \bullet \text{ok} \) and \( N \vdash \langle \text{enclave}(i, c), r, m, K \rangle \). We have to prove that \( \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle r', m', K' \rangle \). From the premise of T-NSQ-CONF, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle r, m, K \rangle \) and \( pc, E, \Gamma, K, \emptyset \vdash_{\delta SH_{\|N\|}} c : \Gamma' \). So, \( pc, E, \Gamma, K, \emptyset \vdash_{\delta SH_{\|N\|}} \langle c, r, m, K \rangle : \Gamma \bullet \text{ok} \). Also, \( E, \Gamma \vdash_{\delta SH_{\|N\|}} \langle r'', m', K'' \rangle \). Applying induction hypothesis, we thus have \( \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle r', m', K' \rangle \). Hence \( \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle r', m', K' \rangle \). ok.

Case NSQ-IF-ELSE: Given \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle e \text{ if then } c_1 \text{ else } c_2, r, m, K \rangle \) and \( \mu \vdash \langle e \text{ if then } c_1 \text{ else } c_2, r, m, K \rangle \). We have to prove that \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{if then } c_1 \text{ else } c_2, r, m, K \rangle \) and \( \mu, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{if then } c_1 \text{ else } c_2, r, m, K \rangle \). From the premise of T-NSQ-CONF, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle c, c_1, c_2, r, m, K \rangle : \Gamma \bullet \text{ok} \). Also, \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle c, c_1, c_2, r, m, K \rangle : \Gamma \bullet \text{ok} \). From the premise of T-NSQ-CONF, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle c, c_1, c_2, r, m, K \rangle : \Gamma \bullet \text{ok} \). Then we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{if then } c_1 \text{ else } c_2, r, m, K \rangle \).

Case NSQ-WHILE: Given \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \) and \( \mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \). We have to prove that \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \) and \( \mu, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \). From the premise of T-NSQ-CONF, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle e, c, r, m, K \rangle \) and \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \). Applying induction hypothesis to the premise \( \mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \), we thus have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \).

Case NSQ-CALL: Given \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{call}(e), r, m, K \rangle \) and \( \mu \vdash \langle \text{call}(e), r, m, K \rangle \). We have to prove that \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{call}(e), r, m, K \rangle \) and \( \mu, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{call}(e), r, m, K \rangle \). From the premise of T-NSQ-CONF, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle e, r, m, K \rangle \) and \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{call}(e), r, m, K \rangle \). Applying induction hypothesis to the premise \( \mu \vdash \langle \text{call}(e), r, m, K \rangle \), we thus have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{call}(e), r, m, K \rangle \).

Case NSQ-IF-DIV: Given \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{if then } c_0 \text{ else } c_1, r, m, K \rangle \) and \( \mu \vdash \langle \text{if then } c_0 \text{ else } c_1, r, m, K \rangle \). We have to prove that \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{if then } c_0 \text{ else } c_1, r, m, K \rangle \) and \( \mu, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{if then } c_0 \text{ else } c_1, r, m, K \rangle \). From the initial configuration, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle c, r, m, K \rangle \) and \( \mu, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle c, r, m, K \rangle \). From the premise of NSQ-IF-DIV, we have \( \mu \vdash \langle c, r, m, K \rangle \). From the premise of T-NSQ-CONF, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle c_0, c_1, r, m, K \rangle \). Applying induction hypothesis to the premise \( \mu \vdash \langle c, r, m, K \rangle \), we thus have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle c, r, m, K \rangle \).

Case NSQ-WHILE-DIV: Given \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \) and \( \mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \). We have to prove that \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \) and \( \mu, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \). From the initial configuration, we have \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle e, r, m, K \rangle \) and \( pc, \mu, \Gamma, \Gamma' \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \). From the premise of NSQ-WHILE-DIV, we have \( \mu \vdash \langle e, r, m, K \rangle \). Let \( z \) be such that \( \Gamma' = \{v_1 \mid v_2\} \). If \( \Gamma(z) = \sigma_\emptyset \), then either \( \Gamma(z) = \sigma_\emptyset \) or there is an assignment to \( z \) in 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 \( pe' \)).

Let \( m(l) = \langle v_1 \mid v_2 \rangle \) and \( \Gamma(l) = \sigma_\emptyset \). Since the type of the 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 \( \mu, \Gamma \vdash_{\delta SH_{\|N\|}} \langle \text{while } e \text{ do } c, r, m, K \rangle \).
of NSQ-CALL-DIV, we have \( \mu \vdash \langle e, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 (v_0 \mid v_1) \). So \( \mu \neq N, \text{protected}(q, S) \) and since \( q \leq p, \text{protected}(p, S) \) follows.

Let \( z \) be such that \( \bar{r}(z) = (v_1 \mid v_2) \). If \( r(z) = (v_1 \mid v_2) \) and \( \Gamma(z) = \sigma_y \), then from the premise of T-NSQ-CONF, we already have \( \text{protected}(y, S) \). If \( r(z) \neq (v_1 \mid v_2) \) i.e., not a pair value, and \( \Gamma(z) = \sigma_y \), then from the well-typedness \( p, \mu, \Gamma, K', U \vdash _{\deltaSHminiNch} \langle c, r, m, K \rangle : \Gamma' \cdot \text{chaos} \cdot \Gamma' \cdot K' \cdot t' \) we have \( \text{protected}(p, S) \) and so \( \text{protected}(y, S) \) (because an assignment is at least as restrictive as \( p \)). Similarly, let \( m(t) = (v_1 \mid v_2) \) 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. So \( |K|_1 = |K|_2 \). Hence \( \mu, \Gamma \vdash _{\deltaSHminiNch} \langle r, m, K \rangle \cdot \text{ok} \).

Hence proved.

\[ \square \]

**Lemma 14 (IMPE\textsuperscript{2N-chaos} N-chaos Type Preservation).** Let \( \Gamma \) be a well-formed typing context and \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle c, r, m, K \rangle : \Gamma' \cdot \text{ok} \). If \( \mu \vdash \langle c', r', m', K' \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; \Gamma' \cdot t' \) is an immediate (command) premise in the evaluation of \( \mu \vdash \langle c, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; \Gamma \cdot t \cdot \text{ok} \), then \( \exists \hat{p} \mu, \Gamma, \Gamma', U, \text{such that } \mu \leq \hat{p} \mu, \text{either } U \subseteq \hat{U} \text{ or } \hat{U} = \emptyset \)

**Proof.** The proof is by induction on the derivation of the large step \( \mu \vdash \langle c, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; K' \cdot t' \). 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\textsuperscript{2N-chaos} command premises, the only relevant cases are NSQ-ENCLAVE, NSQ-ELSE, NSQ-WHILE, NSQ-SEQ, NSQ-CALL.

**Case NSQ-ENCLAVE:** Given \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle \text{enclave}(i, c, r, m, K) : \Gamma' \cdot \text{ok} \rangle \). From the premises of the T-NSQ-CONF, we have \( \mu, \Gamma \vdash _{\deltaSHminiNch} \langle c, r, m, K \rangle : \text{ok} \) and \( \mu, \Gamma \vdash _{\deltaSHminiNch} \langle \text{enclave}(i, c, r, m, K) : \Gamma' \cdot \text{ok} \rangle \). From the premises of the IMPE\textsuperscript{2N-chaos} large-step, we have \( E_i \vdash \langle c, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; K' \cdot t' \cdot \text{ok} \). Hence \( pc, \emptyset, \Gamma, E_i \vdash _{\deltaSHminiNch} \langle c, r, m, K \rangle : \Gamma' \cdot \text{ok} \).

**Case NSQ-IF-ELSE:** Given \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle : \Gamma' \cdot \text{ok} \). From the premises of the IMPE\textsuperscript{2N-chaos} large-step, we have \( \mu \vdash \langle c_1, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; \Gamma' \cdot t' \cdot \text{ok} \). From the premises of the T-NSQ-CONF, we have \( \mu, \Gamma \vdash _{\deltaSHminiNch} \langle c_1, r, m, K \rangle : \text{ok} \) and \( \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle c_1, r, m, K \rangle : \Gamma' \cdot \text{ok} \). From the premises of the IMPE\textsuperscript{2N-chaos} large-step, we have \( \mu \vdash \langle c_2, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; \Gamma' \cdot t' \cdot \text{ok} \). Hence \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle c_2, r, m, K \rangle : \Gamma' \cdot \text{ok} \).

Note that if \( e = \text{isunset}(\text{end}) \), then we have \( pc', \mu, \Gamma, U \cup \{ \text{end} \} \vdash _{\deltaSHminiNch} \langle c_1, r, m, K \rangle : \Gamma' \cdot \text{ok} \) and \( pc', \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle c_2, r, m, K \rangle : \Gamma' \cdot \text{ok} \).

**Case NSQ-WHILE:** Given \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle \text{while } e \text{ do } c', r, m, K \rangle : \Gamma, \text{ok} \). From the premises of the IMPE\textsuperscript{2N-chaos} large-step, we have \( \mu \vdash \langle e, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; K' \cdot t' \cdot \text{ok} \). Hence \( pc, \mu, \Gamma, E_i \vdash _{\deltaSHminiNch} \langle e, r, m, K \rangle : \Gamma, \text{ok} \). Applying Lemma \([13]\) to \( pc', \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle c', r, m, K \rangle : \Gamma, \text{ok} \), we have \( \mu, \Gamma \vdash _{\deltaSHminiNch} \langle c', r, m, K \rangle : \text{ok} \).

**Case NSQ-CALL:** Given \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle \text{call}(e), r, m, K \rangle : \Gamma', \text{ok} \). From the premises of the IMPE\textsuperscript{2N-chaos} large-step, we have \( \mu \vdash \langle c, r, m, K \rangle \cdot \downarrow_{N-\text{chaos}}^2 r'; m'; \Gamma' \cdot t' \cdot \text{ok} \). Hence \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle c, r, m, K \rangle : \Gamma', \text{ok} \).

**Case NSQ-SEQ:** Given \( pc, \mu, \Gamma, U \vdash _{\deltaSHminiNch} \langle c_1, \ldots, c_n, r_0, m_0, K_0 \rangle : \Gamma, \text{ok} \). From the premises of the IMPE\textsuperscript{2N-chaos} large-step, we have \( \mu \vdash \langle c_i, r_{i-1}, m_{i-1}, K_{i-1} \rangle \cdot \downarrow_{N-\text{chaos}}^2 r_i; m_i; K_i \cdot t_i \cdot \text{ok} \). From the premises of the T-NSQ-CONF, we have \( \mu, \Gamma \vdash _{\deltaSHminiNch} \langle r_0, m_0, K_0 \rangle : \text{ok} \). Hence \( pc, \mu, \Gamma, E_i \vdash _{\deltaSHminiNch} \langle c_i, r_i, m_i, K_i \rangle : \text{ok} \). Applying Lemma \([13]\) we have \( \mu, \Gamma \vdash _{\deltaSHminiNch} \langle r_1, m_1, K_1 \rangle : \text{ok} \).

Hence proved.

\[ \square \]

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

Γ

trace

The proof follows by induction on the derivation of Proof.

Let $m_1$ be some initial memory for which $N \vdash (c, r_{\text{init}}, m_1, K) \Downarrow \text{chaos}^N r_1^1; m_1' ; K' \triangleright t \cdot t_{\text{obs}} \cdot t'$ 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

$$k^N \Downarrow \text{chaos}^N(c, t_{\text{obs}}) \supseteq M$$

where

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

Let $S$ be the set of conditions that are set at the beginning of $t_{\text{obs}}$, i.e., $S = \{\text{cnd} | m' \text{(cnd)} = 1\}$. 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. $\mathcal{H} = \{e | (e, m) \in [t \cdot t_{\text{obs}}]_{\text{exec}}\}$.

Let $m_2 \in M$. Also let $N \vdash (c, r_{\text{init}}, m_2, K) \Downarrow \text{chaos}^N r_2^1; m_2'; K' \triangleright t_2$ such that

$$[t_2]_{1, \text{cmd}} = [t_2]_{2, \text{cmd}}$$

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

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 $l \in S$. Why? Suppose for some $l$, $l \in S$. Then for some 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

$$\forall e \in \mathcal{H}, v \sim \delta (e, r_{\text{init}}, m_1, K) \Downarrow v \Leftrightarrow \mu \vdash \delta (e, r, m_2, K) \Downarrow v$$

We will construct an IMP$_{2\text{-chaos}}$ execution that represents the IMPE executions starting from $m_0$ and $m_2$. Type-preservation of IMP$_{2\text{-chaos}}$ (Lemma 13) will ensure that both executions produce the same observable trace, thus showing that $m_2 \in k^N \Downarrow \text{chaos}^N(c, t_{\text{obs}})$.

Let IMP$_{2\text{-chaos}}$ memory $m = \text{merge}(m_1, m_2)$. If $\mu \vdash (c, r_{\text{init}}, m, K) \Downarrow \text{chaos}^N r^*; m^*; K^* \triangleright t^*$ such that the attacker modifies the program in the same way in both the executions. By the adequacy of IMP$_{2\text{-chaos}}$ (Lemma 11), we have that the IMP$_{2\text{-chaos}}$ 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 $[t_{\text{obs}}^*]_1 = t_{\text{obs}}$. Define observation overlapped (same as the function defined in Section E.1.2 but repeated here for the ease of reference) by an IMP$_{2\text{-chaos}}$ trace $t^*$ as:

$$\text{obsOverlap}(t^*, t^*_{\text{pre}}, t^*_{\text{obs}}, t^*_{\text{post}}) = \left\{ \begin{array}{ll}
\epsilon & \text{if } t^*_{\text{pre}} \leq \text{lex } t^*_{\text{pre}} \\
[t^*_{\text{obs}}]_{1} & \text{if } t^*_{\text{pre}} \cdot t_{\text{obs}}^* \leq \text{lex } t^* \\
[t^*_{\text{obs}}]_{2} & \text{if } t^*_{\text{pre}} \cdot t_{\text{obs}}^* \leq \text{lex } t^*_{\text{pre}}\text{ and } t^*_{\text{pre}} \leq \text{lex } t^*_{\text{obs}}
\end{array} \right.$$}

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 $L, \mu, \Gamma, K, \emptyset \vdash \delta \text{SH}_{\text{chaos}} c : \Gamma' \triangleright \text{chaos}$ and so $L, \mu, \Gamma, K, \emptyset \vdash \delta \text{SH}_{\text{chaos}} c : \Gamma' \triangleright \text{chaos}$, from Lemma 15 we have $L, \mu, \Gamma, K, \emptyset \vdash \delta \text{SH}_{\text{chaos}} c : \Gamma' \triangleright \text{chaos}$. Note that our initial configuration satisfies

$$L, N, \Gamma, \emptyset \vdash \delta \text{SH}_{\text{chaos}} c : \Gamma' \triangleright \text{chaos}$$

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 $\mu, \Gamma, U \vdash \delta \text{SH}_{\text{chaos}} c : \Gamma' \triangleright \text{chaos}$ and $\mu \vdash \delta (c, r, m, K) \Downarrow t^* \text{chaos} \triangleright \hat{t} \cdot \hat{m}; K' \triangleright \hat{e}$, then

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

Proof. The proof follows by induction on the derivation of $\mu \vdash \delta (c, r, m, K) \Downarrow t^* \text{chaos} \triangleright \hat{t} \cdot \hat{m}; K' \triangleright \hat{e}$.
Case NSq-Skip: Emitted trace is empty.
Case NSq-Assign: Emitted trace is empty.
Case NSq-Declassify: Emitted trace does not include \textit{out} event.
Case NSq-Update: Emitted trace is empty.
Case NSq-SkipCond: Emitted trace does not include \textit{out} event.

Case NSq-Output: Given $pc, \mu, \Gamma, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} \langle e, r, m, K \rangle : \Gamma', K' \bullet \text{ok} \quad \text{and} \quad \mu \vdash \langle \text{output } e \text{ to } \ell, r, m, K \rangle \bullet \nu_{\text{change}}^2 r; m; K \triangleright \text{Mem}(m) \cdot \text{Out}(\ell, v)$. Let $\ell = \text{Mem}(m) \cdot \text{Out}(\ell, v)$. From the premise of T-NSq-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash \text{output } e \text{ to } \ell, K$ and so $\mu, \Gamma \vdash \delta_{\text{Sh}^0_{\text{NCh}}} e : \sigma_p$ \text{and} 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

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]

Case NSq-If-Else: Given $pc, \mu, \Gamma, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K) : \Gamma', K' \bullet \text{ok} \quad \text{and} \quad \mu \vdash \langle \text{if } e \text{ then } c_1 \text{ else } c_2, r, m, K \rangle \bullet \nu_{\text{change}}^2 r'; m'; K'' \triangleright t'$. Let $\ell = t'$. Since $\mu \vdash (e, r, m, K) \downarrow v$ such that $v$ is not a pair, applying induction hypothesis to the premises of NSQ-IF-ELSE gives us

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]

From Lemma [14], we have $pc, \mu, \Gamma, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{while } e \text{ do } c, r, m, K) : \Gamma, K \bullet \text{ok} \quad \text{and} \quad \mu \vdash \langle \text{while } e \text{ do } c, r, m', K \rangle \bullet \nu_{\text{change}}^2 r''; m''; K'' \triangleright t''$. We have $\mu \vdash (\forall_{\text{change}}^2 r''; m''; K'' \triangleright t'')$, we have

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]

Hence

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]

Case NSq-While: Given $pc, \mu, \Gamma, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{call}(e), r, m, K) : \Gamma', K' \bullet \text{ok} \quad \text{and} \quad \mu \vdash \langle \text{call}(e), r, m, K \rangle \bullet \nu_{\text{change}}^2 r'; m'; K' \triangleright t'$. 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

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]

Case NSq-If-Div: Given $pc, \mu, \Gamma, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{if } e \text{ then } c_0 \text{ else } c_1, r, m, K) : \Gamma', K' \bullet \text{ok} \quad \text{and} \quad \mu \vdash (\text{if } e \text{ then } c_0 \text{ else } c_1, r, m, K) \bullet \nu_{\text{change}}^2 r; m; K \triangleright \text{if }$. From the premises of T-NSQ-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{if } e \text{ then } c_0 \text{ else } c_1) : \Gamma', K'$ Since $\mu \vdash (e, r, m, K) \downarrow v$ such that $v$ is a pair, we have protected$(p, S)$. From the well-typedness, neither $c_1$ nor $c_0$ do emit any out events to $L$ channel. Hence

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]

Case NSq-While-Div: Given $pc, \mu, \Gamma, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{while } e \text{ do } c, r, m, K) : \Gamma, K \bullet \text{ok} \quad \text{and} \quad \mu \vdash (\text{while } e \text{ do } c, r, m, K) \bullet \nu_{\text{change}}^2 r; m; K \triangleright \text{if }$. From the premises of T-NSQ-CONFIG, \text{we have} $pc, \mu, \Gamma, K, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{while } e \text{ do } c, r, m, K) \bullet \nu_{\text{change}}^2 r; m; K \triangleright \text{if }$. Since $\mu \vdash (e, r, m, K) \downarrow v$ such that $v$ is a pair, we have protected$(p, S)$. From the well-typedness, command $c$ does not emit any out events to $L$ channel. Hence

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]

Case NSq-Call-Div: Given $pc, \mu, \Gamma, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{call}(e), r, m, K) : \Gamma', K' \bullet \text{ok} \quad \text{and} \quad \mu \vdash \langle \text{call}(e), r, m, K \rangle \bullet \nu_{\text{change}}^2 r; m; K \triangleright \text{if }$. From the premises of T-NSQ-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash \delta_{\text{Sh}^0_{\text{NCh}}} (\text{call}(e), r, m, K) \bullet \nu_{\text{change}}^2 r; m; K \triangleright \text{if }$. Since $\mu \vdash (e, r, m, K) \downarrow v$ such that $v$ is a pair, we have protected$(p, S)$. From the well-typedness, command $c$ does not emit any out events to $L$ channel. Hence

\[
\text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post}) \equiv_L \text{obsOverlap}(\hat{i}, t^*_\text{pre}, t^*_\text{obs}, t^*_\text{post})
\]
Case NSq-Seq: Given \( pc, \mu, \Gamma_0, U \vdash_{\text{NSq-CONFIG}} \langle c_1; \ldots; c_n, r_0, m_0, K_0 \rangle : \Gamma_n, K_n \cdot \text{ok} \) and \( \mu \vdash \langle c_1; \ldots; c_n \rangle \cdot r_0, m_0, K_0 \). From the premises of T-NSq-CONFIG, we have \( pc, \mu, \Gamma_0, K_0, U \vdash_{\text{NSq-CONFIG}} \langle c_1; \ldots; c_n \rangle : \Gamma_n, K_n \cdot \text{ok} \).

Applying induction hypothesis to the premise, \( \mu \vdash \langle c_1; r_0, m_0, K_0 \rangle \cdot |_{N\text{-chaos}} r_n; m_n; K_n \triangleright t_1; \ldots; t_n \cdot \). From Lemma 14, we have \( pc, \mu, \Gamma_1, U \vdash_{\text{NSq-CONFIG}} \langle c_2, r_1, m_1, K_1 \rangle : \Gamma_2, K_2 \cdot \text{ok} \). Applying inductive hypothesis to the next premise, \( \mu \vdash \langle c_2, r_1, m_1, K_1 \rangle \cdot |_{N\text{-chaos}} r_2; m_2; K_2 \triangleright t_2 \cdot \). From Lemma 14, we have \( pc, E_1, \Gamma_0 \vdash_{\text{NSq-CONFIG}} \langle c, r, m, K \rangle : \Gamma', K' \cdot \text{ok} \). Applying induction hypothesis to the premise \( E_1 \vdash \langle E, \Gamma', \emptyset \rangle \cdot |_{N\text{-chaos}} r'; m'; K' \triangleright t' \cdot \). Since we have \( L, N, \Gamma, \emptyset \vdash_{\text{NSq-CONFIG}} \langle c, r, m, \emptyset \rangle : \Gamma' \cdot \text{ok} \), applying Lemma 15 on \( \mu \vdash \langle E, \Gamma', \emptyset \rangle \cdot |_{N\text{-chaos}} r; m; K \triangleright t \cdot \). Hence proved that \( m_2 \in L|_{N\text{-chaos}} (c, t) \).

E.1.6 Proofs for E1-chaos Security

In this section we use an even more permissive E1-chaos system and show that a IMPE program that is well-typed for the type system in Section 4 is also well-typed for E1-chaos system. Figure 21 presents the E1-chaos type system. It further relaxes the N-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 \( L, N, \Gamma, \emptyset, \emptyset \vdash_{\Gamma'} c : \Gamma', K' \), then \( pc, \mu, \Gamma, K, U \vdash_{\text{NSq-CONFIG}} \langle c, r, m, K \rangle : \Gamma' \cdot \text{ok} \).

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 IMPE2E1-chaos Adequacy

The language IMPE\^2E1-chaos is adequate for reasoning about executions of two IMPE\^2E1-chaos programs. We show that the execution of IMPE\^2E1-chaos program using semantics \( \mu \vdash_{\text{E1-chaos}} \) is sound (i.e., large-step taken by a IMPE\^2E1-chaos program corresponds to a large-step taken by either side of the execution) and complete (given two IMPE\^2E1-chaos executions, there exists an IMPE\^2E1-chaos execution).

Lemma 17 (IMPE\^2E1-chaos is Sound). If \( \mu \vdash \langle c, r, m, K \rangle \cdot |_{E1\text{-chaos}} r; m; K \triangleright t \cdot \), then \( E_{\text{1-chaos}}[c, r, m, K] = \{ c, r, m, K \} \cdot \vdash_{\text{E1-chaos}} [r; m; t] \). for \( i \in \{1, 2\} \).

Proof Sketch. Proof is by induction on the derivation of \( \mu \vdash \langle c, r, m, K \rangle \cdot |_{E1\text{-chaos}} r; m; K \triangleright t \cdot \).

Lemma 18 (IMPE\^2E1-chaos is Complete). If \( \mu \vdash \langle c, r, m, K \rangle \cdot |_{E1\text{-chaos}} r; m; K \triangleright t \cdot \), then \( \mu \vdash \langle c, r, m, K \rangle \cdot |_{E1\text{-chaos}} r; m; K \triangleright t \cdot \) such that \( \mu \vdash \langle c, r, m, K \rangle \cdot |_{E1\text{-chaos}} r; m; K \triangleright t \cdot \) and \( [r; m; t] = \langle c, r, m, K \rangle \cdot \)

Proof Sketch. Follows along the lines of proof of Lemma 2.
The definition differs from ⊤ raised to IMP

\begin{align*}
\text{EI-Skip-N} & \quad pc, N, \Gamma, K, U \vdash_{\text{Ei-N}} \text{skip} : \Gamma, K \\
\text{EI-Assign} & \quad \mu, \Gamma \vdash_{Ei-N} e : \sigma_p \quad \mu \not\in I \\
\text{EI-Output} & \quad \mu, \Gamma, K, U \vdash_{Ei-N} \text{output} e \to \ell : \Gamma, K \\
\text{EI-Seq} & \quad \forall i \in \{1 \ldots n\}, pc, \mu, \Gamma_{i-1}, K_{i-1}, U \vdash_{Ei-N} \text{cnd}_i : \Gamma_i, K_i \\
\text{EI-If-Isunset} & \quad \mu, \Gamma \vdash_{Ei-N} \text{isunset}(\text{cnd}) : \text{int}_\ell \\
\text{EI-If-Else} & \quad \mu, \Gamma \vdash_{Ei-N} \text{int}_p \\
\text{EI-While} & \quad pc, \mu, \Gamma, K, U \vdash_{Ei-N} \text{while} e : \Gamma, K \\
\text{EI-Call} & \quad \mu, \Gamma \vdash_{Ei-N} \text{call}(\text{e}) : \Gamma_{\text{out}}, K^+ \\
\text{EI-Decl} & \quad \mu, \Gamma \vdash_{Ei-N} \text{call}(\text{e}) : \Gamma_{\text{out}}, K^+ \\
\text{EI-Kill} & \quad pc, N, \Gamma, K, U \vdash_{Ei-N} \text{kill}(i) : \Gamma, K \cup \{E_i\} \\
\text{EI-Update} & \quad \mu, \Gamma \vdash_{Ei-N} e_1 : (\sigma_p^{\text{ref}^t})_q \\
\text{EI-SetCnd} & \quad \delta(\text{cnd}) = N \\
\end{align*}

Figure 21. $E_i$-chaos typing rules for IMP

### E.1.8 IMP$^{2E_i}$-chaos $E_i$-chaos Type System

Let $S$ be the set of conditions set during some observed trace $t_{\text{obs}}$, $\mathcal{H}$ be the set of escape hatches till the observed trace and $\hat{n}_0$ be the initial IMP$^{2E_i}$-chaos memory. A policy is now protected if it is either $\top$ or $\ell$ and $\hat{n}_0 \cap \mathcal{H}$ t.s. $m \cap \text{cond} = 1$. We define $\text{protected}_i(p, S)$ as follows:

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

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

The IMP$^{2E_i}$-chaos type system is parametrized by $\delta$, $S$, $\mathcal{H}$ and $\hat{n}_0$. The typing judgment for commands and expressions is shown below.

$$
pc, \mu, \Gamma, K, U \vdash_{\delta S\mathcal{H} n_0 E_i} \text{cnd} : \Gamma', K' \\
\mu, \Gamma \vdash_{\delta S\mathcal{H} n_0 E_i} \text{cnd} : \sigma_p
$$

The typing rules are shown in Figure 21 and ensure that commands running in enclaves that aren’t killed are well-typed according to IMP$^\delta$ type system. Rules for typing configurations are shown in Figure 22 and are similar to T-NSQ-CONFIG and T-NSQ-VALUE.
\[ \forall cn \in U, m(cn) = 0 \quad \text{pc,} \mu, \Gamma, K, U \vdash_{\delta \text{SH}\text{N}+i} e : \Gamma', K' \]

\[ \forall e \in \text{Vars}, r(x) = (v_1 | v_2) \text{ and } \Gamma(x) = \sigma_p \implies \text{protected}_1(p, S) \text{ and } \mu \in I \]

\[ \forall l \in \text{Loc} \setminus \text{Cond}, m(l) = (v_1 | v_2) \text{ and } \Gamma(l) = (\sigma_p, r_l) \implies \text{protected}_1(p, S) \text{ and } \delta(l) \in I \]

\[ \forall e \in \mathcal{H}, \mu \vdash \langle e, r_{\text{init}}, m_0, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \implies \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \quad \forall \Gamma_1 = | K_1 |, \Gamma_2 = | K_2 | \]

**T-ESQ-CONFIG**

\[ \text{pc,} \mu, \Gamma, U \vdash_{\delta \text{SH}\text{N}+i} (c, r, m, K) : \Gamma' \bullet \text{ok} \]

\[ \forall e \in \text{Vars}, r(x) = (v_1 | v_2) \text{ and } \Gamma(x) = \sigma_p \implies \text{protected}_1(p, S) \]

\[ \forall l \in \text{Loc} \setminus \text{Cond}, m(l) = (v_1 | v_2) \text{ and } \Gamma(l) = (\sigma_p, r_l) \implies \text{protected}_1(p, S) \text{ and } \mu \in I \]

\[ \forall e \in \mathcal{H}, \mu \vdash \langle e, r_{\text{init}}, m_0, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \implies \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \text{ and } \delta(l) \in I \]

**T-ESQ-VALUE**

\[ \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r, m, K \rangle \bullet \text{ok} \]

---

**Figure 22.** \( E_{1-\text{chaos}} \) Typing IMPE\(^{2E_{1-\text{chaos}}}_1 \) configurations

**Lemma 19** (\( E_{1-\text{chaos}} \) Value Type Preservation). If \( \mu, \Gamma, U \vdash_{\delta \text{SH}\text{N}+i} e : \sigma_p \) and \( \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \), then \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \).

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

**Lemma 20** (\( E_{1-\text{chaos}} \) Protected Expression). Let \( \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r, m, K \rangle \bullet \text{ok} \). If \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} e : \sigma_p \) and \( \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \) such that \( v = (v_1 | v_2) \) for some values \( v_1 \) and \( v_2 \), then \( \text{protected}_1(p, S) \) and \( \mu \in I \).

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

**Lemma 21** (IMPE\(^{2E_{1-\text{chaos}}}_1 \) \( E_{1-\text{chaos}} \) 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 \( \mathcal{H} \) be the set of escape hatches and \( m_0 \) be the initial IMPE\(^{2E_{1-\text{chaos}}}_1 \) memory such that \( l \in \{ \text{locations}(e) \mid e \in \mathcal{H} \}, m_0(l) \neq (v_1 | v_2) \), i.e., not a pair value. If \( \text{pc,} \mu, \Gamma, U \vdash_{\delta \text{SH}\text{N}+i} \langle c, r, m, K \rangle : \Gamma' \bullet \text{ok} \) and \( \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} r'; m' \); \( \Gamma' \triangleright t' \bullet \), then \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r', m', K \rangle \bullet \text{ok} \).

**Proof.** The proof is by induction on the derivation of the large step \( \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} r'; m' \); \( \Gamma' \triangleright t' \bullet \).

**Case ESQ-SKIP:** Given \( \text{pc,} \mu, \Gamma, U \vdash_{\delta \text{SH}\text{N}+i} \langle \text{skip}, r, m, K \rangle : \Gamma' \bullet \text{ok} \) and \( \mu \vdash \langle \text{skip}, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} r; m; \Gamma \triangleright \bullet \).

Configuration is not changed.

**Case ESQ-ASSIGN:** Given \( \text{pc,} \mu, \Gamma, U \vdash_{\delta \text{SH}\text{N}+i} \langle x := e, r, m, K \rangle : \Gamma' \bullet \text{ok} \) and \( \mu \vdash \langle x := e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} r'; m; K \triangleright e \bullet \) such that \( \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \) and \( r' = r[x \mapsto v] \). We have to prove that \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r', m', K \rangle \bullet \text{ok} \).

From the initial configuration, we have \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r, m, K \rangle \bullet \text{ok} \). Register files \( r \) and \( r' \) differ only in variable \( x \). Let \( v = (v_1 | v_2) \). If \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} e : \sigma_p \), we have \( \text{protected}_1(p, S). \) \( \Gamma' = \Gamma[x \mapsto \sigma_{pc, p}]. \) Applying Lemma 20, we have protected\(_1(p \sqcup q, S) \) and \( \mu \in I. \) Hence proved.

**Case ESQ-DECLASSIFY:** Given \( \text{pc,} \mu, \Gamma, U \vdash_{\delta \text{SH}\text{N}+i} \langle \text{declassify}(x)e, r, m, K \rangle : \Gamma' \bullet \text{ok} \) and \( \mu \vdash \langle \text{declassify}(x)e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} r'; m; K \triangleright e \bullet \) such that \( \mu \vdash \langle e, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \) and \( r' = r[x \mapsto v] \).

Also expression \( e \) has no variables syntactically present (large-step has the premise hasNoVars\(_1(e)\)). We have to prove that \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r', m', K \rangle \bullet \text{ok} \).

From the initial configuration, we have \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r, m, K \rangle \bullet \text{ok} \). Register files \( r \) and \( r' \) differ only for \( x \). Let \( v = (v_1 | v_2) \) for some \( v_1 \) and \( v_2 \). We have \( \Gamma' = \Gamma[x \mapsto L] \). From the well-typedness, we have allLocImmutable\(_1(e)\). Thus \( e \in \mathcal{H} \) and so \( v \neq (v_1 | v_2) \) (not a pair value).

Hence proved.

**Case ESQ-UPDATE:** Given \( \text{pc,} \mu, \Gamma, U \vdash_{\delta \text{SH}\text{N}+i} \langle e_1 \leftarrow e_2, r, m, K \rangle : \Gamma' \bullet \text{ok} \) and \( \mu \vdash \langle e_1 \leftarrow e_2, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} r; m'; K \triangleright \bullet \) such that \( \mu \vdash \langle e_1, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} l, \mu \vdash \langle e_2, r, m, K \rangle \bullet \frac{2}{E_{1-\text{chaos}}} v \) and \( m' = m[l \mapsto v] \).

We have to prove that \( \mu, \Gamma \vdash_{\delta \text{SH}\text{N}+i} \langle r, m', K \rangle \bullet \text{ok} \).
From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m, K \rangle \bullet \text{ok}$, $\mu, \Gamma \vdash_{\text{SHtno,E}} e_1 \cdot \langle \sigma_p^r \text{ ref } \rangle_q$ and $\mu, \Gamma \vdash_{\text{SHtno,E}} i_2 \cdot \sigma_p$ such that $p' \cup q \cup \text{pc} \subseteq p$.

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

Since $\mu, \Gamma \vdash_{\text{SHtno,E}} l \cdot \langle \sigma_p^r \text{ ref } \rangle_L$, from the well-typedness of environment, we have $\delta(l) = \mu' \in I$. Hence $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m', K \rangle \bullet \text{ok}$.

**Case l ≠ (l_1 \mid l_2), v = (v_1 \mid v_2):** Same as above.

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

Since $\mu, \Gamma \vdash_{\text{SHtno,E}} l \cdot \langle \sigma_p^r \text{ ref } \rangle_L$, from the well-typedness of environment, we have $\delta(l) = \mu' \in I$. Hence $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m', K \rangle \bullet \text{ok}$.

**Case l ≠ (l_1 \mid l_2), v ≠ (v_1 \mid v_2):** Trivially $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m', K \rangle \bullet \text{ok}$.

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

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

**Case ESQ-SETCNDB:** Given $pc, \mu, \Gamma, U \vdash_{\text{SHtno,Nosh}} \langle \text{set } \text{cn}d, r, m, K \rangle : \Gamma' \bullet \text{ok}$ and $\mu \vdash \langle \text{set } \text{cn}d, r, m, K \rangle \cdot \|_{E_{chaos}} r; m; K \triangleright \text{Mem}(m) \bullet \text{Q}$. We have to prove that $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m', K \rangle \bullet \text{ok}$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m, K \rangle \bullet \text{ok}$ since $m$ and $m'$ do not differ (set cn) always sets $\text{cn}d$ to a non-pair value, we have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m, K \rangle \bullet \text{ok}$.

**Case ESQ-KILL:** Given $pc, \mu, \Gamma, U \vdash_{\text{SHtno,Nosh}} \langle \text{kill}(i), r, m, K \rangle : \Gamma' \bullet \text{ok}$ and $\mu \vdash \langle \text{kill}(i), r, m, K \rangle \cdot \|_{E_{chaos}} r; m; K \triangleright \text{Mem}(m) \bullet \text{Q}$. We have to prove that $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m', K \rangle \bullet \text{ok}$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m, K \rangle \bullet \text{ok}$.

**Case ESQ-ENCLAVE:** Given $pc, \mu, \Gamma, U \vdash_{\text{SHtno,Nosh}} \langle \text{enclave}(i, c, r, m, K) \rangle : \Gamma' \bullet \text{ok}$ and $\mu \vdash \langle \text{enclave}(i, c, r, m, K) \rangle \cdot \|_{E_{chaos}} r; m; K \triangleright \text{Mem}(m) \bullet \text{Q}$. We have to prove that $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r', m', K' \rangle \bullet \text{ok}$. From the premise of T-ESQ-CONFIG, we have $\mu, \Gamma, U \vdash_{\text{SHtno,E}} \langle \text{enclave}(i, c, r, m, K) \rangle \cdot \|_{E_{chaos}} r; m; K \triangleright \text{Mem}(m) \bullet \text{Q}$. Applying induction hypothesis, we thus have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r', m', K' \rangle \bullet \text{ok}$.

**Case ESQ-IF-ELSE:** Given $pc, \mu, \Gamma, U \vdash_{\text{SHtno,E}} \langle \text{if } \text{then } c \text{ else } c' \text{ r, m, K} \rangle : \Gamma' \bullet \text{ok}$ and $\mu \vdash \langle \text{if } \text{then } c \text{ else } c' \text{ r, m, K} \rangle \cdot \|_{E_{chaos}} r'; m'; K' \triangleright \text{Q}$. We have to prove that $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r', m', K' \rangle \bullet \text{ok}$.

From the premise of T-ESQ-CONF, we have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m, K \rangle \bullet \text{ok}$ and $\mu, \Gamma, U \vdash_{\text{SHtno,E}} \langle \text{if } \text{then } c \text{ else } c' \text{ r, m, K} \rangle \cdot \|_{E_{chaos}} r'; m'; K' \triangleright \text{Q}$. Applying induction hypothesis to each of the premises $\mu \vdash \langle c, r, m, K \rangle \cdot \|_{E_{chaos}} r'; m'; K' \triangleright \text{Q}$, we thus have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r', m', K' \rangle \bullet \text{ok}$.

**Case ESQ-WHILE:** Given $pc, \mu, \Gamma, U \vdash_{\text{SHtno,Nosh}} \langle \text{while } e \text{ do } c, r, m, K \rangle : \Gamma' \bullet \text{ok}$ and $\mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \cdot \|_{E_{chaos}} r''; m''; K'' \triangleright \text{Q}$. We have to prove that $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r'', m'', K'' \rangle \bullet \text{ok}$.

From the premise of T-ESQ-CONF, we have $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r, m, K \rangle \bullet \text{ok}$ and $\mu, \Gamma, U \vdash_{\text{SHtno,E}} \langle \text{while } e \text{ do } c, r, m, K \rangle \cdot \|_{E_{chaos}} r''; m''; K'' \triangleright \text{Q}$. From the well-typedness, we have $K = K''$. Applying induction hypothesis to the premise $\mu \vdash \langle c, r, m, K \rangle \cdot \|_{E_{chaos}} r''; m''; K'' \triangleright \text{Q}$, we thus have $\mu \vdash_{\text{SHtno,E}} \langle r'', m'', K'' \rangle \bullet \text{ok}$. From the well-typedness, we have $K = K''$. Hence $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r'', m'', K'' \rangle \bullet \text{ok}$.

**Case ESQ-CALL:** Given $pc, \mu, \Gamma, U \vdash_{\text{SHtno,Nosh}} \langle \text{call} , e, r, m, K \rangle : \Gamma' \bullet \text{ok}$ and $\mu \vdash \langle \text{call} , e, r, m, K \rangle \cdot \|_{E_{chaos}} r''; m''; K'' \triangleright \text{Q}$. We have to prove that $\mu, \Gamma \vdash_{\text{SHtno,E}} \langle r'', m'', K'' \rangle \bullet \text{ok}$. Also from the premise of ESQ-CALL, we have $\mu \vdash \langle e, r, m, K \rangle \cdot \|_{E_{chaos}} \lambda . c \bullet \mu \vdash \langle c, r, m, K \rangle \cdot \|_{E_{chaos}} r''; m''; K'' \triangleright \text{Q}$.
From the premise of T-ESQ-CONFIG, we have \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle r, m, K \rangle \bullet ok \) and \( pc, \mu, \Gamma, K^* \), \( U \vdash_{\delta SH\tau_0 E} \) call \( e \) such that \( \Gamma^* \subseteq \Gamma \), \( \Gamma^* \vdash \Gamma \) and \( K = K^* = K^* \). From subsumption, \( p, \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle c, r, m, K \rangle : \Gamma^* \bullet ok \). Applying induction hypothesis to \( \mu \vdash \langle c, r, m, K \rangle \bullet \psi_E^{1}\text{-chaos} \ r'; m'; K' \triangleright t' \bullet \), we thus have \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle r', m', K' \rangle \bullet ok \).

**Case ESQ-IF-DIV:** Given \( pc, \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \text{if } e \text{ then } c_0 \text{ else } c_1, r, m, K \rangle : \Gamma' \bullet ok \) and \( \mu \vdash \langle \text{if } e \text{ then } c_0 \text{ else } c_1, r, m, K \rangle \bullet \psi_E^{2}\text{-chaos} \ r'; \hat{m}; K \triangleright \hat{e} \bullet \). We have to prove that \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \hat{r}, \hat{m}, K \rangle \bullet ok \).

From the initial configuration, we have \( pc, \mu, \Gamma, K, U \vdash_{\delta SH\tau_0 E} \psi_E \langle c_0, r, m, K \rangle \). Similarly, let \( \hat{m}(l) = (v_l | v_2) \) and \( \Gamma(l) = \sigma_q \). Since the type of location is invariant throughout the program, from the initial configuration we have \( \hat{e}(q, S) \).

A well-typed escape hatch has immutable locations and thus evaluates to the same value. Since both branches \( c_0 \) and \( c_1 \) have same killsets, we have \( K_1 = K_2 \). So \( \hat{K}_1 = \hat{K}_2 \). Hence \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \hat{r}, \hat{m}, K \rangle \bullet ok \).

**Case ESQ-WHILE-DIV:** Given \( pc, \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \text{while } e \text{ do } c, r, m, K \rangle : \Gamma, K \bullet ok \) and \( \mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \bullet \psi_E^{2}\text{-chaos} \ r'; \hat{m}; K \triangleright \hat{e} \bullet \). We have to prove that \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \hat{r}, \hat{m}, K \rangle \bullet ok \).

From the initial configuration, we have \( pc, \mu, \Gamma, K, U \vdash_{\delta SH\tau_0 E} \psi_E \langle c, r, m, K \rangle \). Similarly, let \( \hat{m}(l) = (v_l | v_2) \). From the premise of T-ESQ-DIV, we have \( \mu \vdash \langle c, r, m, K \rangle \bullet \psi_E^{2}\text{-chaos} \ r' ; \hat{m} ; K \triangleright \hat{e} \bullet \). Since the type of location is invariant throughout the program, from the initial configuration we have \( \hat{e}(q, S) \).

A well-typed escape hatch has immutable locations and thus evaluates to the same value. Killsets are unmodified. So \( \hat{K}_1 = \hat{K}_2 \). Hence \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \hat{r}, \hat{m}, K \rangle \bullet ok \).

**Case ESQ-CALL-DIV:** Given \( pc, \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \bullet ok \) and \( \mu \vdash \langle \text{call}(e), r, m, K \rangle \bullet \psi_E^{2}\text{-chaos} \ r'; \hat{m}; K \triangleright \hat{e} \bullet \). We have to prove that \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle \hat{r}, \hat{m}, K \rangle \bullet ok \).

From the initial configuration, we have \( \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \psi_E \langle c, r, m, K \rangle \bullet ok \). From the premise of ESQ-DIV, we have \( \mu \vdash \langle c, r, m, K \rangle \bullet \psi_E^{2}\text{-chaos} \ r'; \hat{m}; K \triangleright \hat{e} \bullet \). Since the type of location is invariant throughout the program, from the initial configuration we have \( \hat{e}(y, S) \).

Hence proved.

**Lemma 22 (IMPE^{2E_{1\text{-chaos}}}_E\text{-chaos Type 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 IMPE^{2E_{1\text{-chaos}}} \) memory such that \( e \in \text{locations}(e) \) and is well-typed for \( \delta \) such that \( \Gamma \) is not a pair value and \( pc, \mu, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle c, r, m, K \rangle : \Gamma' \bullet ok \). If \( \mu \vdash \langle c', r', m', K' \rangle \bullet \psi_E^{2}\text{-chaos} \ r'; \hat{m}; K \triangleright t \bullet \), then \( \exists pc, \Gamma, U \vdash_{\delta SH\tau_0 E} \langle c', r', m', K' \rangle : \Gamma' \bullet ok \).

**Proof.** The proof is by induction on the derivation of the large step. \( \mu \vdash \langle c, r, m, K \rangle \bullet \psi_E^{2}\text{-chaos} \ r'; m'; K' \triangleright t' \bullet \).

Since rules ESQ-ASSIGN, ESQ-SKIP, ESQ-UPDATE, ESQ-KILL, ESQ-OUTPUT, ESQ-SETCOND, ESQ-IF-DIV, ESQ-WHILE-DIV and
Case **ESQ-ENCLAVE**: Given $pc, \mu, \Gamma, U \vdash_{\triangleleft \SH_{mio}E^p} \langle \text{enclave}(i, c), r, m, K \rangle : \Gamma' \cdot ok$. From the premises of T-SQ-CONFIG, we have $\Gamma \vdash_{\triangleleft \SH_{mio}E^p} \langle r, m, K \rangle \cdot ok$ and $pc, E_i, \Gamma, K, \emptyset \vdash_{\triangleleft \SH_{mio}E^p} \langle c, r, m, K \rangle : \Gamma', K'$. From the premises of the IMPE$_{2E_1-\text{chaos}}$ large-step, we have $E_i \vdash_{\triangleleft \ES} m' \cdot \langle c, r, m, K \rangle : K' \downarrow t'$. Hence, $pc, \emptyset, \Gamma, E_i \vdash_{\triangleleft \SH_{mio}E^p} \langle c, r, m, K \rangle : \Gamma' \cdot ok$.

Case **ESQ-IF-ELSE**: Given $pc, \mu, U, r, m, K \vdash_{\triangleleft \SH_{mio}E^p} \langle e \text{ then } c_2 \text{ else } c_2, r, m, K \rangle : \Gamma \cdot ok$.

Case **ESQ-WHILE**: Given $pc, \mu, \Gamma, U \vdash_{\triangleleft \SH_{mio}E^p} \langle e \text{ while } e \Rightarrow c', r, m, K \rangle : \Gamma \cdot ok$.

Case **ESQ-CALL**: Given $pc, \mu, \Gamma, U \vdash_{\triangleleft \SH_{mio}E^p} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \cdot ok$. From the premises of the IMPE$_{2E_1-\text{chaos}}$ large-step, we have $\mu \vdash_{\triangleleft \ES} c, r, m, K \Rightarrow \langle e, r, m, K \rangle : \mu \vdash_{\triangleleft \ES} c, r, m, K : K' \downarrow t' \cdot ok$.

Case **ESQ-SEQ**: Given $pc, \mu, \Gamma, U \vdash_{\triangleleft \SH_{mio}E^p} (c_1 ; \ldots ; c_n, r_0, m_0, K_0) : \Gamma_n, K_n \cdot ok$. From the premises of the IMPE$_{2E_1-\text{chaos}}$ large-step, we have $\mu \vdash_{\triangleleft \ES} c_1, r_{i-1}, m_{i-1}, K_{i-1} \Rightarrow \langle c_1, r_0, m_0, K_0 \rangle \cdot ok$ and $pc, \mu, \Gamma, U \vdash_{\triangleleft \SH_{mio}E^p} (c_1, r_0, m_0, K_0) : \Gamma_i, K_i$ for $i = 1, \ldots, n$.

Hence proved.

Using Lemma 21 and Lemma 22 we prove the final part of Theorem 1 for semantics $\Downarrow_{E_1-\text{chaos}}$ and specification $\gamma'$.

**Proof.** Given $L, \mu, \Gamma, K, \emptyset \vdash e : \Gamma', K'$. Let $m_1$ be some initial memory for which $N \vdash_{\triangleleft} \langle c, r_{\text{init}}, m_1, K \rangle \Downarrow_{E_1-\text{chaos}} m'_1 \cdot K' \downarrow t \cdot t_{\text{obs}} \cdot t'$. Let $t_{\text{obs}} = m' \cdot t''$ 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

$$k_L^\Downarrow_{E_1-\text{chaos}}(c, t_{\text{obs}}) \geq M$$

where

$$M = \left( \bigcap_{m' \in \{t_{\text{obs}}\}_{m_{\text{mem}}} \vdash \text{ind}(m_0, \gamma'), \{m | m' \cdot t' \leq \text{kind}(m_0, m', \gamma) \}} \right)$$

Let $S$ be the set of conditions that are set at the beginning of $t_{\text{obs}}$, i.e., $S = \{m | m' \cdot t' \leq \text{kind}(m_0, m', \gamma) \}$. If Cond represents the set of all condition variables, then Cond \ $S$ 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. $H = \{e | (e, m) \in t \cdot t_{\text{obs}} \}_{ex}$. Let $m_2 \in M$. Also let $N \vdash_{\triangleleft} \langle c, r_{\text{init}}, m_2, K \rangle \Downarrow_{E_1-\text{chaos}} m'_2 \cdot K'_2 \downarrow t_2$ such that

$$|t_2|_{1, \text{cmd}} = |t_2|_{2, \text{cmd}}$$
To ensure $k_{L}^{\mathcal{E}_{1}^{\text{chaos}}}(c,t_{\text{obs}}) \supseteq M$, we need to show that $m_{2} \in k_{L}^{\mathcal{E}_{1}^{\text{chaos}}}(c,t_{\text{obs}})$

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 $\lnot\text{protected}(p, S)$. So, $p = \ell$ or $\ell_{1}$ and $\ell_{2}$ s.t. $\ell_{1} \cap \ell_{2} \neq S$. Then 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, $\text{protected}(p, S)$ must hold.

Also note that $m_{1}$ and $m_{2}$ satisfy

$$\forall e \in \mathcal{H}, \mu \vdash_{\delta} \langle e, r_{\text{init}}, m_{1}, K \rangle \Downarrow v \iff \mu \vdash_{\delta} \langle e, r, m_{2}, K \rangle \Downarrow v$$

We will construct an $\text{IMPE}^{\mathcal{E}_{1}^{\text{chaos}}}$ execution that represents the IMPE executions starting from $m_{1}$ and $m_{2}$. Type-preservation of $\text{IMPE}^{\mathcal{E}_{1}^{\text{chaos}}}$ (Lemma 21) will ensure that both executions produce the same observable trace, thus showing that $m_{2} \in k_{L}^{\mathcal{E}_{1}^{\text{chaos}}}(c,t_{\text{obs}})$.

Let $\text{IMPE}^{\mathcal{E}_{1}^{\text{chaos}}}$ memory $m = \text{merge}(m_{1}, m_{2})$ and $\mu \vdash \langle c, r_{\text{init}}, m, K \rangle \Downarrow \mathcal{E}_{1}^{\text{chaos}} r^{*}; m^{*}; K \triangleright t^{*}$ such that the attacker modifies the program in the same way in both the executions. By the adequacy of $\text{IMPE}^{\mathcal{E}_{1}^{\text{chaos}}}$ (Lemma 18), we have that the $\text{IMPE}^{\mathcal{E}_{1}^{\text{chaos}}}$ execution represents IMPE executions with $m_{1}$ and $m_{2}$ as initial memories.

Let $t^{*} = t^{*}_{\text{pre}} \cdot t^{*}_{\text{obsp}} \cdot t^{*}_{\text{post}}$ for some $t^{*}_{\text{obsp}}$ such that $[t^{*}_{\text{obsp}}]_{1} = t_{\text{obs}}$. Define observation overlapped (same as the function defined in Section E.1.3 but repeated here for the ease of reference) by an $\text{IMPE}^{\mathcal{E}_{1}^{\text{chaos}}}$ trace $t^{*}$ as:

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

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

Since $L, \mu, \Gamma, K, \emptyset \vdash_{\delta} c : \Gamma', K'$, from Lemma 16 we have $L, \mu, \Gamma, K, \emptyset \vdash_{\delta_{S}^{\mathcal{H}n_{\mu}^{n_{\delta}^{c}}}} \langle e, r_{\text{init}}, m, \emptyset \rangle : \Gamma' \bullet \text{ok}$ and $\mu \vdash \langle c, r, m, K \rangle \Downarrow \mathcal{E}_{1}^{\text{chaos}} \hat{r}; \hat{m} : K \triangleright \hat{t}$. Note that our initial configuration satisfies

$$L, N, \Gamma, \emptyset \vdash_{\delta_{S}^{\mathcal{H}n_{\mu}^{n_{\delta}^{c}}}} \langle c, r_{\text{init}}, m, \emptyset \rangle : \Gamma' \bullet \text{ok}$$

**Lemma 23** (Observational Equivalence is Preserved). Let $S$ be the set of conditions that are set(non-zero) in some observed trace $t_{\text{obs}}$. If $pc, \mu, \Gamma, U \vdash_{\delta_{S}^{\mathcal{H}n_{\mu}^{n_{\delta}^{c}}}} \langle c, r, m, K \rangle : \Gamma', K' \bullet \text{ok}$ and $\mu \vdash \langle c, r, m, K \rangle \Downarrow \mathcal{E}_{1}^{\text{chaos}} \hat{r}; \hat{m} : K \triangleright \hat{t}$, then

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

**Proof.** The proof follows by induction on the derivation of $\mu \vdash \langle c, r, m, K \rangle \Downarrow \mathcal{E}_{1}^{\text{chaos}} \hat{r}; \hat{m} : K \triangleright \hat{t}$.

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

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

**Case ESq-Declassefy**: 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 $pc, \mu, \Gamma, U \vdash_{\delta_{S}^{\mathcal{H}n_{\mu}^{n_{\delta}^{c}}}} \langle c, r, m, K \rangle : \Gamma', K' \bullet \text{ok}$ and $\mu \vdash \langle \text{output } e \mid \ell, r, m, K \rangle \Downarrow \mathcal{E}_{1}^{\text{chaos}} r;m : K \triangleright \text{Mem}(m) \cdot \text{Out}(\ell, v)$. Let $\ell = \text{Mem}(m) \cdot \text{Out}(\ell, v)$. From the premise of T-ESq-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_{\delta_{S}^{\mathcal{H}n_{\mu}^{n_{\delta}^{c}}}} \text{out } e \mid \ell, K$ and so $\mu, \Gamma \vdash_{\delta_{S}^{\mathcal{H}n_{\mu}^{n_{\delta}^{c}}}} e : \sigma_{p}$ 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

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

**Case ESq-If-Else**: Given $pc, \mu, \Gamma, U \vdash_{\delta_{S}^{\mathcal{H}n_{\mu}^{n_{\delta}^{c}}}} \langle \text{if } e \text{ then } c_{1} \text{ else } c_{2}, r, m, K \rangle : \Gamma', K' \bullet \text{ok}$ and $\mu \vdash \langle \text{if } e \text{ then } c_{1} \text{ else } c_{2}, r, m, K \rangle \Downarrow \mathcal{E}_{1}^{\text{chaos}} r'; m' : K' \triangleright t'$. 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 ESq-If-Else gives us

$$\text{obsOverlap}(t^{*}_{\text{pre}}, t^{*}_{\text{obsp}}, t^{*}_{\text{post}})_{1} \approx_{L} \text{obsOverlap}(t^{*}_{\text{pre}}, t^{*}_{\text{obsp}}, t^{*}_{\text{post}})_{2}$$
Case ESq-While: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle \text{while } e \text{ do } c, r, m, K \rangle : \Gamma, K \bullet \text{ok}$ and $\mu \vdash \langle \text{while } e \text{ do } c, r, m, K \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ such that $v$ is 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 $pc, \mu, \Gamma, U \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle \text{while } e \text{ do } c, r, m', K \rangle : \Gamma, K \bullet \text{ok}$. Applying induction hypothesis to $\mu \vdash \langle \text{while } e \text{ do } c, r', m', K \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ where $v$ is a pair, 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

$$[\text{obsOverlap}(t', t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*)]_1 \approx_L [\text{obsOverlap}(t', t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*)]_2$$

Case ESQ-Call: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \bullet \text{ok}$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ such that $v$ is a pair, we have protected$_f(p, S)$. From the well-typedness, command $e$ does not emit any out events to $L$ channel. Hence

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

Case ESq-If-Div: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle \text{if } \text{then } c_1 \text{ else } c_2, r, m, K \rangle : \Gamma', K' \bullet \text{ok}$ and $\mu \vdash \langle \text{if } \text{then } c_1 \text{ else } c_2, r, m, K \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ such that $v$ is a pair, we have protected$_f(p, S)$. From the well-typedness, command $e$ does not emit any out events to $L$ channel. Hence

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

Case ESq-While-Dir: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle \text{while } \text{do } c, r, m, K \rangle : \Gamma, K \bullet \text{ok}$ and $\mu \vdash \langle \text{while } \text{do } c, r, m, K \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ such that $v$ is a pair, we have protected$_f(p, S)$. From the well-typedness, command $e$ does not emit any out events to $L$ channel. Hence

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

Case ESQ-Call-Div: Given $pc, \mu, \Gamma, U \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle \text{call}(e), r, m, K \rangle : \Gamma', K' \bullet \text{ok}$ and $\mu \vdash \langle \text{call}(e), r, m, K \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ such that $v$ is a pair, we have protected$_f(p, S)$. From the well-typedness, command $e$ does not emit any out events to $L$ channel. Hence

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

Case ESQ-Seq: Given $pc, \mu, \Gamma, 0 \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle c_1; \ldots ; c_n, r_0, m_0, K_0 \rangle : \Gamma_n, K_n \bullet \text{ok}$ and $\mu \vdash \langle c_1; \ldots ; c_n, r_0, m_0, K_0 \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ such that $v$ is a pair, we have protected$_f(p, S)$. From the well-typedness, command $e$ does not emit any out events to $L$ channel. Hence

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

From Lemma 22, we have $pc, \mu, \Gamma, 0 \vdash_{\delta \mathcal{S} \mathcal{H} \mu \mathcal{N} \mathcal{C}} \langle c_2, r_1, m_1, K_1 \rangle : \Gamma_2, K_2 \bullet \text{ok}$. Applying induction hypothesis to the next premise, $\mu \vdash \langle c_2, r_1, m_1, K_1 \rangle \cdot \|_{\mathcal{E}_1-\text{chaos}} v$ we have

$$[\text{obsOverlap}(t_2, t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*)]_1 \approx_L [\text{obsOverlap}(t_2, t_{\text{pre}}^*, t_{\text{obs}}^*, t_{\text{post}}^*)]_2$$

Applying the induction 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 $pc, \mu, \Gamma, U \vdash_{\delta_SH\tilde{m}_0,N^\text{ch}} \langle \text{enclave}(i, c), r, m, K \rangle : \Gamma', K' \bullet \text{ok}$ and $N \vdash_{\langle \text{enclave}(i, c), r, m, K \rangle}$.

Proof. From the premises of T-ESQ-CONFIG, we have $pc, \mu, \Gamma, K, U \vdash_{\delta_SH\tilde{m}_0,E_i^\text{ch}} \langle \text{enclave}(i, c), \rangle : \Gamma', K'$. From Lemma 23, we have $pc, E_i, \Gamma, \emptyset \vdash_{\delta_SH\tilde{m}_0,N^\text{ch}} \langle c, r, m, K \rangle : \Gamma', K' \bullet \text{ok}$. Applying induction hypothesis to the premise $E_i \vdash_{\langle c, r, m, K \rangle}$, we have

$$\vdash_{\delta_E^\text{ch} \cdot \text{chaos}} r^*; m^*; K' \triangleright t^*.$$

Hence proved that $m_2 \in p_{\delta_L^E}(c, t_\text{obs})$.

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 $pc, G, \emptyset \vdash \vdash c : G'$ 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 $\exists c_1, c_2, \text{cnd.}$ such that $c'$ is a sub-command of $c$ and $c_{\text{sub}}$ is a sub-command of $c_1$.

Proof. Given $pc, G, \emptyset \vdash \vdash c : G'$. It is easy to see that the only typing judgments that add to the set $U$ for the sub-commands are T-FUNCTION and T-IF-ISUNSET. The remaining judgments T-ASSIGN, T-UPDATE, SEQ, T-IF-ELSE T-WHILE, T-SETND, T-CALL and T-KILL do not change the set $U$ for their sub-commands. Rule T-ENCLOSE nullifies the set $U$ for its sub-commands.

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 $\{ \text{if isunset(\text{cnd}) then } c_1 \text{ else } c_2 \}$.

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

Case TR-INT: Given $G, n, \text{int}_{\Gamma} \Rightarrow \mu, \Gamma, \delta, n, \text{int}_{\Gamma}$. From T-INT, we have $\mu, \Gamma \vdash \delta n : \text{int}_{\Gamma}$.

Case TR-VAR: Given $G, x, \sigma_p \Rightarrow \mu, \Gamma, \delta, x, \sigma_p$. Hence $\Gamma(x) = \sigma_p$. From T-VAR, we thus have $\mu, \Gamma \vdash \delta x : \sigma_p$.

Case TR-LOC: Given $G, l, (\sigma_p, \text{ref}_{\Gamma})_q \Rightarrow \mu, \Gamma, \delta, l, (\sigma_p', \text{ref}_{\Gamma})_q$. From the premises, $\Gamma(l) = \sigma_p$ and $\delta(l) = \sigma_p'$. From T-LOC, we thus have $\mu, \Gamma \vdash \delta l : (\sigma_p', \text{ref}_{\Gamma})_q$.

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

Case TR-DEREF: Given $G, *e, \sigma_{\text{plq}} \Rightarrow \mu, \Gamma, \delta, *e, \sigma_{\text{plq}}$. Applying induction hypothesis to the premise, we have $\mu, \Gamma \vdash *e : (\sigma_p', \text{ref}_{\Gamma})_q$. Also, $\mu' \neq N \Rightarrow \mu = \mu'$. From T-DEREF, we thus have $\mu, \Gamma \vdash \delta *e : \sigma_{\text{plq}}$.

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

Case TR-FUNCTION: Given $G, \lambda c, (G^c, U \Downarrow^c G^c)_q \Rightarrow \mu, \Gamma, \delta, \lambda c, (G^c, K', U \Downarrow^c G^c)_q$. Since $G \vdash \lambda c : G^c, U \Downarrow^c G^c$, we have $q = L$. Applying induction hypothesis to the premise, we have $p, \mu, \Gamma, K', U \Downarrow^c c : \Gamma', K'$. Since, We also have $q = L$. From T-FUNCTION, we thus have $\mu, \Gamma \vdash \delta \lambda c : (G^c, K', U \Downarrow^c G^c)_q$.

Case TR-OP: Given $G, e_1 \oplus e_2, \sigma_{\text{plq}} \Rightarrow \mu, \Gamma, \delta, e_1 \oplus e_2, \sigma_{\text{plq}}$. Applying induction hypothesis to the premises, we have $\mu, \Gamma \vdash e_1 : \text{int}_{\Gamma}$ and $\mu, \Gamma \vdash e_2 : \text{int}_{\Gamma}$. From T-OP, we thus have $\mu, \Gamma \vdash \delta e_1 \oplus e_2 : \text{int}_{\Gamma}$.

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


Case TR-ASSIGN: Given \( pc,G,U,x := e,G[x \mapsto σ_{pc,U}] \rightarrow \mu,Γ,K,δ, x := e' \), \( Γ[x \mapsto σ_{pc,U}] \rightarrow K \). From the well-typedness of IMPS expression \( e \), i.e. \( G \vdash e : σ_q \), we have \( q \neq T \). Applying induction hypothesis to the premise we have \( μ,Γ \vdash_δ e' : σ_q \). From the premises, \( (pc \sqcup q) \not\leq L \implies μ \neq N, μ \not\in K \) and T-ASSIGN, we thus have \( pc,μ,Γ,K,U \vdash x := e' : Γ[x \mapsto σ_{pc,U}],K \).

Case TR-DECLASSIFY: Given \( L,G,U,x := \text{declasify}(e),G[x \mapsto σ_L] \rightarrow μ,Γ,K,δ, x := \text{declasify}(e'),Γ[x \mapsto σ_L],K \). From the well-typedness of IMPS expression \( e \), i.e. \( G \vdash e : σ_q \), we have \( q \neq T \). Applying induction hypothesis to the premise we have \( μ,Γ \vdash_δ e' : σ_q \). From the premises, \( (pc \sqcup q) \not\leq L \implies μ \neq N, μ \not\in K \) and T-DECLASSIFY, we thus have \( pc,μ,Γ,K,U \vdash x := \text{declasify}(e') : Γ[x \mapsto σ_L],K \).

Case TR-OUTPUT: Given \( pc,G,U \), output \( e \) to \( t,G \Rightarrow μ,Γ,K,δ, \) output \( e' \) to \( t,Γ,K \). From the well-typedness of IMPS expression \( e \), i.e. \( G \vdash e : σ_q \), we have \( p \neq T \). Applying induction hypothesis to the premise we have \( μ,Γ \vdash_δ e' : σ_q \). From T-OUTPUT, we thus have \( pc,μ,Γ,K,U \vdash \text{output } e' \) to \( t,Γ,K \).

Case TR-SETCND: Given \( pc,G,U,\text{set(cnd)},G \Rightarrow μ,Γ,K,δ,\text{set(cnd)},Γ,K \). From the well-typedness of IMPS command \( \text{set(cnd)} \), i.e. \( pc,G,U \vdash \text{set(cnd)} : G \), we have \( \text{cnd} \in \text{Cond} \setminus U \). From the premises and T-SETCND, we thus have \( pc,μ,Γ,K,U \vdash \text{set(cnd)} : Γ,K \).

Case TR-UPDATE: Given \( pc,G,U,e_1 \leftarrow e_2,G \Rightarrow μ,Γ,K,δ,e'_1 \leftarrow e'_2,Γ,K \). From the well-typedness of IMPS command \( e_1 \leftarrow e_2 \), i.e. \( G \vdash e_1 : σ_q \), we have \( p,p',q \neq T \). Applying induction hypothesis to the premises, we have \( μ,Γ \vdash_δ e_1 : (σ_{p'} \text{ref} \tau) \) and \( μ,Γ \vdash_δ e_2 : σ_{p'p} \). From the remaining premises and T-UPDATE, we thus have \( pc,μ,Γ,K,U \vdash e_1 \leftarrow e_2,Γ,K \).

Case TR-SEQ: Given \( pc,G_0,U,c_1;…;c_n,G_n \Rightarrow μ_0,Γ_0,K_0,δ,c',Γ_n,K_n+1 \). Applying induction hypothesis to the premises, we have \( \forall i \in \{1,…,n\}, pc,μ_i,Γ_i−1,K_i−1, U \vdash c_i : Γ_i \), \( K_i \).

Consider the case when \( \text{processSeqOutput}(\vec{c}_m;μ_0,\vec{μ}_m;K_0) \text{ matches } \vec{N},(E_j,…,E_j,N,\vec{μ}_m) \). To show that the output \( \text{enclave}(j,c_1;…;c_{m+i}) : \text{processKill}(K_{m+i−1}) \) is well-typed, we first show that \( pc,μ_0,Γ_0,K_0,U \vdash \text{enclave}(j,c_1;…;c_{m+i}) : Γ_{m+i−1},K_{m+i−1} \). If \( U \neq \emptyset \), from Lemma \( 24 \) we have that \( c_1;…;c_{m+i} \) is a sub-command of some if uniset(cnd) then \( s_1 \) else \( s_2 \). However, rule TR-IF-UNSET ensures that \( μ_0 \neq N \) which is a contradiction (since \( μ_0 = N \). Hence \( U = \emptyset \). Premise \( μ_0 \neq N \implies (μ_0 = μ_i \land K''_{m+i} = \emptyset) \) ensures that \( K_1 = K_2 = … = K_{m+i−1} = K''_{m+i−1} \). From T-ENCLAVE, we thus have \( pc,μ_0,Γ_0,K_0,U \vdash \text{enclave}(j,c_1;…;c_{m+i}) : Γ_{m+i−1},K''_{m+i−1} \).

Next we show that \( pc,μ_0,Γ_0, K_{m+i−1}′, U \vdash \text{kill}(j) : Γ_i, K_{m+i}′′ \cup K_{m+i−1}′ \). Consider the case when \( \text{processKill}(K_i) \) matches \( k \cup K' \). From premise \( K''_{m+i} \cap K_i = \emptyset \) we have \( k \notin K''_{m+i−1} \). Also, premise \( μ_0 \neq N \implies (μ_0 = μ_i \land K''_{m+i} = \emptyset) \) ensures that \( μ_0 = N \). From T-KILL, we have \( pc,μ_0,Γ_0, K_{m+i−1}′, U \vdash \text{kill}(j) : Γ_i, K_{m+i−1}′ \cup K''_{m+i−1}′ \). Thus the output \( \text{enclave}(j,c_1;…;c_{m+i}) : \text{processKill}(K_{m+i−1}) \) is well-typed.

For the remaining cases, no enclave or kill statements are inserted. From T-SEQ, we thus have \( pc,μ,Γ_0,K_0,U \vdash \text{c}_1;…;\text{c}_n : Γ_n,K_n \).

Case TR-IF-ELSE: Given \( pc,G,U,if e then c_1 else c_2, G' \Rightarrow μ,Γ,K,δ,if e' then c'_1 else c'_2,Γ',K' \). Applying induction hypothesis to the premises, we have \( μ,Γ \vdash_δ e : \text{int}_p \) and \( pc',μ',Γ,K,U \vdash c_i : Γ_i',K_i' \) for \( i = \{1,2\} \). From the remaining premises and T-IF-ELSE, we thus have \( pc,μ,Γ,K,U \vdash e \) then \( c_1 \) else \( c_2 : Γ',K' \).

Case TR-IF-UNSET: Given \( pc,G,U,if \text{uniset(cnd)} then c_3, G' \Rightarrow μ,Γ,K,δ,if \text{uniset(cnd)} then c'_3 else c'_2,Γ',K' \). Applying induction hypothesis to the premises, we have \( μ,Γ \vdash_δ e : \text{int}_p \) and \( pc',μ',Γ,K,U \vdash c_i : Γ_i',K_i' \) for \( i = \{1,2\} \). From T-IF-UNSET, we thus have \( pc,μ,Γ,K,U \vdash \text{if uniset(cnd)} then c_1 \) else \( c_2 : Γ',K' \).

Case TR-WHILE: Given \( pc,G,U,while e do c,G \Rightarrow μ,Γ,K,δ,while e do c',Γ,K \). Applying induction hypothesis to the premises, we have \( μ,Γ \vdash_δ e : \text{int}_p \) and \( pc',μ',Γ,K,U \vdash c_i : Γ_i',K_i' \). From the remaining premises and T-WHILE, we thus have \( pc,μ,Γ,K,U \vdash \text{while } e \text{ do } c : Γ',K \).

Case TR-CALL: Given \( pc,G,U,call(e),G' \Rightarrow μ,Γ,K,δ,call(e'),G'_OUT,K'_OUT \). Applying induction hypothesis to the premise, we have \( μ,Γ \vdash e : (Γ',K',U \overset{pc}{⇒} Γ',K')_q \). From the remaining premises and T-CALL, we thus have \( pc,μ,Γ,K',U \vdash call(e) : Γ'_OUT,K'_OUT \).

Case TR-SUB: Given \( pc_1,G_2,U,c,G'_2 \Rightarrow μ,Γ_2,K,δ,c',Γ'_2 \). Applying induction hypothesis to the premise, we have \( pc_1,μ,Γ_1,K, U \vdash c_i : Γ_i',K' \). Also from translation of typing environment in Figure 10 we have \( \vdash_δ Γ_i' \text{ ok} \) for \( i = \{1,2\} \). From the remaining premises and T-SUB, we thus have \( pc_2,μ,Γ_2,K, U \vdash c_i : Γ'_2, K'_2 \).

□