

Logical Relations for Noninterference with Cryptography

Sonya Simkin

CMU-CS-25-145

December 2025

Computer Science Department
School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Thesis Committee:

Stephanie Balzer, Chair

Robert Harper

*Submitted in partial fulfillment of the requirements
for the Master's degree in Computer Science.*

Keywords: logical relations, information-flow control, noninterference, possibilistic, cryptography

Abstract

Cryptographic primitives, such as encryption, decryption, and key generation, are vital to the security of many of today's applications, but are difficult to reason about in an information-flow setting. In particular, they conflict with the notion of noninterference, the property that observable outputs are uninfluenced by secret inputs in an information-flow secure program. Not only do ciphertexts often rely on secure data (and thus would be ruled out in a typical information-flow setting), the use of nondeterminism in their generation may serve as a source of information-flow leak (called occlusion). Logical relations are a technique which can be used to prescribe properties of a program based on its computational behavior, rather than relying on static well-formedness. Through this semantic approach, one can not only validate well-typed terms by showing their inhabitation of the logical relation (via the "fundamental theorem"), but also validate ill-typed terms which behave "correctly" with respect to the definition of the logical relation. In this thesis, we extend a version of the simply-typed lambda calculus with cryptographic primitives, and define an information-flow control type system to statically enforce safe usage of said primitives. We then use the technique of logical relations to define a semantic verification method for noninterference. In particular, to combat occlusion, we define a possibilistic logical relation, which considers the set of all possible values an expression could evaluate to.

Acknowledgments

First and foremost, I would like to thank my advisor, Prof. Stephanie Balzer. Thank you for taking a leap of faith with me when I asked to assist with research in any way that I could, for advocating for me, and for helping me become a better researcher. I could not imagine getting to where I am today without your guidance. I would also like to thank Harrison Grodin for encouraging me to reach out to Prof. Balzer in the first place and not letting me rest until I did. Additional thank yous go to Robert Harper, Frank Pfenning, Michael Erdmann, Dilsun Kaynar, my sister, Infra Dance Company, and Angy Malloy.

Contents

- 1 Introduction 1**
 - 1.1 Motivation and Background 1
 - 1.2 Related Work 3
 - 1.3 Outline 4

- 2 Cryptography and Security 5**
 - 2.1 Security Lattice 5
 - 2.2 Cryptographic Schemes 5
 - 2.3 Cryptographic Assumptions 6

- 3 Language 7**
 - 3.1 Grammar 7
 - 3.2 Statics 9
 - 3.3 Dynamics 13

- 4 Logical Relations 17**
 - 4.1 Possibilistic Noninterference 17
 - 4.2 Set-Lifted Dynamics 21
 - 4.3 Leaf-Determinism 21
 - 4.3.1 Sets to Singletons 23
 - 4.4 Binary and Unary Relations 24
 - 4.4.1 Fundamental Theorems 25
 - 4.4.2 Lemmas 29

- 5 Conclusion 31**
 - 5.1 Discussion 31
 - 5.2 Future Work 31

- A Appendix 33**
 - A.1 Proof of Leaf-Determinism FTLR 33
 - A.1.1 Proofs of Lemmas 33
 - A.1.2 FTLR 37
 - A.2 Proof of Binary FTLR 49
 - A.3 Proof of Unary FTLR 70

A.4 Proofs of Remaining Lemmas	81
Bibliography	99

Figures

3.1	Grammar for higher-order language with cryptography	8
3.2	Typing rules for cryptographic expressions	10
3.3	Typing rules for non-cryptographic expressions	11
3.4	Inference rules for the judgment $\ell \triangleleft \tau$	11
3.5	Inference rules for the judgment $\tau \blacktriangleleft \ell$	11
3.6	Subtyping rules	12
3.7	Inference rules for the judgment $e \mathbf{val}_\Sigma$	14
3.8	Evaluation rules for cryptographic expressions	14
3.9	Evaluation rules for non-cryptographic expressions	15
4.1	Set-lifted evaluation rules for cryptographic expressions	19
4.2	Set-lifted evaluation rules for non-cryptographic expressions	20
4.3	Logical relation for leaf-determinism	22
4.4	Binary logical relation	26
4.5	Unary logical relation	27

Chapter 1

Introduction

1.1 Motivation and Background

The security of information is a crucial concern in many modern computing applications. There exist many strategies for ensuring the safety and correctness of security-critical systems, including the employment of information flow control types. Information flow control types (IFC) are types used to enforce the property of *noninterference* [6], which asserts that public outputs that are not influenced by secret inputs. Typically, this is done by assigning security levels to types and defining a type system [16, 18, 22] to statically enforce for a given program that no high-level information is leaked to a low-level observer upon evaluation. While this is an established method for information-flow verification, static typing can be overly conservative in designating what programs can be deemed secure. For example, consider the following code which uses a high-level boolean h :

$$\text{if } h \text{ then } \bar{1} \text{ else } \bar{1}$$

From an information-flow perspective, the above program should be secure, since the resulting value of the expression (the numeral $\bar{1}$) is independent of the exact value of h . However, since typing is a static process, an IFC type system would reject the above program as ill-typed at a low-level, since differing branch results could leak the value of the boolean. Aside from the limitations of static typing, noninterference itself is often considered to be too restrictive of a security requirement, with some applications requiring some amount of data transfer from high to low security to function [17]. Given these drawbacks, we might consider approaches to noninterference that either

1. Safely relax the requirements for full security, or
2. Broaden the scope of acceptable programs.

For Item 1, we consider *cryptography*, which is another widely-used tool in ensuring the security of data within programs. Using encryption schemes, we can safely “hide” some piece of high-level data, making the resultant ciphertext secure to distribute at a lower level. By nature, cryptography conflicts with noninterference, since noninterference requires all expressions (including ciphertexts) to be independent of secret data. However, encryption can also provide a form of *declassification* [17] — for a sufficiently secure key, we can encrypt some high-level data and convert it to a low-level ciphertext without causing a leak. This can help with relaxing the

constraints imposed by noninterference by permitting the passage of high data to low observers in secure circumstances. Facilitating this kind of declassification is not as simple as appending cryptographic primitives to a language, however. As observed by Askarov et al. [2], the presence of cryptography in an IFC system leads to a leak called *occlusion* [17], where a declassification operation (in this case, encryption) produces a leak for high-level data which was not meant to be declassified. For example, consider the following piece of code for a high-level boolean h , encryption key k , and plaintext v :

```
let  $x = \text{encrypt}(k, v)$  in
  if  $h$  then  $\langle x, x \rangle$  else  $\langle x, \text{encrypt}(k, v) \rangle$ 
```

In this example, we encrypt the value v using k and then branch on h , returning either the pair $\langle x, x \rangle$ of the same invocation of the encryption operation or the pair $\langle x, \text{encrypt}(k, v) \rangle$ of distinct invocations. For a perfect, deterministic encryption scheme, this example would not reveal any information about h , since $\text{encrypt}(k, v)$ should return the same result for the same inputs. However, most modern cryptographic schemes utilize a source of nondeterminism to grant probabilistic (rather than exact) guarantees about the indistinguishability of the resultant ciphertexts. As a consequence, different invocations of the same encryption operation may produce different ciphertexts, and if a low-observer is able to compare whether the elements of the pair are always equal or (almost) always distinct, then the value of h could be revealed. To address this, we will need to expand our notion of noninterference to account for *all* possible values a piece of code can evaluate to. This leads to the notion of *possibilistic noninterference* [10], which lifts the definition of noninterference to operate on the sets of possible values returned by different program runs. Under this lifting, we can address the example leak by checking whether the sets of possible values in each branch are the same. In this case, set produced in the `then` branch is only a subset of the possible values in the `else` branch, ruling this code insecure.

For Item 2, we consider the use of *logical relations* [5, 12, 13, 19, 21]. Logical relations are a technique which allow one to prescribe properties of a program based on its computational behavior, rather than any static requirement of well-formedness. Such a semantic approach accommodates the validation of not only well-typed terms (via the “fundamental theorem” of the logical relation), but also of ill-typed terms which are “well-behaved” with respect to the definition of the logical relation. Additionally, logical relations facilitate the *composition* of both well-typed and ill-typed terms — so long as both terms are inhabitants of the logical relation, they can be combined into a compound inhabitant in accordance with the type structure. Using this verification method for noninterference would allow us to expand the amount of programs which can be certified as “secure,” even if they are not accepted by the type system.

Each of the above issues have, in part, been addressed by other works. Askarov et al. [2] defined an IFC type system for safe usage of nondeterministic encryption operators, as well as identified and addressed issues of occlusion through the proof of possibilistic noninterference. Gregersen et al. [7] developed logical relations to prove noninterference for an IFC-typed higher-order language. Sumii and Pierce [20] presented logical relations for an extension of the simply-typed lambda calculus with perfect encryption constructs. In this thesis, we combine each of these three explorations to develop a *semantic* verification method for *possibilistic noninterference* for a higher-order language with *nondeterministic cryptographic primitives* via the technique of *logical relations*.

1.2 Related Work

The results in this thesis are largely inspired by three prior works: Askarov et al. [2], Gregersen et al. [7], and Sumii and Pierce [20]. In this section, we discuss the similarity and differences of these works to the thesis, as well as acknowledge other foundational works.

Askarov et al. [2] presents a proof of noninterference for a simple imperative language with cryptographic primitives. In particular, they introduce an information flow type system that statically ensures security for programs in the language, and they use that type system to prove possibilistic noninterference. Our work follows their model of cryptography, as well as their approach of lifting noninterference to a possibilistic version to account for the nondeterminism of encryption (and to prevent information flows caused by occlusion). However, while the approach is logical relation inspired, the result in *op. cit.* focuses on guaranteeing the security of programs that adhere to the given type system, limiting the scope of the noninterference statement to well-typed code. In this thesis, we develop a semantic approach to proving possibilistic noninterference, granting the ability to show the security of all well-behaved expressions regardless of whether they are statically well-formed. Our work also expands on the base development in *op. cit.*, adding sum and arrow types to the type system and generalizing the information flow labels to a lattice of security levels.

Gregersen et al. [7] provides the definition and mechanization of logical relations for noninterference in the Iris logical framework. In their work, they present an information flow type system for a higher-order language with higher-order store and use this system to derive a semantic verification method via logical relations. Our work adopts a similar approach to *op. cit.* for proving noninterference, particularly by defining both a unary and a binary relation, but with the addition of cryptographic primitives to the language. This leads to a divergence in not only the overall statement of noninterference, but also how the logical relations need to be defined to accommodate said statement. In particular, our work lifts noninterference to possibilistic noninterference, forcing the term interpretations in the logical relations to operate on sets of possible values rather than a single value. Additionally, the type systems that our respective works use for IFC are different — in *op. cit.*, they require that all types have an external security label, whereas in our work that is only required of positive types. This change, which was implemented based on an observation made in Pottier and Simonet [14], leads to differences in the definitions of the logical relations and in the statements and proofs of certain lemmas.

Sumii and Pierce [20] develops a logical relation for an extension of the simply-typed lambda calculus with cryptographic primitives, and they use this relation to prove behavioral equivalence for the language. While our works have similar goals in extending logical relations to account for cryptographic operations, *op. cit.* assumes a perfect model of encryption, meaning it does not take into account the nondeterministic nature of many modern cryptographic schemes. Our work accommodates probabilistic encryption schemes by defining the logical relations over sets of possible values for a given expression. The result in *op. cit.* is also independent of any information flow considerations for security. Since our work is defined using an IFC type system, we are able to accommodate both information flow and cryptographic modes of security, while simultaneously addressing any data flow leaks introduced by encryption (i.e. occlusion). Zhang [24] also provides an approach to defining logical relations for cryptography, but since it is based on Sumii and Pierce [20], it has the same disparities from our work in their assumption perfect

encryption and not having an IFC type system.

The type system defined in this work, as in Gregersen et al. [7], is largely based on the type systems developed in Rajani and Garg [15] and Pottier and Simonet [14]. As mentioned previously, our type system makes a slight departure from the norm in that only positive types (i.e. sum, numeral, and encryption types) have external security labels, whereas negative types (i.e. product and arrow types) do not. This is directly based on the choice in Pottier and Simonet [14] to exclude the label from the product type, and the observation made in their discussion about doing the same for arrows. Additionally, we utilized the $\ell \triangleleft \tau$ and $\tau \blacktriangleleft \ell$ judgments defined in Pottier and Simonet [14] to define our version of the IFC type system, with the latter being used to unify the definition of safe usage for cryptographic operations in Askarov et al. [2] with the methodology of Pottier and Simonet [14].

The logical relations in this work are defined in terms of Kripke-style possible worlds [1, 3, 11] to account for the generation of key names and values. This follows the development in Rajani and Garg [15], which uses a Kripke-style step-indexed logical relation to accommodate higher-order state in their languages (for which they subsequently prove noninterference). Regarding logical relations for IFC and noninterference at large, Zdancewic [23] and Heintze and Riecke [8] both present logical relations arguments for proving noninterference in an IFC-typed language. Each of these works serves as the foundation for the results derived in this thesis, which combined Kripke-style logical relations with those for noninterference and extends them to include cryptographic constructs.

1.3 Outline

The remainder of the thesis document is organized as follows:

- In Chapter 2, we define the model of cryptography that will be used to define the language, along with any cryptographic assumptions we make to ensure the correct statement and proof of noninterference
- In Chapter 3, we give the definition of the higher-order language with cryptographic primitives, which includes the grammar of types and expressions, the IFC type system, and the rules governing the evaluation of expressions
- In Chapter 4, we present the definition of the logical relation for possibilistic noninterference, which consists of a logical relation for a well-formedness property called *leaf-determinism*, unary and binary relations for noninterference, proofs of the “fundamental theorem” for each of these logical relations, and the overall statement and proof for noninterference
- In Chapter 5, we discuss some of the design choices made in this work, explore avenues for future work, and conclude our findings

Chapter 2

Cryptography and Security

In this chapter, we introduce the cryptographic model that will be used in the language, as well as any definitions relevant to defining the security requirements for the language. This includes introducing the notion of a cryptographic scheme and the detailing of any assumptions we hold about said schemes. This chapter also defines any assumptions about IFC security labels that will be carried throughout the rest of the thesis. We adopt the cryptographic model presented in Askarov et al. [2], with some small changes arising from the inclusion of multiple security levels.

2.1 Security Lattice

The IFC type system is defined in terms of a *security lattice* [4], which enumerates all available security levels and the relationships between those levels. The definition of a security lattice is given as follows:

Definition 1 (Secrecy Lattice). *A secrecy lattice \mathcal{L} is a join semilattice $\mathcal{L} = (L, \sqsubseteq, \perp, \top, \sqcup)$, where*

- L is a set of security levels,
- $\ell_1 \sqsubseteq \ell_2$ for $\ell_1, \ell_2 \in \mathcal{L}$ indicates that information flows from level ℓ_1 to level ℓ_2 ,
- $\perp \in L$ is the level such that $\forall \ell \in L, \perp \sqsubseteq \ell$,
- $\top \in L$ is the level such that $\forall \ell \in L, \ell \sqsubseteq \top$,
- $\ell_1 \sqcup \ell_2$ produces the least element $\ell \in L$ such that $\ell_1 \sqsubseteq \ell$ and $\ell_2 \sqsubseteq \ell$ (i.e. join/least upper bound operation)

Given this definition, we have that every lattice must have a least and most security level, and that the join of any two elements in the lattice must exist. We additionally have the operator $\ell_1 \not\sqsubseteq \ell_2$ for $\ell_1, \ell_2 \in L$ to indicate that ℓ_2 is greater than or unrelated to ℓ_1 . For convenience, we write $\ell \in \mathcal{L}$ to represent a security level ℓ associated with a particular lattice \mathcal{L} .

2.2 Cryptographic Schemes

For each lattice \mathcal{L} , and for each $\ell \in \mathcal{L}$, we associate a symmetric key encryption scheme \mathcal{S}_ℓ which guarantees the secure encryption of any data that has level ℓ or lower. The encryption

scheme is defined as follows:

Definition 2 (Encryption Scheme). *An encryption scheme is a triple $\mathcal{S}_\ell = (\mathcal{G}, \mathcal{E}_\ell, \mathcal{D}_\ell)$ with the following properties:*

- $\mathcal{G}(\ell)$ is a key generation algorithm that generates a new key at security level ℓ from a set of keys associated with the scheme
- $\mathcal{E}_\ell(v_k, v)$ is a **nondeterministic** encryption algorithm which takes a key v_k and a value v and returns some bitstring ciphertext u such that $u \in \mathcal{E}_\ell(v_k, v)$ (i.e. it is one of possible many ciphertexts produced by the algorithm)
- $\mathcal{D}_\ell(v_k, u)$ is a **deterministic** decryption algorithm which takes a key v_k and a ciphertext u and either returns the plaintext v if the key v_k matches the one used to encrypt or fails

Note that \mathcal{D}_ℓ is a keyed left inverse for \mathcal{E}_ℓ , meaning that $u \in \mathcal{E}_\ell(v_k, v)$ implies $\mathcal{D}_\ell(v_k, u) = v$ and vice versa [2]. For the quantities v_k and u , we assume that they are elements of a set of key bistrings and ciphertext bitstrings (respectively) associated with the scheme. For the value v , we assume that it is a value from the language, and so we additionally assume that there exists a way to encode and decode that value as a bitstring. This is left implicit in the definition of \mathcal{E}_ℓ and \mathcal{D}_ℓ .

2.3 Cryptographic Assumptions

As in Askarov et al. [2], in order to state and prove possibilistic noninterference, we demand the following properties from a given encryption scheme \mathcal{S}_ℓ :

1. **Confidentiality:** We assume that, for all observer levels ξ such that $\ell \not\geq \xi$, that ciphertexts are *indistinguishable*. That is, for encryption results which are made with and unobservable (i.e. high-level) key, an observer cannot learn anything about the underlying plaintext.
2. **Authenticity:** We assume that decrypting a ciphertext with the wrong key fails, i.e.

$$u \in \mathcal{E}_\ell(v_k, v) \implies \mathcal{D}_\ell(v'_k, u) = \perp$$

(note that \perp here represents the failure for the decryption function to return, rather than the least element in a lattice)

The property described in Item 2 leads to the following lemma about the uniqueness of decryption keys [2]:

Lemma 1 (Uniqueness of Keys). *If $\mathcal{D}_\ell(v_{k1}, u) = v_1$ and $\mathcal{D}_\ell(v_{k2}, u) = v_2$ for values v_1, v_2 , then $v_{k1} = v_{k2}$*

Proof. Note that if $\mathcal{D}_\ell(v_{k1}, u) = v_1$ and $\mathcal{D}_\ell(v_{k2}, u) = v_2$, then neither of them fail. First, observe that $\mathcal{D}_\ell(v_{k1}, u) = v_1 \implies u \in \mathcal{E}_\ell(v_{k1}, v_1)$ by the definition of an encryption scheme. Then, suppose that $v_{k1} \neq v_{k2}$. Given this, by Item 2, we should have that $\mathcal{D}_\ell(v_{k2}, u) = \perp$ for $u \in \mathcal{E}_\ell(v_{k1}, v_1)$. However, this contradicts the fact that $\mathcal{D}_\ell(v_{k2}, u) = v_2$, meaning it must be the case that $v_{k1} = v_{k2}$. \square

In Section 4.1, we will discuss the importance of Item 1 in the realm of noninterference, and how we will need to change the typical approach to noninterference to account for it.

Chapter 3

Language

In this chapter, we present the language upon which the logical relations will be defined. This language is an extension of the simply-typed lambda calculus with cryptographic primitives for encryption, decryption, and key generation. In Section 3.1, we give the grammar for the types and expressions in the language and discuss certain design choices made with respect to security labels. In Section 3.2, we define the information-flow control typing system for the language. In Section 3.3, we show the evaluation rules for the language, which involve a notion of state to handle key name and value generation as well as storage of keys.

3.1 Grammar

The grammar for the language is given in Figure 3.1. The grammar defines the following:

- We have access to labels ℓ and kc from a lattice \mathcal{L} , as specified in Definition 1.
- The types in the grammar are split between so called “basic” types and “primitive” types. Basic types consist of the type of natural numbers, sum types, and two types related to encryption, namely the $\tau \text{ result}$ type and the $\text{enc}_\ell \tau$ type. The $\tau \text{ result}$ type represents the type of decrypted ciphertexts, which can either be a successful decryption of a value of type τ or a failed decryption. The $\text{enc}_\ell \tau$ represents the type of ciphertexts, with ℓ being the security level of the key used to encrypt the ciphertext and τ being the type of the underlying plaintext. Primitive types consist of all of the basic types wrapped with an additional security label, as well as the unit type, product type, arrow type, and the type key_ℓ of keys with security level ℓ .

All expressions in the language are typed at a primitive type. This means that the basic types will have an exterior label (e.g. $(\tau_1 + \tau_2)_\ell$) while product and arrow types will not. We claim there is a correspondence between polarity and the need for a type to have an external label:

- Since positive types are defined by their construction, the choice of constructor we use to create a value may be a source of information flow. As such, we annotate the basic types to indicate the security level of the constructors themselves in addition to the security of any underlying values.

Labels	$\ell, \text{kc} \in \mathcal{L}$		security labels
Key ID	K	$::= \dots$	key identifiers
Basic types	t	nat	natural numbers
		$\tau_1 + \tau_2$	binary sum
		$\tau \text{ result}$	decryption result type
		$\text{enc}_\ell \tau$	encrypted values
Prim. types	τ	t_ℓ	labeled type
		unit	nullary product
		$\tau_1 \times \tau_2$	binary product
		$\tau_1 \xrightarrow{\ell_k} \tau_2$	function
		key_ℓ	key type
Expressions	e	x	variable
		\bar{n}	numeral
		$\langle \rangle$	unit
		$\langle e_1, e_2 \rangle$	pair
		$e \cdot 1$	left projection
		$e \cdot 2$	right projection
		$1 \cdot e$	left injection
		$2 \cdot e$	right injection
		$\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}$	case analysis
		$\lambda(x : \tau_1).e$	lambda abstraction
		$e_1(e_2)$	application
		$\text{encrypt}_\ell(e_1; e_2)$	encryption
		$\text{decrypt}_\ell(e_1; e_2)$	decryption
		Error	failed decryption
		$\text{Ok}(e)$	successful decryption
		$\text{resMatch } e \{ e_0 \mid x.e_1 \}$	result matching
		$\text{gen}\langle \ell \rangle$	key generation
		$\text{key}\langle K \rangle$	reified key

Figure 3.1: Grammar for higher-order language with cryptography

- Since negative types are defined by their destruction, their overall “security” is defined in terms of the information gained upon elimination. This means, converse to positive types, that their construction does not necessarily introduce a source of information flow, so they do not need the outer label.

This design decision is largely based on observations made by Pottier and Simonet [14], and we will continue the discussion of polarity in the language design in the conclusion.

- The arrow type carries an additional label ℓ_k , which is known as the “latent effect label” [7, 14, 15]. This label sets a lower bound on the encapsulated effects. That is, if the function is applied, any keys that are generated are guaranteed to have a level greater than or equal to ℓ_k .
- The expressions in the language are generally the same as the ones in the simply-typed lambda calculus, with some additional constructs for encryption operators:
 - The expression $\text{encrypt}_\ell(e_1; e_2)$ represents the encryption operation for a given encryption scheme. For a security level ℓ , key e_1 , and value e_2 , the operator will obtain a $u \in \mathcal{E}_\ell(v_1, v_2)$, where v_1 is the key value associated with e_1 and v_2 is the value of e_2 .
 - The expression $\text{decrypt}_\ell(e_1; e_2)$ represents the decryption operation for a given encryption scheme. For a security level ℓ , key e_1 , and ciphertext e_2 , the operator will either return an $\text{Ok}(v)$ for $\mathcal{D}_\ell(v_1, v_2) = v$ or Error otherwise, where v_1 is the key value associated with e_1 and v_2 is the value of e_2 .
 - The expressions $\text{Ok}(e)$, Error , and $\text{resMatch } e \{e_0 \mid x_1.e_1\}$ exist for working with the result of a decryption. Since decryption has the possibility to fail, we have the $\text{Ok}(e)$ and Error constructors for either a success or failure (respectively), and resMatch serves as the elimination for the τ result.
 - The expressions $\text{gen}\langle\ell\rangle$ and $\text{key}\langle K\rangle$ relate to the generation of keys for encryption. The construct $\text{gen}\langle\ell\rangle$ generates a new key at security level ℓ and stores it into local memory. When a key needs to be access for encryption or decryption, it is done so through the $\text{key}\langle K\rangle$ construct, which represents a key via its corresponding name in the signature. It is important to note that $\text{key}\langle K\rangle$ is strictly a runtime construct, meaning a user will never directly interact with the signature of key names.

3.2 Statics

Typing rules are of the form

$$\Sigma; \Gamma \vdash_{\text{kc}} e : \tau$$

where Σ is the signature of generated keys, Γ is the variable context, kc is the “key counter,” e is the expression being typed, and τ is the type. The key counter kc is a lower bound on the security labels of all keys generated in e , and it is used to statically prevent any implicit leaks that could occur through the observation of such effects.

The typing rules for cryptographic constructs are given in Figure 3.2, and the typing rules for the remaining expressions are given in Figure 3.3. The rules employ two judgments, original

$$\begin{array}{c}
\text{T-ENC-MOBILE} \\
\frac{\Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau \quad \tau \triangleleft \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{encrypt}_\ell(e_1; e_2) : (\text{enc}_\ell \tau)_\perp} \\
\\
\text{T-ENC-STATIC} \\
\frac{\Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau \quad \tau \triangleleft \ell' \quad \ell' \not\sqsubseteq \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{encrypt}_\ell(e_1; e_2) : (\text{enc}_\ell \tau)_{\ell'}} \\
\\
\text{T-DEC} \\
\frac{\Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : (\text{enc}_\ell \tau)_\epsilon}{\Sigma; \Gamma \vdash_{\text{kc}} \text{decrypt}_\ell(e_1; e_2) : \tau \text{ result}_{\epsilon \sqcup \ell}} \\
\\
\text{T-ERROR} \qquad \qquad \qquad \text{T-SUCCESS} \\
\frac{}{\Sigma; \Gamma \vdash_{\text{kc}} \text{Error} : \tau \text{ result}_\ell} \qquad \frac{\Sigma; \Gamma \vdash_{\text{kc}} e : \tau}{\Sigma; \Gamma \vdash_{\text{kc}} \text{Ok}(e) : \tau \text{ result}_\ell} \\
\\
\text{T-DEC-MATCH} \\
\frac{\Sigma; \Gamma \vdash_{\text{kc}} e : \tau \text{ result}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc} \sqcup \ell} e_0 : \tau' \quad \Sigma; \Gamma, x : \tau \vdash_{\text{kc} \sqcup \ell} e_1 : \tau' \quad \ell \triangleleft \tau'}{\Sigma; \Gamma \vdash_{\text{kc}} \text{resMatch } e \{e_0 \mid x.e_1\} : \tau'} \\
\\
\text{T-KEY-GEN} \qquad \qquad \qquad \text{T-KEY-ACCESS} \\
\frac{\text{kc} \sqsubseteq \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{gen}(\ell) : \text{key}_\ell} \qquad \frac{}{\Sigma, K \sim \ell; \Gamma \vdash_{\text{kc}} \text{key}\langle K \rangle : \text{key}_\ell}
\end{array}$$

Figure 3.2: Typing rules for cryptographic expressions

$$\begin{array}{c}
\text{T-VAR} \\
\hline
\Sigma; \Gamma, x : \tau \vdash_{\text{kc}} x : \tau \\
\\
\text{T-UNIT} \\
\hline
\Sigma; \Gamma \vdash_{\text{kc}} \langle \rangle : \text{unit} \\
\\
\text{T-NAT} \\
\hline
n \in \mathbb{N} \\
\Sigma; \Gamma \vdash_{\text{kc}} \bar{n} : \text{nat}_\ell \\
\\
\text{T-PAIR} \\
\hline
\Sigma; \Gamma \vdash_{\text{kc}} e : \tau_1 \quad \Sigma; \Gamma \vdash_{\text{kc}} e : \tau_2 \\
\Sigma; \Gamma \vdash_{\text{kc}} \langle e_1, e_2 \rangle : \tau_1 \times \tau_2 \\
\\
\text{T-PROJ-I} \\
\hline
\Sigma; \Gamma \vdash_{\text{kc}} e : \tau_1 \times \tau_2 \quad i \in \{1, 2\} \\
\Sigma; \Gamma \vdash_{\text{kc}} e \cdot i : \tau_i \\
\\
\text{T-INJ-I} \\
\hline
\Sigma; \Gamma \vdash_{\text{kc}} e : \tau_i \quad i \in \{1, 2\} \\
\Sigma; \Gamma \vdash_{\text{kc}} i \cdot e : (\tau_1 + \tau_2)_\ell \\
\\
\text{T-CASE} \\
\hline
\Sigma; \Gamma \vdash_{\text{kc}} e : (\tau_1 + \tau_2)_\ell \quad \Sigma; \Gamma, x_1 : \tau_1 \vdash_{\text{kc} \sqcup \ell} e_1 : \tau \quad \Sigma; \Gamma, x_2 : \tau_2 \vdash_{\text{kc} \sqcup \ell} e_2 : \tau \quad \ell \triangleleft \tau \\
\Sigma; \Gamma \vdash_{\text{kc}} \text{case } e \{ x_1.e_1 \mid x_2.e_2 \} : \tau \\
\\
\text{T-FUN} \\
\hline
\Sigma; \Gamma, x : \tau_1 \vdash_{\ell_k} e : \tau_2 \\
\Sigma; \Gamma \vdash_{\text{kc}} \lambda(x : \tau_1).e : \tau_1 \xrightarrow{\ell_k} \tau_2 \\
\\
\text{T-APP} \\
\hline
\Sigma; \Gamma \vdash_{\text{kc}} e_1 : \tau_1 \xrightarrow{\ell_k} \tau_2 \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau_1 \quad \text{kc} \sqsubseteq \ell_k \\
\Sigma; \Gamma \vdash_{\text{kc}} e_1(e_2) : \tau_2 \\
\\
\text{T-SUB} \\
\hline
\Sigma; \Gamma \vdash_{\text{kc}'} e : \tau' \quad \text{kc} \sqsubseteq \text{kc}' \quad \tau' \leq \tau \\
\Sigma; \Gamma \vdash_{\text{kc}} e : \tau
\end{array}$$

Figure 3.3: Typing rules for non-cryptographic expressions

$$\begin{array}{c}
\frac{\ell \sqsubseteq \ell'}{\ell \triangleleft t_{\ell'}} \quad \frac{}{\ell \triangleleft \text{unit}} \quad \frac{\ell \triangleleft \tau_1 \quad \ell \triangleleft \tau_2}{\ell \triangleleft \tau_1 \times \tau_2} \quad \frac{\ell \sqsubseteq \ell_k \quad \ell \triangleleft \tau_2}{\ell \triangleleft \tau_1 \xrightarrow{\ell_k} \tau_2} \quad \frac{\ell \sqsubseteq \ell'}{\ell \triangleleft \text{key}_{\ell'}}
\end{array}$$

Figure 3.4: Inference rules for the judgment $\ell \triangleleft \tau$

$$\begin{array}{c}
\frac{}{\text{unit} \triangleleft \ell} \quad \frac{\ell' \sqsubseteq \ell}{\text{nat}_{\ell'} \triangleleft \ell} \quad \frac{\ell' \sqsubseteq \ell \quad \tau \triangleleft \ell}{\tau \text{ result}_{\ell'} \triangleleft \ell} \quad \frac{\epsilon \sqsubseteq \ell}{(\text{enc}_{\ell'} \tau)_\epsilon \triangleleft \ell} \\
\\
\frac{\ell' \sqsubseteq \ell \quad \tau_1 \triangleleft \ell \quad \tau_2 \triangleleft \ell}{(\tau_1 + \tau_2)_{\ell'} \triangleleft \ell} \quad \frac{\tau_1 \triangleleft \ell \quad \tau_2 \triangleleft \ell}{\tau_1 \times \tau_2 \triangleleft \ell} \quad \frac{\tau_2 \triangleleft \ell \quad \ell_k \sqsubseteq \ell}{\tau_1 \xrightarrow{\ell_k} \tau_2 \triangleleft \ell}
\end{array}$$

Figure 3.5: Inference rules for the judgment $\tau \triangleleft \ell$

$$\begin{array}{c}
\frac{\ell_1 \sqsubseteq \ell_2}{\text{unit}_{\ell_1} \leq \text{unit}_{\ell_2}} \quad \frac{\ell_1 \sqsubseteq \ell_2}{\text{nat}_{\ell_1} \leq \text{nat}_{\ell_2}} \quad \frac{\tau_1 \leq \tau'_1 \quad \tau_2 \leq \tau'_2 \quad \ell_1 \sqsubseteq \ell_2}{(\tau_1 + \tau_2)_{\ell_1} \leq (\tau'_1 + \tau'_2)_{\ell_2}} \\
\frac{\tau_1 \leq \tau'_1 \quad \tau_2 \leq \tau'_2}{\tau_1 \times \tau_2 \leq \tau'_1 \times \tau'_2} \quad \frac{\tau'_1 \leq \tau_1 \quad \tau_2 \leq \tau'_2 \quad \ell'_k \sqsubseteq \ell_k}{\tau_1 \xrightarrow{\ell_k} \tau_2 \leq \tau'_1 \xrightarrow{\ell'_k} \tau'_2} \quad \frac{\tau_1 \leq \tau_2 \quad \epsilon_1 \sqsubseteq \epsilon_2}{(\text{enc}_\ell \tau_1)_{\epsilon_1} \leq (\text{enc}_\ell \tau_2)_{\epsilon_2}} \\
\hline
\text{key}_\ell \leq \text{key}_\ell
\end{array}$$

Figure 3.6: Subtyping rules

defined by [14], to ensure the information-flow safety of the expressions: $\ell \triangleleft \tau$ and $\tau \blacktriangleleft \ell$.

The judgment $\ell \triangleleft \tau$ (read as “type τ is protected at level ℓ ”) is defined inductively with the inference rules in Figure 3.4. Intuitively, this judgment describes when the security level of an expression of type τ is at least the level ℓ , and it is used to ensure that an expression does not release high-level information to a low-level type. For example, consider the rule T-CASE. In this rule, we have an expression e of type $(\tau_1 + \tau_2)_\ell$ that we case on, and then we use the “protected at” judgment to ensure that the result type τ is at a security level no less than ℓ . This is done to ensure that after learning some information at level ℓ (i.e. the constructor used to create the expression e), we do not disseminate that information to a lower security level. This typing rule also shows how the kc is used to prevent implicit leaks. In the premises for the branches, the lower bound on all effects must be $\text{kc} \sqcup \ell$, meaning there cannot be any keys produced of level lower than ℓ . This prevents an attacker from learning the information of level ℓ by observing the keys produced during different runs of the program.

The judgment $\tau \blacktriangleleft \ell$ (read as “type τ is upper bounded by level ℓ ”) is defined inductively via inference rules in Figure 3.5. In Pottier and Simonet [14], this judgment was used to define the typing of “black box” generic operators. Since the implementation of such operators is unknown, the amount of information they take advantage of is also unknown, so we impose a constraint on *all*¹ of the security labels within a type, including all subcomponent types. In the context of this work, we treat encryption as such a “black box” operation, and so we take advantage of the $\tau \blacktriangleleft \ell$ judgment to define both secure and insecure uses of encryption. With this, we can examine the two typing rules and observe how they are defined to ensure safe usage (and thus safe declassification) of encryption:

- In the rule T-ENC-MOBILE, for a key with level ℓ , we require that the plaintext type τ be upper bounded by ℓ , i.e. that $\tau \blacktriangleleft \ell$. This ensures that the key used to encrypt is sufficiently strong to hide *all* of the information in the plaintext. Given that, the result type of the expression is $(\text{enc}_\ell \tau)_\perp$, meaning the result of the encryption has been downgraded all the way to the lowest level in the lattice. This typing rule demonstrates how declassification

¹This is true for all types except for the $(\text{enc}_\ell \tau)_\epsilon$ type, which only examines the outer label ϵ . This is in agreement with Askarov et al. [2], which also only examines the top label to determine whether a ciphertext is safe to encrypt and downgrade.

can be safely supported in the IFC type system.

- In the rule T-ENC-STATIC, we have the case where a key is not sufficiently strong to declassify the plaintext data. In particular, we have that $\tau \blacktriangleleft \ell'$ for some level ℓ' which is greater than or unrelated to ℓ . As such, after encrypting the plaintext, we can at most type the ciphertext at the security level ℓ' , meaning there is no downgrading that can occur.

We also have rules for subtyping, as given in Figure 3.6. These rules are standard with the exception of the key_ℓ , which has a “permanent” label that is assigned when the key is created and cannot be “weakened” or otherwise changed through subtyping.

3.3 Dynamics

The dynamics are defined in terms of a state $\nu\Sigma\{e \parallel \mu\}$, where Σ is the signature of keys, e is the expression being evaluated, and μ is the memory containing the values of generated keys. We define the dynamics judgment

$$\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{v \parallel \mu'\}$$

to represent big-step evaluation, and additionally the judgment $v \text{val}_\Sigma$ to describe when an expression v is a value.

The full evaluation state also contains a stream of key values \mathcal{G} and a stream of key names \mathcal{K} . The stream \mathcal{G} is a map from security levels ℓ in the security lattice to streams of key bitstrings v_k generated by repeated calls to the function $\mathcal{G}(\ell)$ from the corresponding encryption scheme. Similarly, \mathcal{K} is a map from security levels to finite streams of symbols. We assume that the symbols within and between streams are unique. When a key of level ℓ is generated in the program, we will access the streams $\mathcal{G}[\ell]$ and $\mathcal{K}[\ell]$, pop the top element off each stream, store the popped name and value in the signature and memory (respectively), and update streams at ℓ in both mappings.

For the most part, the \mathcal{G} and \mathcal{K} maps are passed forward through the dynamics rules without being directly interacted with, e.g.

$$\begin{array}{c} \text{PAIR-EVAL} \\ \frac{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{e_1 \parallel \mu\}) \Downarrow (\mathcal{G}_1, \mathcal{K}_1, \nu\Sigma_1\{e_1 \parallel \mu_1\}) \quad (\mathcal{G}_1, \mathcal{K}_1, \nu\Sigma\{e_2 \parallel \mu\}) \Downarrow (\mathcal{G}_2, \mathcal{K}_2, \nu\Sigma_2\{e_2 \parallel \mu_2\})}{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{\langle e_1, e_2 \rangle \parallel \mu\}) \Downarrow (\mathcal{G}_2, \mathcal{K}_2, \nu\Sigma_1 \cup \Sigma_2\{e_1 \parallel \mu_1 \cup \mu_2\})} \end{array}$$

Because of this, \mathcal{G} and \mathcal{K} are omitted from the stepping rules, and will only be included in the rule where they are modified/interacted with (i.e. GEN-EVAL).

The rules dictating which expressions are considered to be values are given in Figure 3.7. The evaluation rules for cryptographic constructs are given in Figure 3.8, and the evaluation rules for the remaining constructs are in Figure 3.9.

Besides the rule for key generation, the most notable rule is ENC-EVAL. This rule is defined to be *nondeterministic*, since it chooses some arbitrary u from the encryption algorithm to return.

UNIT-VAL	NAT-VAL	PAIR-VAL	INJ-VAL-1	INJ-VAL-2
$\frac{}{\langle \rangle \text{val}_\Sigma}$	$\frac{}{\bar{n} \text{val}_\Sigma}$	$\frac{v_1 \text{val}_{\Sigma_1} \quad v_2 \text{val}_{\Sigma_2}}{\langle v_1, v_2 \rangle \text{val}_{\Sigma_1 \cup \Sigma_2}}$	$\frac{v_1 \text{val}_\Sigma}{1 \cdot v_1 \text{val}_\Sigma}$	$\frac{v_2 \text{val}_\Sigma}{2 \cdot v_2 \text{val}_\Sigma}$
LAM-VAL	ENC-VAL		OK-VAL	ERR-VAL
$\frac{}{\lambda(x : \tau_1. e) \text{val}_\Sigma}$	$\frac{u \in \mathcal{E}_\ell(v_k, v) \quad v \text{val}_\Sigma}{u \text{val}_\Sigma}$		$\frac{v \text{val}_\Sigma}{\text{Ok}(v) \text{val}_\Sigma}$	$\frac{}{\text{Error} \text{val}_\Sigma}$
KEY-VAL				
$\frac{}{\text{key}\langle K \rangle \text{val}_{\Sigma, K \sim \ell}}$				

Figure 3.7: Inference rules for the judgment $e \text{val}_\Sigma$

ENC-EVAL
$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{v_2 \parallel \mu_2\} \quad u \in \mathcal{E}_\ell(v_k, v)}{\nu\Sigma\{\text{encrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{u \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}$
DEC-SUCC-EVAL
$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{u \parallel \mu_2\} \quad \mathcal{D}_\ell(v_k, u) = v}{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\text{Ok}(v) \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}$
DEC-FAIL-EVAL
$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{u \parallel \mu_2\} \quad \mathcal{D}_\ell(v_k, u) = \perp}{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\text{Error} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}$
MATCH-ERR-EVAL
$\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\text{Error} \parallel \mu'\} \quad \nu\Sigma'\{e_0 \parallel \mu'\} \Downarrow \nu\Sigma_0\{v_0 \parallel \mu_0\}}{\nu\Sigma\{\text{resMatch } e \{e_0 \mid x.e_1\} \parallel \mu\} \Downarrow \nu\Sigma_0\{v_0 \parallel \mu_0\}}$
MATCH-OK-EVAL
$\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\text{Ok}(v) \parallel \mu'\} \quad \nu\Sigma'\{[v/x]e_1 \parallel \mu'\} \Downarrow \nu\Sigma_1\{v_1 \parallel \mu_1\}}{\nu\Sigma\{\text{resMatch } e \{e_0 \mid x.e_1\} \parallel \mu\} \Downarrow \nu\Sigma'\{v_1 \parallel \mu'\}}$
GEN-EVAL
$\frac{\mathcal{G} = \mathcal{G}'[\ell \mapsto v_k :: v_k s] \quad \mathcal{K} = \mathcal{K}'[\ell \mapsto K :: K s]}{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{\text{gen}\langle \ell \rangle \parallel \mu\}) \Downarrow (\mathcal{G}'[\ell \mapsto v_k s], \mathcal{K}'[\ell \mapsto K s], \nu\Sigma, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu \otimes K \hookrightarrow v_k\})}$

Figure 3.8: Evaluation rules for cryptographic expressions

$$\begin{array}{c}
\text{PAIR-EVAL} \\
\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{v_1 \parallel \mu_1\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{v_2 \parallel \mu_2\}}{\nu\Sigma\{\langle e_1, e_2 \rangle \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\langle v_1, v_2 \rangle \parallel \mu_1 \cup \mu_2\}} \\
\\
\text{PROJ-EVAL-1} \\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\langle v_1, v_2 \rangle \parallel \mu'\} \quad (i \in \{1, 2\})}{\nu\Sigma\{e \cdot i \parallel \mu\} \Downarrow \nu\Sigma'\{v_i \parallel \mu'\}} \\
\\
\text{INJ-EVAL-1} \\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{v \parallel \mu'\} \quad (i \in \{1, 2\})}{\nu\Sigma\{i \cdot e \parallel \mu\} \Downarrow \nu\Sigma'\{i \cdot v \parallel \mu'\}} \\
\\
\text{CASE-EVAL-1} \\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{1 \cdot v_1 \parallel \mu'\} \quad \nu\Sigma'\{[v_1/x_1]e_1 \parallel \mu'\} \Downarrow \nu\Sigma_1\{v \parallel \mu_1\}}{\nu\Sigma\{\text{case } e \{ x_1.e_1 \mid x_2.e_2 \} \parallel \mu\} \Downarrow \nu\Sigma_1\{v \parallel \mu_1\}} \\
\\
\text{CASE-EVAL-2} \\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{2 \cdot v_2 \parallel \mu'\} \quad \nu\Sigma'\{[v_2/x_2]e_2 \parallel \mu'\} \Downarrow \nu\Sigma_2\{v \parallel \mu_2\}}{\nu\Sigma\{\text{case } e \{ x_1.e_1 \mid x_2.e_2 \} \parallel \mu\} \Downarrow \nu\Sigma_2\{v \parallel \mu_2\}} \\
\\
\text{APP-EVAL} \\
\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\lambda(x : \tau_1.e) \parallel \mu_1\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{v_2 \parallel \mu_2\} \quad \nu\Sigma_1 \cup \Sigma_2\{[v_2/x]e \parallel \mu_1 \cup \mu_2\} \Downarrow \nu\Sigma^*\{v \parallel \mu^*\}}{\nu\Sigma\{e_1(e_2) \parallel \mu\} \Downarrow \nu\Sigma^*\{v \parallel \mu^*\}}
\end{array}$$

Figure 3.9: Evaluation rules for non-cryptographic expressions

Chapter 4

Logical Relations

In this chapter, we define the verification framework for proving noninterference. First, we will specify a strategy for proving noninterference in the face of nondeterminism (via possibilistic noninterference), and then we will present the prerequisite definitions for the proof, including a set-lifted dynamics and a logical relation for leaf-determinism. Afterwards, we will define the logical relations for proving possibilistic noninterference and prove the “fundamental theorem” of the logical relations, which shows that the logical relations subsume well-typed programs as a part of their verification guarantees.

4.1 Possibilistic Noninterference

Recall the two assumptions we made in Section 2.3 about encryption schemes in this setting. We have discussed the importance of Item 2 in the determinism of decryption, but now that we have fully defined our language, we can discuss Item 1 and its relevance to noninterference, particularly when it comes to occlusion.

As Askarov et al. [2] point out, it would be a mistake to take the indistinguishability of high-security ciphertexts to mean that all ciphertexts should simply be considered equivalent to one another. To elucidate this, recall the occlusive example from Section 1.1:

$$\begin{aligned} &\text{let } x = \text{encrypt}(k, v) \text{ in} \\ &\quad \text{if } h \text{ then } \langle x, x \rangle \text{ else } \langle x, \text{encrypt}(k, v) \rangle \end{aligned}$$

If all ciphertexts are considered to be equivalent, then the above example would be accepted as noninterfering, since there is no difference between x and $\text{encrypt}(k, v)$ in that case. However, for an attacker who has access to the source code and can physically compare the pair of ciphertexts, they would still be able to learn the value of h .

To address the above issue, Askarov et al. [2] utilize the notion of *possibilistic noninterference* [10]. At a high level, when checking possibilistic noninterference for expressions (e_1, e_2) , we consider the sets of values $(\mathbb{V}_1, \mathbb{V}_2)$ that the expressions respectively evaluate to. Then, for all $v_1 \in \mathbb{V}_1$, we check whether there exists a *possible* value $v_2 \in \mathbb{V}_2$ that is equivalent, and we do the same thing for each $v_2 \in \mathbb{V}_2$. If there does exist a possibility for each value in each respective set, the two expressions can be considered equivalent.

More concretely, for some relation $\mathbf{equiv}(v_1, v_2)$, we want to show the following:

$$\forall v_1 \in \mathbb{V}_1. \exists v_2 \in \mathbb{V}_2. \mathbf{equiv}(v_1, v_2)$$

$$\forall v_2 \in \mathbb{V}_2. \exists v_1 \in \mathbb{V}_1. \mathbf{equiv}(v_1, v_2)$$

By doing this, we are able to “flatten” the nondeterminism in the language and have noninterference cover every possibility immediately, rather than only considering an arbitrary choice.

While this is a step in the right direction for the occlusive example, we have yet to solve the issue of defining equivalence between ciphertexts, even with the consideration of all possibilities. Thus, Askarov et al. [2] define a relation \doteq to represent equivalence at ξ between two ciphertexts as follows:

Definition 3. For $\ell \not\sqsubseteq \xi$, we have

1. $\forall u_1 \in \mathcal{E}_\ell(v_{k1}, v_1) \implies \exists u_2. u_2 \in \mathcal{E}_\ell(v_{k2}, v_2) \wedge u_1 \doteq u_2$
2. $\exists u_1, u_2. u_1 \in \mathcal{E}_\ell(v_{k1}, v_1) \wedge u_2 \in \mathcal{E}_\ell(v_{k2}, v_2) \wedge u_1 \not\dot{=} u_2$

In the above definition, the first part allows for safe usage of encryption, and the second prevents occlusion. For the former, the fact that there exists a ciphertext u_2 for any ciphertext u_1 with $u_1 \doteq u_2$ allows one to satisfy the \mathbf{equiv} relation in possibilistic noninterference. For the latter, we can use it to show how our running occlusive example would be rejected when comparing two different substitutions for h .

Proof. Suppose the example is noninterfering. In that case, when h is substituted for `true`, we have the set of possible values

$$\mathbb{V}_1 = \{\langle u, u \rangle \mid u \in \mathcal{E}_\ell(k, v)\}$$

In the case that h is substituted for `false`, we have the set of possible values

$$\mathbb{V}_2 = \{\langle u_1, u_2 \rangle \mid u_1 \in \mathcal{E}_\ell(k, v), u_2 \in \mathcal{E}_\ell(k, v)\}$$

Suppose we pick u_1 and u_2 such that $u_1 \not\dot{=} u_2$. Then there would not exist an element in \mathbb{V}_1 that is equivalent to an element in \mathbb{V}_2 , since each element in \mathbb{V}_1 is of the form $\langle u, u \rangle$. Thus, these programs cannot be noninterfering. \square

This sets the foundation for our strategy going forward. In the next section, we will define the *set-lifted dynamics*, a proof-specific set of rules which make explicit the set of possible values an expression evaluates to. Afterwards, we define a well-formedness condition called *leaf-determinism* to ensure that the only source of nondeterminism in the language is from encryption. From there, we can put these ideas together to make our outline of possibilistic more concrete.

$$\begin{array}{c}
\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V} \parallel \mu_2\} \quad \mathbb{U} = \{u \mid v \in \mathbb{V}, u \in \mathcal{E}_\ell(v_k, v)\}}{\nu\Sigma\{\text{encrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\mathbb{U} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}} \\
\\
\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{U} \parallel \mu_2\} \quad \mathbb{V} = \{\mathcal{D}(v_k, u) \mid u \in \mathbb{U}\}}{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\{\text{Ok}(v) \mid v \in \mathbb{V}\} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}} \\
\\
\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{U} \parallel \mu_2\} \quad (\mathcal{D}(v_k, u) = \perp)_{\forall u \in \mathbb{U}}}{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\{\text{Error}\} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}} \\
\\
\frac{\nu\Sigma\{\text{Error} \parallel \mu\} \Downarrow \nu\Sigma\{\{\text{Error}\} \parallel \mu\} \quad \nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\}}{\nu\Sigma\{\text{Ok}(e) \parallel \mu\} \Downarrow \nu\Sigma'\{\{\text{Ok}(v) \mid v \in \mathbb{V}\} \parallel \mu'\}} \\
\\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\{\text{Error}\} \parallel \mu'\} \quad \nu\Sigma'\{e_0 \parallel \mu'\} \Downarrow \nu\Sigma_0\{\mathbb{V}_0 \parallel \mu_0\}}{\nu\Sigma\{\text{resMatch } e \{e_0 \mid x_1.e_1\} \parallel \mu\} \Downarrow \nu\Sigma_0\{\mathbb{V}_0 \parallel \mu_0\}} \\
\\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (\nu\Sigma'\{[v'/x]e_1 \parallel \mu'\} \Downarrow \nu\Sigma_1\{\mathbb{V}^v \parallel \mu_1\})_{v=\text{Ok}(v')}}{\nu\Sigma\{\text{resMatch } e \{e_0 \mid x_1.e_1\} \parallel \mu\} \Downarrow \nu\Sigma_1\{\bigcup_{v \in \mathbb{V}} \mathbb{V}^v \parallel \mu_1\}} \\
\\
\frac{\mathcal{G} = \mathcal{G}'[\ell \mapsto v_k :: v_k s] \quad \mathcal{K} = \mathcal{K}'[\ell \mapsto K :: K s]}{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{\text{gen}\langle \ell \rangle \parallel \mu\}) \Downarrow (\mathcal{G}'[\ell \mapsto v_k s], \mathcal{K}'[\ell \mapsto K s], \nu\Sigma, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu \otimes K \hookrightarrow v_k\})} \\
\\
\frac{}{\nu\Sigma, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu \otimes K \hookrightarrow v_k\} \Downarrow \nu\Sigma, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu \otimes K \hookrightarrow v_k\}}
\end{array}$$

Figure 4.1: Set-lifted evaluation rules for cryptographic expressions

$$\begin{array}{c}
\frac{}{\nu\Sigma\{\langle \rangle \parallel \mu\} \Downarrow \nu\Sigma\{\{\langle \rangle\} \parallel \mu\}} \qquad \frac{}{\nu\Sigma\{\bar{n} \parallel \mu\} \Downarrow \nu\Sigma\{\{\bar{n}\} \parallel \mu\}} \\
\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_2\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}}{\nu\Sigma\{\langle e_1, e_2 \rangle \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\} \parallel \mu_1 \cup \mu_2\}} \\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (i \in \{1, 2\})}{\nu\Sigma\{e \cdot i \parallel \mu\} \Downarrow \nu\Sigma'\{\{v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}\} \parallel \mu'\}} \qquad \frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (i \in \{1, 2\})}{\nu\Sigma\{i \cdot e \parallel \mu\} \Downarrow \nu\Sigma'\{\{i \cdot v \mid v \in \mathbb{V}\} \parallel \mu'\}} \\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (\nu\Sigma'\{[v'/x_1]e_1 \parallel \mu'\} \Downarrow \nu\Sigma_1\{\mathbb{V}^v \parallel \mu_1\})_{v=1..v'}}{\nu\Sigma\{\text{case } e \{x_1.e_1 \mid x_2.e_2\} \parallel \mu\} \Downarrow \nu\Sigma_1\{\bigcup_{v \in \mathbb{V}} \mathbb{V}^v \parallel \mu_1\}} \\
\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (\nu\Sigma'\{[v'/x_2]e_2 \parallel \mu'\} \Downarrow \nu\Sigma_2\{\mathbb{V}^v \parallel \mu_2\})_{v=2..v'}}{\nu\Sigma\{\text{case } e \{x_1.e_1 \mid x_2.e_2\} \parallel \mu\} \Downarrow \nu\Sigma_2\{\bigcup_{v \in \mathbb{V}} \mathbb{V}^v \parallel \mu_2\}} \\
\frac{}{\nu\Sigma\{\lambda(x : \tau_1.e) \parallel \mu\} \Downarrow \nu\Sigma\{\{\lambda(x : \tau_1.e)\} \parallel \mu\}} \\
\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}}{(\nu\Sigma_1 \cup \Sigma_2\{[v_2/x]e \parallel \mu_1 \cup \mu_2\} \Downarrow \nu\Sigma^*\{\mathbb{V}^{v_1, v_2} \parallel \mu^*\})_{v_1 = \lambda(x : \tau_1.e)}} \\
\nu\Sigma\{e_1(e_2) \parallel \mu\} \Downarrow \nu\Sigma^*\{\bigcup_{(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2} \mathbb{V}^{v_1, v_2} \parallel \mu^*\}
\end{array}$$

Figure 4.2: Set-lifted evaluation rules for non-cryptographic expressions

4.2 Set-Lifted Dynamics

We now define the judgment

$$\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\}$$

where e is an expression and \mathbb{V} is the set of possible values that e could evaluate to. The dynamics should ensure that for all $v \in \mathbb{V}$, $v \text{ val}_{\Sigma'}$, where Σ' is the “end state” signature from the evaluation judgment.

Even though the results are lifted to sets, the effects are still deterministic, and so the effects that were present in the original dynamics are the same in the new version. As such, we continue to omit the \mathcal{G} and \mathcal{K} maps except for in the rules where they are interacted with/modified.

The set-lifted dynamics for cryptographic expressions are given in Figure 4.1, and the dynamics for non-cryptographic expressions are given in Figure 4.2.

4.3 Leaf-Determinism

In order to interact with the set-lifted dynamics, it is convenient to know that for a set of values, the only variation within that set comes from the presense of ciphertexts. For example, to apply the elimination rule for sums, one would need to assert that the set of values are either all of the form $1 \cdot v_1$ or all of the form $2 \cdot v_2$, and not some mixture of the two injections. In other words, we would like to show that the only source of nondeterminism in the language is from encryption, and that otherwise the sets of values are “uniform.”

Askarov et al. [2] introduces this exact property as “leaf-determinism,” and defines it as a relation on well-typed terms. However, since leaf-determinism is a semantic property (i.e. it is a consequence of how the set-lifted dynamics are defined), we define the property using a logical relation. In this definition, we define a term interpretation $\mathbb{E} \in \mathcal{L}_{\Sigma}[\tau]$ and a value interpretation $\mathbb{V} \in \mathcal{LV}_{\Sigma}[\tau]$. In the term interpretation, the symbol \mathbb{E} represents a set of expressions, and \mathbb{E} being an inhabitant of the logical relation means that for all expressions $e \in \mathbb{E}$, e evaluates to a set of values \mathbb{V} such that the union of all those sets \mathbb{V} is leaf-deterministic at type τ . This is quite a strong statement — we’re claiming not only that each of the individual expressions produce well-formed sets, but that each of these sets also comply with one another. For $\mathbb{V} \in \mathcal{LV}_{\Sigma}[\tau]$, we proceed by induction on the type, characterizing what it means for \mathbb{V} to be a well-formed set of τ values. The logical relations are also indexed with the signature Σ of keys in order to verify the well-formedness of key values.

The definition of the logical is given in Figure 4.3. As a part of the logical relation, we define and make use of the following judgments:

- We define the judgment $\Sigma' \leq \Sigma$ to say that Σ is a “future world” of Σ' . This means that, for all $K \sim \ell \in \Sigma'$, we have $K \sim \ell \in \Sigma$.
- We define the judgment $\mu : \Sigma$ to describe some memory μ being well-formed with respect to Σ . This judgment is defined as

$$\frac{\forall K \in \mu. K \sim \ell \in \Sigma \text{ (for some } \ell) \quad \forall K \sim \ell \in \Sigma. \mu(K) = v_k \quad \mathcal{G}(\ell) = v_k}{\mu : \Sigma}$$

$$\begin{aligned}
\mathbb{E} \in \mathcal{L}_\Sigma[\tau] &\iff \text{if } \mu : \Sigma \text{ then we have} \\
&\quad \forall e \in \mathbb{E}. \nu_\Sigma\{e \parallel \mu\} \Downarrow \nu_{\Sigma'}\{\mathbb{V}^e \parallel \mu'\} \wedge \mu' : \Sigma' \wedge \\
&\quad \bigcup_{e \in \mathbb{E}} \mathbb{V}^e \in \mathcal{L}_{\mathcal{V}_{\Sigma'}}[\tau] \\
\mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[\text{unit}] &\iff \mathbb{V} = \{\langle \rangle\} \\
\mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[\text{nat}] &\iff \mathbb{V} = \{n\}, n \in \mathbb{N} \\
\mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau_1 \times \tau_2] &\iff \mathbb{V} = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\}, \\
&\quad \mathbb{V}_1 \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau_1] \wedge \mathbb{V}_2 \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau_2] \\
\mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau_1 \xrightarrow{\ell_k} \tau_2] &\iff \forall v \in \mathbb{V}, v =_\alpha \lambda(x : \tau_1). e \\
&\quad \forall \Sigma' \text{ s.t. } \Sigma' \leq \Sigma, \\
&\quad \forall \mathbb{V}_1 \in \mathcal{L}_{\mathcal{V}_{\Sigma'}}[\tau_1], \\
&\quad \{[v_1/x]e \mid v_1 \in \mathbb{V}_1\} \in \mathcal{L}_{\Sigma'}[\tau_2] \\
\mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[\text{key}_\ell] &\iff \mathbb{V} = \{\text{key}\langle K \rangle\} \wedge K \sim \ell \in \Sigma \\
\mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[(\tau_1 + \tau_2)_\ell] &\iff (\mathbb{V} = \{1 \cdot v_1 \mid v_1 \in \mathbb{V}_1\} \text{ for } \mathbb{V}_1 \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau_1]) \vee \\
&\quad (\mathbb{V} = \{2 \cdot v_2 \mid v_2 \in \mathbb{V}_2\} \text{ for } \mathbb{V}_2 \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau_2]) \\
\mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau \text{ result}_\ell] &\iff \mathbb{V} = \{\text{Error}\} \vee \\
&\quad (\mathbb{V} = \{\text{Ok}(v') \mid v' \in \mathbb{V}'\} \text{ for } \mathbb{V}' \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau]) \\
\mathbb{U} \in \mathcal{L}_{\mathcal{V}_\Sigma}[(\text{enc}_\ell \tau)_\epsilon] &\iff \mathbb{U} = \{u \mid u \in \mathcal{E}_\ell(v_k, v), v \in \mathbb{V}\} \text{ such that } \mathbb{V} \in \mathcal{L}_{\mathcal{V}_\Sigma}[\tau]
\end{aligned}$$

Figure 4.3: Logical relation for leaf-determinism

Observe how the sum case, among others, ensures that each of the values in the set is constructed with the same injection. Another interesting case to consider is the arrow case. We begin by quantifying a future signature Σ' and using it to introduce an arbitrary set $\mathbb{V}_1 \in \mathcal{L}_{\mathcal{V}_{\Sigma'}}[\tau_1]$. This is a common pattern in defining the arrow case — we quantify the inputs to the function a future world since keys could have been added since the function was defined. Afterwards, we check whether the set $\{[v_1/x]e \mid v_1 \in \mathbb{V}_1\} \in \mathcal{L}_{\Sigma'}[\tau_2]$, since the result of the substitution is a set of expressions. In other words, we check that a set of lambdas is leaf-deterministic by checking whether they produce leaf-deterministic sets of values (given well-formed inputs).

Next, we define the *fundamental theorem* for the leaf-determinism logical relation. The fundamental theorem bridges the gap between static well-formedness and semantic verification by claiming that any well-typed expression is also a well-behaved inhabitant of the relation. Since the fundamental theorem is defined for possibly open terms, we begin by defining a closing substitution.

Definition 4 (Well-Formed Substitution Map (LD)). *The judgment $\sigma :_{\text{LD}} \Gamma; \Sigma$ is defined as*

$$\sigma :_{\text{LD}} \Gamma; \Sigma \triangleq \forall x : \tau \in \Gamma, \sigma(x) \in \mathcal{L}\mathcal{V}_\Sigma[\tau]$$

The closing substitution $\hat{\sigma}(e)$ is defined by structural induction on the expression e , with an example case being

$$\hat{\sigma}(\langle e_1, e_2 \rangle) \triangleq \{ \langle v_1, v_2 \rangle \mid v_1 \in \hat{\sigma}(e_1), v_2 \in \hat{\sigma}(e_2) \}$$

Note that different values from σ could be substituted for the same variable in e_1 and e_2 . This is not an issue, since the values being plugged in come from a leaf-deterministic set, meaning interchanging any individual value from that set should not affect the well-formedness of the final result.

With this, we are ready to define the fundamental theorem for leaf-determinism:

Theorem 1 (Leaf-Determinism FTLR). *If $\Sigma; \Gamma \vdash_{\text{kc}} e : \tau, \forall \Sigma'$ such that $\Sigma' \leq \Sigma$, if $\sigma :_{\text{LD}} \Gamma; \Sigma'$, then $\hat{\sigma}(e) \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau]$.*

The proof for the fundamental theorem can be found in Appendix A.1.2.

The proof of the fundamental theorem makes use of the following lemmas. Their proofs/outlines can be found in Appendix A.1.1.

Lemma 2 (LD-Antimonotonicity). *If $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau]$ and $\Sigma' \leq \Sigma$, then $\mathbb{V} \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau]$.*

Lemma 3. *If $\sigma :_{\text{LD}} \Gamma; \Sigma$ and $\Sigma' \leq \Sigma$, then $\sigma :_{\text{LD}} \Gamma; \Sigma'$.*

Lemma 4. *If $\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\}$, then $|\mathbb{V}| > 0$.*

Lemma 5. *If $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau]$, then $|\mathbb{V}| \geq 1$.*

Lemma 6. *If $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau]$ and $\mathbb{V}' \subseteq \mathbb{V}$ with $|\mathbb{V}'| \geq 1$, then $\mathbb{V}' \in \mathcal{L}\mathcal{V}_\Sigma[\tau]$.*

Lemma 7 (LD-Subtype). *If $\tau' \leq \tau$ and $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau']$, then $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau]$.*

4.3.1 Sets to Singletons

In the next section, we will define the fundamental theorems which are used for proving possibilistic noninterference. In the fundamental theorem, we find it necessary to define the closing substitution to be over elements from a set of leaf-deterministic values, rather than just individually well-formed elements. This goes back to the original motivation behind leaf-determinism — we want to be able to apply the set-lifted dynamics rules, and to do that we want to be able to argue about the conformity of sets of values. The following lemmas and definitions are in service of that.

We begin by defining the following operation which lifts a regular map to the set-lifted version used in the Theorem 1:

Definition 5. *Define the operation $\mathbf{set}(\gamma)$ on maps γ such that $\text{dom}(\mathbf{set}(\gamma)) = \text{dom}(\gamma)$ and $\forall x \in \text{dom}(\gamma). \mathbf{set}(\gamma)(x) = \{\gamma(x)\}$.*

We then have the following lemmas on the operation. Their proofs can be found in Appendix A.1.1.

Lemma 8. *For all σ such that $\sigma :_{\text{LD}} \Gamma; \Sigma$ and $\forall \gamma \in \mathbf{sing}(\sigma). \gamma : \Gamma; \Sigma$, then $\mathbf{set}(\gamma) :_{\text{LD}} \Gamma; \Sigma$.*

Lemma 9. For all σ_1, σ_2 such that $\sigma_1 :_{\text{LD}} \Gamma; \Sigma_1$, $\sigma_2 :_{\text{LD}} \Gamma; \Sigma_2$, and $\forall(\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2)$. $\gamma_1 \equiv_{\xi} \gamma_2 : \Gamma; (\Sigma_1 \uplus \Sigma_2)$, $\text{set}(\gamma_1) :_{\text{LD}} \Gamma; \Sigma_1$ and $\text{set}(\gamma_2) :_{\text{LD}} \Gamma; \Sigma_2$.

Lemma 10. For all expressions e and maps γ , $\widehat{\text{set}(\gamma)}(e) = \{\hat{\gamma}(e)\}$.

In the next section, we will define corollaries of Theorem 1 which will be used in the fundamental theorem proofs for the logical relations.

4.4 Binary and Unary Relations

Finally, we can define the binary logical relation which will serve as our verifier for possibilistic noninterference. As with the previous logical relation, this one is split into a term and value interpretation. For $(e_1, e_2) \in \mathcal{E}_{\Sigma_1, \Sigma_2}^{\xi}[\tau]$, we say that (e_1, e_2) inhabit the term interpretation if, given equivalent starting memories, they both evaluate to sets \mathbb{V}_1 and \mathbb{V}_2 such for each $v_1 \in \mathbb{V}_1$, there exists a possible equivalent value in \mathbb{V}_2 according to the value interpretation at that type (and vice versa for \mathbb{V}_2). The binary relation also checks that the resultant memories are equivalent up to the observer level, ensuring that both the observable values and effects are indistinguishable between the two programs. The value interpretation then defines equivalence at a given type between two values, while also casing on whether the value is considered observable in the first place (with respect to ξ). If the values are being checked at an unobservable type, then there is no obligation for them to be actually equivalent to one another, and the binary relation dispenses to the unary one.

For completeness, we have included the treatment of the the key streams \mathcal{G} and \mathcal{K} as a part of the term interpretation in grey font, but as with the dynamics rules, they are only relevant for the cases where they are manipulated by the $\text{gen}\langle \ell \rangle$ operator. Thus, they are deemphasized in both the logical relation and the proof.

The binary logical relation can be found in Figure 4.4. It makes use of the following definitions:

- We define the judgment $\mu \equiv_{\xi} \mu' : \Sigma \uplus \Sigma'$ to be exactly equality on observable memory. This means that $\mu : \Sigma$, $\mu' : \Sigma'$, and,
 - For all $K \sim \ell \in \Sigma$ such that $\ell \sqsubseteq \xi$, it must be the case that $K \sim \ell \in \Sigma'$ with $\mu(K) = \mu'(K)$, i.e. the bitstring values of the keys are exactly equal (and vice versa for keys $K' \sim \ell' \in \Sigma'$ such that $\ell' \sqsubseteq \xi$)
 - For all $K \sim \ell \in \Sigma$ and $K' \sim \ell' \in \Sigma'$ such that $\ell \not\sqsubseteq \xi$ and $\ell' \not\sqsubseteq \xi$, they are trivially related.
- We define the judgment $(\mathcal{G}_1, \mathcal{K}_1) \equiv_{\xi} (\mathcal{G}_2, \mathcal{K}_2)$ to be exact equality on observable key streams. This means that $\mathcal{G}_1(\ell) \approx \mathcal{G}_2(\ell)$ and $\mathcal{K}_1(\ell) \approx \mathcal{K}_2(\ell)$ for all security labels, defined as follows
 - For all $\ell \sqsubseteq \xi$, $\mathcal{G}_1(\ell) \approx \mathcal{G}_2(\ell)$ means:
 - $[\] \approx [\]$
 - $v_k :: v_k s \approx v'_k :: v_k s'$ if $v_k = v'_k$ (i.e. the key value bitstrings are exactly equal to one another) and $v_k s \approx v_k s'$

Similarly, for $\ell \sqsubseteq \xi$, $\mathcal{K}_1(\ell) \approx \mathcal{K}_2(\ell)$ means:

- $[] \approx []$
- $K :: Ks \approx K' :: Ks'$ if $K = K'$ (i.e. the symbols/strings are the same) and $Ks \approx Ks'$
- For all $\ell \not\sqsubseteq \xi$, the streams are trivially related.

We highlight the following notable cases:

- For the arrow case, as with the leaf-determinism relation, we quantify over future worlds for the inputs, but we also quantify a set of leaf-deterministic values which are “possibilistically noninterferent” with one another, rather than a single pair of inputs. This reflects a general expectation for substitutions, both in this particular case of the logical relation and in the statement of the fundamental theorem, that expectation being that the values being substituted in come from a set of leaf-deterministic values. This allows us to utilize results from leaf-determinism within the proof.
- For the ciphertext type, we dispatch on whether the key used to encrypt the plaintext is observable to ξ . If it is not, this means that we have a high-security (i.e. unobservable) encryption, and so, according to our cryptographic assumptions, the attacker cannot learn anything about the underlying plaintext. As such, we can at most enforce the well-formedness of the underlying plaintext, as well as the equivalence of the ciphertext themselves. On the other hand, when ℓ is observable, that means that the attacker does potentially have access to the underlying value, so we should be sure that the underlying plaintexts also agree.

We then also define the unary logical relation, which, for an expression $e \in \mathcal{E}_\Sigma[[\tau]][\text{kc}]$, checks that e is a well-behaved expression at type τ , but also verifies that the levels of any keys generated are lower bounded by the parameter kc . This additional constraint assists with validating values at the arrow type, which carries a latent effect label ℓ_k that lower bounds the key levels that can be generated by applying the body. It also assists with the proving of Lemma 13, a lemma which claims that if two expressions are at an unobservable type, it is sufficient to prove that they individually inhabit the unary relation to show they are in the binary. Having the logical relation ensure that the two expression don’t have any observable effects is the key to showing that they are in the binary relation, since the binary enforces memory compliance.

The unary logical relation can be found in Figure 4.5.

4.4.1 Fundamental Theorems

Before we can state the binary fundamental theorem, we define the following judgments on closing substitutions γ :

Definition 6. Define $\gamma : \Gamma; \Sigma$ to be $\forall x : \tau \in \Gamma, \gamma(x) \in \mathcal{V}_\Sigma^\xi[[\tau]]$.

Definition 7. Define $\gamma \equiv_\xi \gamma' : \Gamma; (\Sigma \uplus \Sigma')$ to be $\forall x : \tau \in \Gamma, (\gamma(x), \gamma'(x)) \in \mathcal{V}_{\Sigma, \Sigma'}^\xi[[\tau]]$.

We also define the following operation to interact with sets of leaf-deterministic values:

Definition 8. Define the operation $\text{sing}(\sigma)$ by induction on the structure of σ as follows:

- If $\sigma = \emptyset$, then $\text{sing}(\emptyset) = \{\emptyset\}$
- If $\sigma = \sigma[x \mapsto \mathbb{V}]$, then $\text{sing}(\sigma[x \mapsto \mathbb{V}]) = \{\gamma[x \mapsto v] \mid \gamma \in \text{sing}(\sigma), v \in \mathbb{V}\}$

$$\begin{aligned}
(e_1, e_2) \in \mathcal{E}_{\Sigma_1, \Sigma_2}^\xi[\tau] &\iff \text{if } \mu_1 \equiv_\xi \mu_2 : \Sigma_1 \uplus \Sigma_2 \text{ and } (\mathcal{G}_1, \mathcal{K}_1) \equiv_\xi (\mathcal{G}_2, \mathcal{K}_2) \text{ then we have} \\
&(\mathcal{G}_1, \mathcal{K}_1, \nu_{\Sigma_1}\{e_1 \parallel \mu_1\}) \Downarrow (\mathcal{G}'_1, \mathcal{K}'_1, \nu_{\Sigma'_1}\{\mathbb{V}_1 \parallel \mu'_1\}) \\
&(\mathcal{G}_2, \mathcal{K}_2, \nu_{\Sigma_2}\{e_2 \parallel \mu_2\}) \Downarrow (\mathcal{G}'_2, \mathcal{K}'_2, \nu_{\Sigma'_2}\{\mathbb{V}_2 \parallel \mu'_2\}) \\
&\text{such that } \mu'_1 \equiv_\xi \mu'_2 : \Sigma'_1 \uplus \Sigma'_2 \wedge (\mathcal{G}'_1, \mathcal{K}'_1) \equiv_\xi (\mathcal{G}'_2, \mathcal{K}'_2) \wedge \\
&\forall v_1 \in \mathbb{V}_1, \exists v_2 \in \mathbb{V}_2. (v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau] \wedge \\
&\forall v_2 \in \mathbb{V}_2, \exists v_1 \in \mathbb{V}_1. (v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau] \\
\\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[t_\ell] &\iff \begin{cases} (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[t] & \text{if } \ell \sqsubseteq \xi \\ v_1 \in \mathcal{V}_{\Sigma_1}^\xi[t] \wedge v_2 \in \mathcal{V}_{\Sigma_2}^\xi[t] & \text{if } \ell \not\sqsubseteq \xi \end{cases} \\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\text{unit}] &\iff v_1 = v_2 = \langle \rangle \\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1 \times \tau_2] &\iff v_1 = \langle v'_1, v''_1 \rangle, v_2 = \langle v'_2, v''_2 \rangle \\
&(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1] \wedge (v''_1, v''_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_2] \\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1 \xrightarrow{\ell_k} \tau_2] &\iff v_1 =_\alpha \lambda(x_1.e_1), v_2 =_\alpha \lambda(x_2.e_2) \\
&\forall \Sigma'_1 \text{ s.t. } \Sigma'_1 \leq \Sigma_1 \text{ and } \Sigma'_2 \text{ s.t. } \Sigma'_2 \leq \Sigma_2, \\
&\forall \mathbb{V}'_1, \mathbb{V}'_2 \text{ s.t. } \mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau_1], \mathbb{V}'_2 \in \mathcal{L}\mathcal{V}_{\Sigma'_2}[\tau_1], \\
&\text{and } \forall v'_1 \in \mathbb{V}_1, \exists v'_2 \in \mathbb{V}'_2, (v'_1, v'_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_1], \\
&\text{and } \forall v'_2 \in \mathbb{V}_2, \exists v'_1 \in \mathbb{V}'_1, (v'_1, v'_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_1], \\
&\forall \text{such } (v'_1, v'_2), ([v'_1/x_1]e_1, [v'_2/x_2]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_2] \wedge \\
&(v_1 \in \mathcal{V}_{\Sigma_1}[\tau_1 \xrightarrow{\ell_k} \tau_2] \wedge v_2 \in \mathcal{V}_{\Sigma_2}[\tau_1 \xrightarrow{\ell_k} \tau_2]) \\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\text{key}_\ell] &\iff v_1 = \text{key}\langle K_1 \rangle, v_2 = \text{key}\langle K_2 \rangle, K_1 \sim \ell_1 \in \Sigma_1, K_2 \sim \ell_2 \in \Sigma_2 \wedge \\
&\begin{cases} K_1 = K_2 & \text{if } \ell \sqsubseteq \xi \\ v_1 \in \mathcal{V}_{\Sigma_1}^\xi[\text{key}_\ell] \wedge v_2 \in \mathcal{V}_{\Sigma_2}^\xi[\text{key}_\ell] & \text{if } \ell \not\sqsubseteq \xi \end{cases} \\
\\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\text{nat}] &\iff v_1 = v_2 = \bar{n}, n \in \mathbb{N} \\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1 + \tau_2] &\iff (v_1 = 1 \cdot v'_1, v_2 = 1 \cdot v'_2 \wedge (v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1]) \vee \\
&(v_1 = 2 \cdot v'_1, v_2 = 2 \cdot v'_2 \wedge (v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_2]) \\
(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau \text{ result}] &\iff (v_1 = v_2 = \text{Error}) \vee \\
&(v_1 = \text{Ok}(v'_1), v_2 = \text{Ok}(v'_2) \wedge (v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau]) \\
(u_1, u_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\text{enc}_\ell \tau] &\iff \exists v_i, v_{ki}. v_i = \mathcal{D}_\ell(v_{ki}, u_i) (i \in \{1, 2\}), \\
&\begin{cases} v_1 \in \mathcal{V}_{\Sigma_1}^\xi[\tau] \wedge v_2 \in \mathcal{V}_{\Sigma_2}^\xi[\tau] \wedge u_1 \doteq u_2 & \text{if } \ell \not\sqsubseteq \xi \\ v_{k1} = v_{k2} \wedge (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau] & \text{if } \ell \sqsubseteq \xi \end{cases}
\end{aligned}$$

Figure 4.4: Binary logical relation

$$\begin{aligned}
e \in \mathcal{E}_\Sigma[[\tau]][\text{kc}] &\iff \text{if } \mu : \Sigma \text{ then we have} \\
&\quad (\mathcal{G}, \mathcal{K}, \nu\Sigma\{e \parallel \mu\}) \Downarrow (\mathcal{G}', \mathcal{K}', \nu\Sigma'\{\mathbb{V} \parallel \mu'\}) \wedge \\
&\quad \forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma'}[[\tau]] \wedge \mu' : \Sigma' \wedge \\
&\quad \forall K \sim \ell \in (\Sigma' \setminus \Sigma). \text{kc} \sqsubseteq \ell \\
\\
v \in \mathcal{V}_\Sigma[[t_\ell]] &\iff v \in \mathcal{V}_\Sigma[[t]] \\
v \in \mathcal{V}_\Sigma[[\text{unit}]] &\iff v = \langle \rangle \\
v \in \mathcal{V}_\Sigma[[\tau_1 \times \tau_2]] &\iff v = \langle v_1, v_2 \rangle, \\
&\quad v_1 \in \mathcal{V}_\Sigma[[\tau_1]] \wedge v_2 \in \mathcal{V}_\Sigma[[\tau_2]] \\
v \in \mathcal{V}_\Sigma[[\tau_1 \xrightarrow{\ell_k} \tau_2]] &\iff v =_\alpha \lambda(x.e_2) \\
&\quad \forall \Sigma' \text{ s.t. } \Sigma' \leq \Sigma, \\
&\quad \forall \mathbb{V}_1 \text{ s.t. } \mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'}[[\tau_1]] \text{ and } \forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma'}[[\tau_1]], \\
&\quad [v_1/x]e_2 \in \mathcal{E}_{\Sigma'}[[\tau_2]][\ell_k] \\
v \in \mathcal{V}_\Sigma[[\text{key}_\ell]] &\iff v = \text{key}\langle K \rangle \wedge K \sim \ell \in \Sigma \\
\\
v \in \mathcal{V}_\Sigma[[\text{nat}]] &\iff v = \bar{n}, n \in \mathbb{N} \\
v \in \mathcal{V}_\Sigma[[\tau_1 + \tau_2]] &\iff (v = 1 \cdot v_1 \wedge v_1 \in \mathcal{V}_\Sigma[[\tau_1]]) \vee \\
&\quad (v = 2 \cdot v_2 \wedge v_2 \in \mathcal{V}_\Sigma[[\tau_2]]) \\
v \in \mathcal{V}_\Sigma[[\tau \text{ result}]] &\iff v = \text{Error} \vee \\
&\quad (v = \text{Ok}(v') \wedge v' \in \mathcal{V}_\Sigma[[\tau]]) \\
u \in \mathcal{V}_\Sigma[[\text{enc}_\ell \tau]] &\iff \exists v, v_k. v = \mathcal{D}(v_k, u), \\
&\quad v \in \mathcal{V}_\Sigma[[\tau]]
\end{aligned}$$

Figure 4.5: Unary logical relation

In other words, the operation **sing** takes a set-map σ and breaks it down into a set of variable-maps γ for each choice of $v \in \sigma(x)$ for each variable $x \in \text{dom}(\sigma)$. Note that the **sing** operation is only defined if the set of values \mathbb{V} associated with any variable is non-empty, so implicitly this is a prerequisite on any σ which is called with **sing**.

We can then state the binary fundamental theorem:

Theorem 2 (Binary Fundamental Theorem). *If $\Gamma; \Sigma \vdash_{\text{kc}} e : \tau$, then $\forall \xi$,*

- $\forall \Sigma_1, \Sigma_2$ such that $\Sigma_1 \leq \Sigma$ and $\Sigma_2 \leq \Sigma$,
- $\forall \sigma_1, \sigma_2$ such that $\sigma_1 :_{\text{LD}} \Gamma; \Sigma_1$, $\sigma_2 :_{\text{LD}} \Gamma; \Sigma_2$, and

$$\forall \gamma_1 \in \mathbf{sing}(\sigma_1). \exists \gamma_2 \in \mathbf{sing}(\sigma_2). \gamma_1 \equiv_{\xi} \gamma_2 : \Gamma; (\Sigma_1 \uplus \Sigma_2)$$

$$\forall \gamma_2 \in \mathbf{sing}(\sigma_2). \exists \gamma_1 \in \mathbf{sing}(\sigma_1). \gamma_1 \equiv_{\xi} \gamma_2 : \Gamma; (\Sigma_1 \uplus \Sigma_2)$$

then \forall such $(\gamma_1, \gamma_2) \in \mathbf{sing}(\sigma_1) \times \mathbf{sing}(\sigma_2)$. $(\hat{\gamma}_1(e), \hat{\gamma}_2(e)) \in \mathcal{E}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau \rrbracket$.

For the proof of the binary fundamental theorem, it is necessary to also appeal to the unary fundamental theorem in the case that some expression is unobservable. We state it as follows:

Theorem 3 (Unary Fundamental Theorem). *If $\Gamma; \Sigma \vdash_{\text{kc}} e : \tau$, then*

- $\forall \Sigma'$ such that $\Sigma' \leq \Sigma$,
- $\forall \sigma$ such that $\sigma :_{\text{LD}} \Gamma; \Sigma'$ and $\forall \gamma \in \mathbf{sing}(\sigma)$. $\gamma : \Gamma; \Sigma'$,

then $\forall \gamma \in \mathbf{sing}(\sigma)$. $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'} \llbracket \tau \rrbracket [\text{kc}]$.

In short, the fundamental theorems are stated for substitutions whose values come from leaf-deterministic sets, not just those that satisfy the value interpretations. Observe that in the statement of the binary and unary fundamental theorems, we quantify the closing substitution over a future world, rather than the conventional method of advancing to a future world within the logical relation itself. This choice was informed by the dynamics of the system, where certain expressions (such as **case**) needed their premises to have access to future worlds in order for the IH to be applicable. We touch more on this in Section 5.1.

The proofs for the binary and unary fundamental theorems are in Appendix A.2 and Appendix A.3, respectively.

We then have the statement of noninterference, which follows as a corollary of Theorem 2 (stated as in Gregersen et al. [7]):

Corollary 1 (Noninterference). *Let $\xi, \perp, \top \in \mathcal{L}$ be security labels such that $\perp \sqsubseteq \xi$ and $\top \not\sqsubseteq \xi$. If we have*

- $x : (\text{unit} + \text{unit})_{\top}; \emptyset \vdash_{\perp} e : (\text{unit} + \text{unit})_{\perp}$,
- $\cdot; \emptyset \vdash_{\perp} v_1 : (\text{unit} + \text{unit})_{\top}$, and
- $\cdot; \emptyset \vdash_{\perp} v_2 : (\text{unit} + \text{unit})_{\top}$,

then

$$\nu \emptyset \{ [v_1/x]e \parallel \emptyset \} \Downarrow \nu \Sigma_1 \{ v'_1 \parallel \mu_1 \}$$

and

$$\nu \emptyset \{ [v_2/x]e \parallel \emptyset \} \Downarrow \nu \Sigma_2 \{ v'_1 \parallel \mu_2 \}$$

with $v'_1 = v'_2$ and $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$.

4.4.2 Lemmas

There are multiple lemmas which are utilized in both the binary and unary fundamental theorem proof, all of which are listed in this section. However, there are a few important lemmas which are worth highlighting specifically. The proofs for all of the lemmas can be found in Appendix A.4.

First, have the following corollaries of the Theorem 1, one for the binary and one for the unary:

Corollary 2. *If $\Sigma; \Gamma \vdash_{\text{kc}} e : \tau$, and*

- $\forall \Sigma'$ such that $\Sigma' \leq \Sigma$,
- $\forall \sigma$ such that $\sigma :_{\text{LD}} \Gamma; \Sigma'$ and $\forall \gamma \in \text{sing}(\sigma)$. $\gamma : \Gamma; \Sigma'$,
- $\mu : \Sigma'$,

we have $\forall \gamma \in \text{sing}(\sigma)$,

$$\nu_{\Sigma'}\{\hat{\gamma}(e) \parallel \mu\} \Downarrow \nu_{\Sigma''}\{\mathbb{V} \parallel \mu'\}$$

with $\mathbb{V} \in \mathcal{LV}_{\Sigma''}[\tau]$.

Corollary 3. *If $\Sigma; \Gamma \vdash_{\text{kc}} e : \tau$, and*

- $\forall \Sigma_1, \Sigma_2$ such that $\Sigma_1 \leq \Sigma$ and $\Sigma_2 \leq \Sigma$,
- $\forall \sigma_1, \sigma_2$ such that $\sigma_1 :_{\text{LD}} \Gamma; \Sigma_1$, $\sigma_2 :_{\text{LD}} \Gamma; \Sigma_2$, and $\forall (\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2)$. $\gamma_1 \equiv_{\xi} \gamma_2 : \Gamma; (\Sigma_1 \uplus \Sigma_2)$, and
- $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$,

we have $\forall (\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2)$,

$$\nu_{\Sigma_1}\{\hat{\gamma}_1(e) \parallel \mu_1\} \Downarrow \nu_{\Sigma'_1}\{\mathbb{V}_1 \parallel \mu'_1\}$$

$$\nu_{\Sigma_2}\{\hat{\gamma}_2(e) \parallel \mu_2\} \Downarrow \nu_{\Sigma'_2}\{\mathbb{V}_2 \parallel \mu'_2\}$$

with $\mathbb{V}_1 \in \mathcal{LV}_{\Sigma'_1}[\tau]$ and $\mathbb{V}_2 \in \mathcal{LV}_{\Sigma'_2}[\tau]$.

These corollaries serve as a shortcut between the powerful result from the leaf-determinism logical relation to the needs of the unary and binary FTLR proofs. In both of the proofs, leaf-determinism is only ever invoked on a single expression, while the leaf-determinism logical relation operates on a whole set of expressions. These corollaries specialize the statement to a singleton set and output a result better fit for the format of the proofs.

Next, we have the following three lemmas:

Lemma 11 (Binary-Unary Subsumption). *If $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[\tau]$, then $v_1 \in \mathcal{V}_{\Sigma_1}[\tau]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[\tau]$.*

Lemma 12 (Value Splitting Lemma). *If $\ell \triangleleft \tau$ and $\ell \not\preceq \xi$, then if $v \in \mathcal{V}_{\Sigma_1}[\tau]$ and $v' \in \mathcal{V}_{\Sigma_2}[\tau]$, then $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[\tau]$.*

Lemma 13 (Term Splitting Lemma). *If $\ell \triangleleft \tau$ and $\ell \not\preceq \xi$, then if $e \in \mathcal{E}_{\Sigma}[\tau][\text{kc}]$ and $e' \in \mathcal{E}_{\Sigma'}[\tau][\text{kc}]$ and $\text{kc} \not\preceq \xi$, then $(e, e') \in \mathcal{E}_{\Sigma, \Sigma'}^{\xi}[\tau]$.*

These lemmas serve as a way to commute between the binary and unary relations. Lemma 11 states that any values in the binary value interpretation are also individually in the unary interpretations. This is because, in addition to checking for equivalence, the binary relation enforces the “well-behavedness” of values at a given type in the same way the unary does. Lemma 12 and Lemma 13 are the opposite direction for Lemma 11. However, going from the unary to the

binary requires more conditions. In particular, it must be the case that the type τ is unobservable, otherwise the two values in the unary enforces nothing about their joint equivalence. Similarly, for Lemma 13, the bound on the effects in the unary term interpretation must be unobservable, otherwise there would be no way to enforce that two disjoint expressions have the same effects (which is what the binary requires).

The remaining lemmas, while utilized during the proof, are relatively straightforward.

Lemma 14 (Transitivity). *If $\Sigma_2 \leq \Sigma_1$ and $\Sigma_3 \leq \Sigma_2$, then $\Sigma_3 \leq \Sigma_1$.*

Lemma 15 (Unary Anti-Monotonicity). *If $v \in \mathcal{V}_\Sigma[\tau]$ and $\Sigma' \leq \Sigma$, then $v \in \mathcal{V}_{\Sigma'}[\tau]$.*

Lemma 16 (Binary Anti-Monotonicity). *If $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau]$ and $\Sigma'_1 \leq \Sigma_1$ and $\Sigma'_2 \leq \Sigma_2$, then $(v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau]$.*

Lemma 17. *If $\gamma : \Gamma; \Sigma$ and $\Sigma' \leq \Sigma$, then $\gamma : \Gamma; \Sigma'$.*

Lemma 18. *If $\gamma \equiv_\xi \gamma' : \Gamma; \Sigma_1 \uplus \Sigma_2$ and $\Sigma'_1 \leq \Sigma_1$, $\Sigma'_2 \leq \Sigma_2$, then $\gamma : \Gamma; \Sigma'_1 \uplus \Sigma'_2$.*

Lemma 19. *If $\mu_1 : \Sigma_1$ and $\mu_2 : \Sigma_2$, then $\mu_1 \cup \mu_2 : \Sigma_1 \cup \Sigma_2$.*

Lemma 20. *If $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and $\mu_2 \equiv_\xi \mu'_2 : \Sigma_2 \uplus \Sigma'_2$, then $\mu_1 \cup \mu_2 \equiv_\xi \mu'_1 \cup \mu'_2 : (\Sigma_1 \cup \Sigma_2) \uplus (\Sigma'_1 \cup \Sigma'_2)$.*

Lemma 21. *For all Σ_1, Σ_2 , $\Sigma_1 \cup \Sigma_2 \leq \Sigma_1$.*

Lemma 22. *For all $\Sigma_1, \Sigma_2, \Sigma_3$, if $\Sigma_1 \leq \Sigma_2$, then $\Sigma_1 \setminus \Sigma_3 = (\Sigma_1 \setminus \Sigma_2) \cup (\Sigma_2 \setminus \Sigma_3)$.*

Lemma 23. *If $(\mathcal{G}, \mathcal{K}, \nu\Sigma\{e \parallel \mu\}) \Downarrow (\mathcal{G}_1, \mathcal{K}_1, \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\})$ and $(\mathcal{G}, \mathcal{K}, \nu\Sigma\{e \parallel \mu\}) \Downarrow (\mathcal{G}_2, \mathcal{K}_2, \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\})$, then $\mathbb{V}_1 = \mathbb{V}_2$, $\Sigma_1 = \Sigma_2$, and $\mu_1 = \mu_2$ (and $\mathcal{G}_1 = \mathcal{G}_2$, $\mathcal{K}_1 = \mathcal{K}_2$).*

Lemma 24. *If $\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\}$, then $\Sigma' \leq \Sigma$.*

Lemma 25. *If $l_1 \not\sqsubseteq l_2$, then for all l , we have that $l_1 \sqcup l \not\sqsubseteq l_2$.*

Lemma 26. *If $l_1 \sqsubseteq l$ and $l_2 \sqsubseteq l$, then $l_1 \sqcup l_2 \sqsubseteq l$.*

Lemma 27. *If $l_1 \sqcup l_2 \sqsubseteq l$, then $l_1 \sqsubseteq l$ and $l_2 \sqsubseteq l$.*

Lemma 28. *If $l_1 \sqsubseteq l_2$ and $l_1 \not\sqsubseteq l_3$, then $l_2 \not\sqsubseteq l_3$.*

Lemma 29. *If $\gamma \equiv_\xi \gamma' : \Gamma; \Sigma \uplus \Sigma'$, then $\gamma : \Gamma; \Sigma$ and $\gamma' : \Gamma; \Sigma'$.*

Lemma 30 (Un-Subtype). *If $\tau' \leq \tau$, then if $v \in \mathcal{V}_\Sigma[\tau']$, then $v \in \mathcal{V}_\Sigma[\tau]$.*

Lemma 31 (Bin-Subtype). *If $\tau' \leq \tau$, then if $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau']$, then $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau]$.*

Chapter 5

Conclusion

5.1 Discussion

Our approach with the definition of the fundamental theorems, especially for the unary and binary fundamental theorems, makes an interesting departure from the typical approach for Kripke-style logical relations [1, 3, 11]. In particular, we ended up quantifying over future worlds in the statement of the fundamental theorem, rather than in the logical relation itself. We felt this was necessary because in the proof of the fundamental theorem, the induction hypothesis needed to be quantified for future worlds, especially for constructs such as casing whether there can be progress in the world after stepping into one of the branches. We are interested in investigating this choice of moving the quantification outside of the logical relation, and whether there is any other work that had encountered that issue before.

5.2 Future Work

For future work, we are interested in possibly introducing a modality to the language and seeing how that affects the definition of the logical relation. There are many avenues for a modality — one is to introduce a modal separation between pure expressions and effects, which may help with decluttering the proof and not needing to constantly address the signature and memory. There is also an avenue for employing a type level separation using call-by-push-value [9], which has a separation between positive and negative types. Since we already observed such a distinction in polarity in this system, it may be natural to switch to that paradigm. Additionally, since we already have a degenerate form of effects in the language, we are interested in extending that to higher-order store and investigating the possible interactions between that and encryption. Otherwise, we are interested in consolidating some parts of the logical relation, particularly in seeing whether the logical relation for leaf-determinism can somehow be folded into the main logical relation, or otherwise if there is a clearer way to justify that the resultant sets are well-formed by definition of the dynamics.

Appendix A

Appendix

A.1 Proof of Leaf-Determinism FTLR

A.1.1 Proofs of Lemmas

Lemma 32 (LD-Antimonotonicity). *If $\mathbb{V} \in \mathcal{LV}_\Sigma[\tau]$ and $\Sigma' \leq \Sigma$, then $\mathbb{V} \in \mathcal{LV}_{\Sigma'}[\tau]$.*

Proof. (Outline) Proceed by induction on the type and analyze each case of the logical relation. Should proceed as the other anti-monotonicity proofs. \square

Lemma 33. *If $\sigma :_{\text{LD}} \Gamma; \Sigma$ and $\Sigma' \leq \Sigma$, then $\sigma :_{\text{LD}} \Gamma; \Sigma'$.*

Proof. (Outline) We can use Lemma 2 to claim that all $\sigma(x) \in \mathcal{LV}_{\Sigma'}[\tau]$, which gives us that $\sigma :_{\text{LD}} \Gamma; \Sigma'$. \square

Lemma 34. *If $\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\}$, then $|\mathbb{V}| > 0$.*

Proof. (Outline) Proceed by induction on the stepping judgment, in all cases the stepping should produce non-empty sets. \square

Lemma 35. *If $\mathbb{V} \in \mathcal{LV}_\Sigma[\tau]$, then $|\mathbb{V}| \geq 1$.*

Proof. (Outline) Proceed by induction on the type, this should go similarly to the above proof where at all steps, the logical relation enforces that the set is non-empty. \square

Lemma 36. *If $\mathbb{V} \in \mathcal{LV}_\Sigma[\tau]$ and $\mathbb{V}' \subseteq \mathbb{V}$ with $|\mathbb{V}'| \geq 1$, then $\mathbb{V}' \in \mathcal{LV}_\Sigma[\tau]$.*

Proof. We proceed by induction on the type τ :

- $\tau = \text{unit}$

In this case, we have that $\mathbb{V} = \{\langle \rangle\}$, as well as $\mathbb{V}' \subseteq \mathbb{V}$ with $|\mathbb{V}'| \geq 1$. The only such subset which satisfies the non-empty condition is $\{\langle \rangle\}$, and that is definitionally in $\mathcal{LV}_\Sigma[\text{unit}]$.

- $\tau = \text{key}_\ell$

In this case, we have that $\mathbb{V} = \{\text{key}\langle K \rangle\}$ for $K \sim \ell \in \Sigma$. Suppose we have $\mathbb{V}' \subseteq \mathbb{V}$ such that $|\mathbb{V}'| \geq 1$. The only such subset which satisfies the non-empty condition is $\{\text{key}\langle K \rangle\}$, which is definitionally in $\mathcal{LV}_\Sigma[\text{key}_\ell]$.

- $\tau = (\tau' \text{ result})_\ell$

In this case, we have that either $\mathbb{V} = \{\text{Error}\}$ or $\mathbb{V} = \{\text{Ok}(v) \mid v \in \mathbb{V}_1\}$ for $\mathbb{V}_1 \in \mathcal{LV}_\Sigma[[\tau']]$.

Suppose we have $\mathbb{V}' \subseteq \mathbb{V}$ with $|\mathbb{V}'| \geq 1$. In the former case, the only non-empty subset of $\{\text{Error}\}$ is $\{\text{Error}\}$, which is definitionally in $\mathcal{LV}_\Sigma[[\tau' \text{ result}]_\ell]$. In the latter case, by the definition of subset, we have that $\mathbb{V}' = \{\text{Ok}(v) \mid v \in \mathbb{V}'_1\}$, where $\mathbb{V}'_1 \subseteq \mathbb{V}_1$. Since $|\mathbb{V}'| \geq 1$, it must be the case that $|\mathbb{V}'_1| \geq 1$, otherwise the set would be empty.

Then, by the **IH**, we have that $\mathbb{V}' \in \mathcal{LV}_\Sigma[[\tau' \text{ result}]_\ell]$.

- $\tau = \tau_1 \times \tau_2$

In this case, we have $\mathbb{V} = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\}$ with $\mathbb{V}_1 \in \mathcal{LV}_\Sigma[[\tau_1]]$ and $\mathbb{V}_2 \in \mathcal{LV}_\Sigma[[\tau_2]]$.

Suppose we have \mathbb{V}' such that $\mathbb{V}' \subseteq \mathbb{V}$ and $|\mathbb{V}'| \geq 1$. This means, by definition of subset, that $\mathbb{V}' = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}'_1, v_2 \in \mathbb{V}'_2\}$, where $\mathbb{V}'_1 \subseteq \mathbb{V}_1$ and $\mathbb{V}'_2 \subseteq \mathbb{V}_2$. Observe also that since $|\mathbb{V}'| \geq 1$, we must have that $|\mathbb{V}'_1| \geq 1$ and $|\mathbb{V}'_2| \geq 1$, otherwise we would contradict the fact that $|\mathbb{V}'| \geq 1$.

Then, by the **IH**, we have that $\mathbb{V}'_1 \in \mathcal{LV}_\Sigma[[\tau_1]]$ and $\mathbb{V}'_2 \in \mathcal{LV}_\Sigma[[\tau_2]]$. Then, by the definition of leaf-determinism, we have that $\mathbb{V}' \in \mathcal{LV}_\Sigma[[\tau_1 \times \tau_2]]$.

- $\tau = (\tau_1 + \tau_2)_\ell$

In this case, we have $\mathbb{V} = \{i \cdot v_i \mid v_i \in \mathbb{V}_i\}$ for $\mathbb{V}_i \in \mathcal{LV}_\Sigma[[\tau_i]]$. Suppose we have $\mathbb{V}' \subseteq \mathbb{V}$ with $|\mathbb{V}'| \geq 1$. This means, by definition of subset, that $\mathbb{V}' = \{i \cdot v_i \mid v_i \in \mathbb{V}'_i\}$ where $\mathbb{V}'_i \subseteq \mathbb{V}_i$. Observe that $|\mathbb{V}'_i| \geq 1$ since $|\mathbb{V}_i| \geq 1$.

Then, by the **IH**, we have that $\mathbb{V}'_i \in \mathcal{LV}_\Sigma[[\tau_i]]$, which then gives us that $\mathbb{V}' \in \mathcal{LV}_\Sigma[[\tau_1 + \tau_2]_\ell]$ by definition.

- $\tau = \tau_1 \xrightarrow{\ell_k} \tau_2$

In this case, we have $\forall v \in \mathbb{V}. v =_\alpha \lambda(x.e)$ such that $\forall \Sigma'$ such that $\Sigma' \leq \Sigma$ and $\forall \mathbb{V}_1 \in \mathcal{LV}_{\Sigma'}[[\tau_1]]$, $\{[v_1/x]e \mid v_1 \in \mathbb{V}_1\} \in \mathcal{LV}_{\Sigma'}[[\tau_2]]$.

Suppose we have a $\mathbb{V}' \subseteq \mathbb{V}$ with $|\mathbb{V}'| \geq 1$. By the definition of subset, we have that $\forall v \in \mathbb{V}'. v =_\alpha \lambda(x.e)$ such that $\forall \Sigma'$ such that $\Sigma' \leq \Sigma$ and $\forall \mathbb{V}_1 \in \mathcal{LV}_{\Sigma'}[[\tau_1]]$, $\{[v_1/x]e \mid v_1 \in \mathbb{V}_1\} \in \mathcal{LV}_{\Sigma'}[[\tau_2]]$. That is, the elements of \mathbb{V}' are simply a smaller set of the elements of \mathbb{V} , which continue to satisfy the same conditions that they had in \mathbb{V} . This gives us, definitionally, that $\mathbb{V}' \in \mathcal{LV}_\Sigma[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$.

- $\tau = (\text{enc}_\ell \tau')_\epsilon$

In this case, we have that $\mathbb{V} = \{u \mid v \in \mathbb{V}_1, u \in \mathcal{E}_\ell(v_k, v)\}$ with $\mathbb{V}_1 \in \mathcal{LV}_\Sigma[[\tau']]$. Suppose we have $\mathbb{V}' \subseteq \mathbb{V}$ with $|\mathbb{V}'| \geq 1$. This means, by definition of subset, that $\mathbb{V}' = \{u \mid v \in \mathbb{V}'_1, u \in \mathcal{E}_\ell(v_k, v)\}$, where $\mathbb{V}'_1 \subseteq \mathbb{V}_1$. Observe that since $|\mathbb{V}_1| \geq 1$, then $|\mathbb{V}'_1| \geq 1$ as well.

Then, by the **IH**, we have that $\mathbb{V}'_1 \in \mathcal{LV}_\Sigma[[\tau']]$, which gives us what we need to show $\mathbb{V}' \in \mathcal{LV}_\Sigma[[\text{enc}_\ell \tau']_\epsilon]$

□

Lemma 37 (LD-Subtype). *If $\tau' \leq \tau$ and $\mathbb{V} \in \mathcal{LV}_\Sigma[[\tau']]$, then $\mathbb{V} \in \mathcal{LV}_\Sigma[[\tau]]$.*

Proof. Suppose we have $\tau' \leq \tau$ and $\mathbb{V} \in \mathcal{LV}_\Sigma[[\tau']]$. We proceed by rule induction on $\tau' \leq \tau$:

- **Case:** $\frac{\tau'_1 \leq \tau_1 \quad \tau'_2 \leq \tau_2 \quad \ell_1 \sqsubseteq \ell_2}{(\tau'_1 + \tau'_2)_{\ell_1} \leq (\tau_1 + \tau_2)_{\ell_2}}$

In this case, we have that $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[(\tau'_1 + \tau'_2)_{\ell_1}]$. By the definition of leaf-determinism, this means that either

$$\mathbb{V} = \{1 \cdot v_1 \mid v_1 \in \mathbb{V}_1\} \text{ with } \mathbb{V}_1 \in \mathcal{L}\mathcal{V}_\Sigma[\tau'_1]$$

or

$$\mathbb{V} = \{2 \cdot v_2 \mid v_2 \in \mathbb{V}_2\} \text{ with } \mathbb{V}_2 \in \mathcal{L}\mathcal{V}_\Sigma[\tau'_2]$$

WLOG, suppose we are in the first case. By the **IH**, since $\tau'_1 \leq \tau_1$, we have that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_\Sigma[\tau_1]$, which gives us that $\{1 \cdot v_1 \mid v_1 \in \mathbb{V}_1\} \in \mathcal{L}\mathcal{V}_\Sigma[(\tau_1 + \tau_2)_\ell]$.

- **Case:** $\frac{\tau'_1 \leq \tau_1 \quad \tau'_2 \leq \tau_2}{\tau'_1 \times \tau'_2 \leq \tau_1 \times \tau_2}$

In this case, we have that $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau'_1 \times \tau'_2]$. By the definition of leaf-determinism, this means that

$$\mathbb{V} = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\} \text{ with } \mathbb{V}_1 \in \mathcal{L}\mathcal{V}_\Sigma[\tau'_1] \text{ and } \mathbb{V}_2 \in \mathcal{L}\mathcal{V}_\Sigma[\tau'_2]$$

By the **IH**, since $\tau'_1 \leq \tau_1$ and $\tau'_2 \leq \tau_2$, we have that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_\Sigma[\tau_1]$ and $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_\Sigma[\tau_2]$, which gives us that $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau_1 \times \tau_2]$.

- **Case:** $\frac{\tau_1 \leq \tau'_1 \quad \tau'_2 \leq \tau_2 \quad \ell_k \sqsubseteq \ell'_k}{\tau'_1 \xrightarrow{\ell'_k} \tau'_2 \leq \tau_1 \xrightarrow{\ell_k} \tau_2}$

In this case, we have that $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau'_1 \xrightarrow{\ell'_k} \tau'_2]$. By the definition of the value interpretation, this means that $\forall v \in \mathbb{V}, v = \lambda(x : \tau'_1.e)$ such that for all Σ' such that $\Sigma' \leq \Sigma$ and for all $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau'_1]$, we have that $\{[v_1/x]e \mid v_1 \in \mathbb{V}_1\} \in \mathcal{L}_{\Sigma'}[\tau'_2]$.

We would like to show that $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau_1 \xrightarrow{\ell_k} \tau_2]$. We already have that $v =_\alpha \lambda(x.e)$.

Suppose that we have some $\Sigma' \leq \Sigma$ and $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_1]$. By the **IH**, since $\tau_1 \leq \tau'_1$, we have that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau'_1]$. From the previous reasoning, this means we can obtain that $\{[v_1/x]e \mid v_1 \in \mathbb{V}_1\} \in \mathcal{L}_{\Sigma'}[\tau'_2]$.

Define $\mathbb{E} = \{[v_1/x]e \mid v_1 \in \mathbb{V}_1\}$. Unfolding the definition of leaf-determinism, we have

- Since $\mathbb{E} \in \mathcal{L}_{\Sigma'}[\tau'_2]$, we have that exists Σ^* such that $\Sigma^* \leq \Sigma'$. Then, we have

$$\forall e' \in \mathbb{E}. \nu\Sigma\{e' \parallel \mu\} \Downarrow \nu\Sigma^*\{\mathbb{V}^{e'} \parallel \mu^*\}$$

such that $\mu^* : \Sigma^*$ and $\bigcup_{e' \in \mathbb{E}} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma^*}[\tau'_2]$.

By the **IH**, we have that each $\bigcup_{e' \in \mathbb{E}} \mathbb{V}^{e'}$ is in $\mathcal{L}\mathcal{V}_{\Sigma^*}[\tau_2]$.

With this, we have what we need to show for the term interpretation $\{[v_1/x]e \mid v_1 \in \mathbb{V}_1\} \in \mathcal{L}_{\Sigma'}[\tau_2]$.

- **Case:** $\frac{\tau_1 \leq \tau_2 \quad \epsilon_1 \sqsubseteq \epsilon_2}{(\text{enc}_\ell \tau_1)_{\epsilon_1} \leq (\text{enc}_\ell \tau_2)_{\epsilon_2}}$

In this case, we have that $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[(\text{enc}_\ell \tau_1)_{\epsilon_1}]$. By the definition of leaf-determinism, this means we have $\mathbb{V} = \{u \mid u \in \mathcal{E}_\ell(v_k, v), v \in \mathbb{V}\}$ for $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau_1]$.

By the **IH**, we have that $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[\tau_2]$, and with the existing v_k , we have what we want to show for $\mathbb{V} \in \mathcal{L}\mathcal{V}_\Sigma[(\text{enc}_\ell \tau_2)_{\epsilon_2}]$.

- **Omitted:** unit, key

□

Lemma 38. For all σ such that $\sigma :_{\text{LD}} \Gamma; \Sigma$ and $\forall \gamma \in \text{sing}(\sigma). \gamma : \Gamma; \Sigma$, then $\text{set}(\gamma) :_{\text{LD}} \Gamma; \Sigma$.

Proof. Suppose we have σ with the above properties. By definition, this means that for all $x : \tau \in \Gamma$, $\sigma(x) \in \mathcal{LV}_{\Sigma}[\tau]$. This means that each non-empty subset of $\sigma(x)$ is leaf-deterministic (Lemma 6). Since each $\gamma \in \text{sing}(\sigma)$ is defined to map variables x to a single element in $\sigma(x)$, we get that $\text{set}(\gamma)$ map variables x to singleton subsets of $\sigma(x)$, which are leaf-deterministic by the above lemma. Thus, we have $\text{set}(\gamma) :_{\text{LD}} \Gamma; \Sigma$. □

Lemma 39. For all σ_1, σ_2 such that $\sigma_1 :_{\text{LD}} \Gamma; \Sigma_1$, $\sigma_2 :_{\text{LD}} \Gamma; \Sigma_2$, and $\forall (\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2). \gamma_1 \equiv_{\xi} \gamma_2 : \Gamma; (\Sigma_1 \uplus \Sigma_2)$, $\text{set}(\gamma_1) :_{\text{LD}} \Gamma; \Sigma_1$ and $\text{set}(\gamma_2) :_{\text{LD}} \Gamma; \Sigma_2$.

Proof. Suppose we have σ_1 and σ_2 with the above properties. Then we have that $\forall x : \tau \in \Gamma. \sigma_1(x) \in \mathcal{LV}_{\Sigma_1}[\tau]$ and $\forall x : \tau \in \Gamma. \sigma_2(x) \in \mathcal{LV}_{\Sigma_2}[\tau]$. This means that each non-empty subset of $\sigma_1(x)$ and $\sigma_2(x)$ are leaf-deterministic (Lemma 6). Since each $(\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2)$ is defined to map variables x to a single element in $\sigma_1(x)$ and $\sigma_2(x)$ (respectively), we get that $\text{set}(\gamma_1)$ and $\text{set}(\gamma_2)$ map variables x to singleton subsets of $\sigma_1(x)$ and $\sigma_2(x)$, which are leaf-deterministic by the above lemma. Thus, we have $\text{set}(\gamma_1) :_{\text{LD}} \Gamma; \Sigma_1$ and $\text{set}(\gamma_2) :_{\text{LD}} \Gamma; \Sigma_2$. □

Lemma 40. For all expressions e and maps γ , $\widehat{\text{set}(\gamma)}(e) = \{\hat{\gamma}(e)\}$.

Proof. We proceed by induction on the structure of e :

- **Case:** $e = x$

We proceed by casing on whether $x \in \text{dom}(\gamma)$:

- $x \in \text{dom}(\gamma)$:

By definition of $\widehat{\text{set}(\gamma)}$, we have $\widehat{\text{set}(\gamma)}(x) = \{\gamma(x)\}$, and by definition of $\hat{\gamma}$, we have $\hat{\gamma}(x) = \gamma(x)$, giving us that $\widehat{\text{set}(\gamma)}(x) = \{\hat{\gamma}(x)\}$.

- $x \notin \text{dom}(\gamma)$:

By definition of $\widehat{\text{set}(\gamma)}$, we have $\widehat{\text{set}(\gamma)}(x) = \{x\}$, and by definition of $\hat{\gamma}$, we have $\hat{\gamma}(x) = x$, meaning $\widehat{\text{set}(\gamma)}(x) = \{\hat{\gamma}(x)\}$.

- **Case:** $e = \langle \rangle$

By definition of $\widehat{\text{set}(\gamma)}$, we have $\widehat{\text{set}(\gamma)}(\langle \rangle) = \{\langle \rangle\}$.

Also, by definition of $\hat{\gamma}$, we have that $\hat{\gamma}(\langle \rangle) = \langle \rangle$, which gives us what we want to show.

- **Case:** $e = \langle e_1, e_2 \rangle$

By the definition of $\widehat{\text{set}(\gamma)}$, we have that $\widehat{\text{set}(\gamma)}\langle e_1, e_2 \rangle = \{\langle e'_1, e'_2 \rangle \mid e'_1 \in \widehat{\text{set}(\gamma)}(e_1), e'_2 \in \widehat{\text{set}(\gamma)}(e_2)\}$.

By the **IH**, we have that $\widehat{\text{set}(\gamma)}(e_1) = \{\hat{\gamma}(e_1)\}$ and $\widehat{\text{set}(\gamma)}(e_2) = \{\hat{\gamma}(e_2)\}$.

By definition of $\hat{\gamma}$, we have that $\hat{\gamma}\langle e_1, e_2 \rangle = \langle \hat{\gamma}(e_1), \hat{\gamma}(e_2) \rangle$. Thus, for $\widehat{\text{set}(\gamma)}\langle e_1, e_2 \rangle$, we get that $\{\langle e'_1, e'_2 \rangle \mid e'_1 \in \hat{\gamma}(e_1), e'_2 \in \hat{\gamma}(e_2)\} = \{\langle e'_1, e'_2 \rangle\} = \{\langle e'_1, e'_2 \rangle \mid e'_1 \in \{\hat{\gamma}(e_1)\}, e'_2 \in \{\hat{\gamma}(e_2)\}\} = \{\langle \hat{\gamma}(e_1), \hat{\gamma}(e_2) \rangle\}$.

- **Case:** $e = e \cdot i$
 By the definition of $\widehat{\text{set}}(\gamma)$, we have that $\widehat{\text{set}}(\gamma)(e \cdot i) = \{e' \cdot i \mid e' \in \widehat{\text{set}}(\gamma)(e)\}$.
 By the **IH**, we have that $\widehat{\text{set}}(\gamma)(e) = \{\hat{\gamma}(e)\}$. By the definition of $\hat{\gamma}$, we have that $\hat{\gamma}(e \cdot i) = \hat{\gamma}(e) \cdot i$.
 Thus, we have that $\{e' \cdot i \mid e' \in \widehat{\text{set}}(\gamma)(e)\} = \{e' \cdot i \mid e' \in \{\hat{\gamma}(e)\}\} = \{\hat{\gamma}(e) \cdot i\}$.
- **Case:** $e = \text{case } e \{x_1.e_1 \mid x_2.e_2\}$
 By the definition of $\widehat{\text{set}}(\gamma)$, we have that $\widehat{\text{set}}(\gamma)(\text{case } e \{x_1.e_1 \mid x_2.e_2\}) = \{\text{case } e' \{x_1.e'_1 \mid x_2.e'_2\} \mid e' \in \widehat{\text{set}}(\gamma)(e), e'_1 \in \widehat{\text{set}}(\gamma)(e_1), e'_2 \in \widehat{\text{set}}(\gamma)(e_2)\}$ up to alpha equivalence on x_1 and x_2 .
 By the **IH**, we have that
 - $\widehat{\text{set}}(\gamma)(e) = \{\hat{\gamma}(e)\}$,
 - $\widehat{\text{set}}(\gamma)(e_1) = \{\hat{\gamma}(e_1)\}$
 - $\widehat{\text{set}}(\gamma)(e_2) = \{\hat{\gamma}(e_2)\}$
 By the definition of $\hat{\gamma}$, we have that $\hat{\gamma}(\text{case } e \{x_1.e_1 \mid x_2.e_2\}) = \text{case } \hat{\gamma}(e) \{x_1.\hat{\gamma}(e_1) \mid x_2.\hat{\gamma}(e_2)\}$ up to alpha equivalence on x_1 and x_2 .
 Thus, we have that $\widehat{\text{set}}(\gamma)(\text{case } e \{x_1.e_1 \mid x_2.e_2\}) = \{\text{case } e' \{x_1.e'_1 \mid x_2.e'_2\} \mid e' \in \widehat{\text{set}}(\gamma)(e), e'_1 \in \widehat{\text{set}}(\gamma)(e_1), e'_2 \in \widehat{\text{set}}(\gamma)(e_2)\} = \{\text{case } e' \{x_1.e'_1 \mid x_2.e'_2\} \mid e' \in \{\hat{\gamma}(e)\}, e'_1 \in \{\hat{\gamma}(e_1)\}, e'_2 \in \{\hat{\gamma}(e_2)\}\} = \{\text{case } \hat{\gamma}(e) \{x_1.\hat{\gamma}(e_1) \mid x_2.\hat{\gamma}(e_2)\}\}$.
- All other cases unfold similarly to the above.

□

A.1.2 FTLR

Suppose we have $\Sigma; \sigma \vdash_{\text{kc}} e : \tau$, Σ' such that $\Sigma' \leq \Sigma$, and $\sigma \text{ :LD } \Gamma; \Sigma'$. We proceed by rule induction on the typing judgment:

- **Case:** T-UNIT
WTS: $\hat{\sigma}(\langle \rangle) \in \mathcal{L}_{\Sigma'}[\text{unit}]$

By the definition of substitution, we have that $\hat{\sigma}(\langle \rangle) = \{\langle \rangle\}$. By the set-lifted dynamics, we have

$$\overline{\nu\Sigma' \{\langle \rangle \parallel \mu\} \Downarrow \nu\Sigma' \{\{\langle \rangle\} \parallel \mu\}}$$

Note that $\bigcup_{e \in \{\langle \rangle\}} \{\langle \rangle\} = \{\langle \rangle\}$ by the definition of set union. Therefore, since $\{\langle \rangle\} \in \mathcal{L}_{\Sigma'}[\text{unit}]$, we have that $\hat{\sigma}(\langle \rangle) \in \mathcal{L}_{\Sigma'}[\text{unit}]$.

- **Case:** T-PROD
WTS: $\hat{\sigma}\langle e_1, e_2 \rangle \in \mathcal{L}_{\Sigma'}[\tau_1 \times \tau_2]$

By the definition of substitution, we have that $\hat{\sigma}\langle e_1, e_2 \rangle = \{\langle e'_1, e'_2 \rangle \mid e'_1 \in \hat{\sigma}(e_1), e'_2 \in \hat{\sigma}(e_2)\}$.

By the **IH**, we have that $\hat{\sigma}(e_1) \in \mathcal{L}_{\Sigma'}[\tau_1]$ and $\hat{\sigma}(e_2) \in \mathcal{L}_{\Sigma'}[\tau_2]$. Suppose we have $\mu : \Sigma'$. Unfolding the term interpretation, this means we have

- Since $\hat{\sigma}(e_1) \in \mathcal{L}_{\Sigma'}[\tau_1]$, then

$$\forall e'_1 \in \hat{\sigma}(e_1). \nu\Sigma'\{e'_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1^{e'_1} \parallel \mu_1\}$$

with $\mu_1 : \Sigma_1$ and $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\tau_1]$.

- Since $\hat{\sigma}(e_2) \in \mathcal{L}_{\Sigma'}[\tau_2]$, then

$$\forall e'_2 \in \hat{\sigma}(e_2). \nu\Sigma'\{e'_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2^{e'_2} \parallel \mu_2\}$$

with $\mu_2 : \Sigma_2$ and $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2}[\tau_2]$.

Note that since $\hat{\sigma}\langle e_1, e_2 \rangle = \{\langle e'_1, e'_2 \rangle \mid e'_1 \in \hat{\sigma}(e_1), e'_2 \in \hat{\sigma}(e_2)\}$, we have that each element e'_1 and e'_2 have a stepping to a set of leaf-deterministic values $\mathbb{V}_1^{e'_1}$ and $\mathbb{V}_2^{e'_2}$, respectively. Then, by the set-lifted dynamics, for each $\langle e'_1, e'_2 \rangle \in \hat{\sigma}\langle e_1, e_2 \rangle$, we have

$$\frac{\nu\Sigma'\{e'_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1^{e'_1} \parallel \mu_1\} \quad \nu\Sigma'\{e'_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2^{e'_2} \parallel \mu_2\}}{\nu\Sigma'\{\langle e'_1, e'_2 \rangle \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1^{e'_1}, v_2 \in \mathbb{V}_2^{e'_2}\} \parallel \mu_1 \cup \mu_2\}}$$

We now need to show $\bigcup_{\langle e'_1, e'_2 \rangle \in \hat{\sigma}\langle e_1, e_2 \rangle} \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1^{e'_1}, v_2 \in \mathbb{V}_2^{e'_2}\} \in \mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau_1 \times \tau_2]$. First, observe that

$$\bigcup_{\langle e'_1, e'_2 \rangle \in \hat{\sigma}\langle e_1, e_2 \rangle} \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1^{e'_1}, v_2 \in \mathbb{V}_2^{e'_2}\} = \{\langle v_1, v_2 \rangle \mid v_1 \in \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1}, v_2 \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2}\}$$

by the definition of $\hat{\sigma}\langle e_1, e_2 \rangle$ and set union.

From the **IH**, we have $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\tau_1]$ and $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2}[\tau_2]$. By Lemma 2, we have that $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau_1]$ and $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau_2]$. Then, by definition of the leaf-determinism value interpretation, we have that the set is in $\mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau_1 \times \tau_2]$.

• **Case: T-PROJ-1**

WTS: $\hat{\sigma}(e \cdot i) \in \mathcal{L}_{\Sigma'}[\tau_i]$ for $i \in \{1, 2\}$

By the definition of substitution, we have that $\hat{\sigma}(e \cdot i) = \{e' \cdot i \mid e' \in \hat{\sigma}(e)\}$.

By the **IH**, we have that $\hat{\sigma}(e) \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_1 \times \tau_2]$. Suppose $\mu : \Sigma'$. By definition of leaf-determinism, we have that

- Since $\hat{\sigma}(e) \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_1 \times \tau_2]$, then

$$\forall e' \in \hat{\sigma}(e). \nu\Sigma'\{e' \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}^{e'} \parallel \mu'\}$$

with $\mu' : \Sigma''$ and $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau_1 \times \tau_2]$.

From the IH, we have that $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_1 \times \tau_2]$. By definition, this means that we have that $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\}$ with $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_1]$ and $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau_2]$. Since the union of these sets are in the value interpretation, and the subsets are the result of evaluations, we have that each individual set $\mathbb{V}^{e'}$ is in the value interpretation (Lemmas 4 and 6), meaning

$$\mathbb{V}^{e'} = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1^{e'}, v_2 \in \mathbb{V}_2^{e'}\}$$

where $\mathbb{V}_1^{e'}$ and $\mathbb{V}_2^{e'}$ are the subsets of \mathbb{V}_1 and \mathbb{V}_2 relevant to e' .

By the set-lifted dynamics rules, for each $e' \cdot i \in \hat{\sigma}(e \cdot i)$, we have

$$\frac{\nu\Sigma'\{e' \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}^{e'} \parallel \mu'\}}{\nu\Sigma'\{e' \cdot i \parallel \mu\} \Downarrow \nu\Sigma''\{\{v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}^{e'}\} \parallel \mu'\}} \quad (i \in \{1, 2\})$$

Note that the set $\bigcup_{e' \cdot i \in \hat{\sigma}(e \cdot i)} \{v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}^{e'}\} = \{v_i \mid \langle v_1, v_2 \rangle \in \bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'}\}$, which is exactly the set \mathbb{V}_i from the IH, meaning we immediately have that $\{v_i \mid \langle v_1, v_2 \rangle \in \bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'}\} \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_i]$, as required.

- **Case: T-INJ-1**

WTS: $\hat{\sigma}(i \cdot e) \in \mathcal{L}_{\Sigma'}[\tau_1 + \tau_2]_\ell$ for $i \in \{1, 2\}$

By the definition of substitution, we have that $\hat{\sigma}(i \cdot e) = \{i \cdot \hat{\sigma}(e') \mid e' \in \hat{\sigma}(e)\}$.

By the **IH**, we have that $\hat{\sigma}(e) \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_i]$. By definition of leaf-determinism, we have that

- Since $\hat{\sigma}(e) \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_i]$, then

$$\forall e' \in \hat{\sigma}(e). \nu\Sigma'\{e' \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}^{e'} \parallel \mu'\}$$

such that $\mu' : \Sigma''$ and $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau_i]$.

By the set-lifted dynamics rules, for each $i \cdot e' \in \hat{\sigma}(i \cdot e)$, we have

$$\frac{\nu\Sigma'\{e' \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}^{e'} \parallel \mu'\}}{\nu\Sigma'\{i \cdot e' \parallel \mu\} \Downarrow \nu\Sigma''\{\{i \cdot v \mid v \in \mathbb{V}^{e'}\} \parallel \mu'\}} \quad (i \in \{1, 2\})$$

We would like to show that $\bigcup_{i \cdot e' \in \hat{\sigma}(i \cdot e)} \{i \cdot v \mid v \in \mathbb{V}^{e'}\} \in \mathcal{L}\mathcal{V}_{\Sigma''}[(\tau_1 + \tau_2)_\ell]$. By definition of set union and $\hat{\sigma}$, we have that $\bigcup_{i \cdot e' \in \hat{\sigma}(i \cdot e)} \{i \cdot v \mid v \in \mathbb{V}^{e'}\} = \{i \cdot v \mid v \in \bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'}\}$. We then get that the set is in $\mathcal{L}\mathcal{V}_{\Sigma''}[(\tau_1 + \tau_2)_\ell]$ from the fact that each element in the set is the same injection and that $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau_i]$ from the IH.

- **Case: T-CASE**

T-CASE

$$\frac{\Sigma; \Gamma \vdash_{\text{kc}} e : (\tau_1 + \tau_2)_\ell \quad \Sigma; \Gamma, x_1 : \tau_1 \vdash_{\text{kc} \sqcup \ell} e_1 : \tau \quad \Sigma; \Gamma, x_2 : \tau_2 \vdash_{\text{kc} \sqcup \ell} e_2 : \tau \quad \ell \triangleleft \tau}{\Sigma; \Gamma \vdash_{\text{kc}} \text{case } e \{ x_1.e_1 \mid x_2.e_2 \} : \tau}$$

WTS: $\hat{\sigma}(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}) \in \mathcal{L}_{\Sigma'}[\tau]$

By definition of substitution (upto alpha-equivalence on x_1 and x_2), we have $\hat{\sigma}(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}) = \{\text{case } e' \{ x_1.e'_1 \mid x_2.e'_2 \} \mid e' \in \hat{\sigma}(e), e'_1 \in \hat{\sigma}(e_1), e'_2 \in \hat{\sigma}(e_2)\}$.

By **IH**, we have

- $\hat{\sigma}(e) \in \mathcal{L}_{\Sigma'}[\tau]$
- $\forall \Sigma_1 \text{ s.t. } \Sigma_1 \leq \Sigma, \forall \sigma_1 : \Gamma, x_1 : \tau_1; \Sigma_1, \hat{\sigma}_1(e_1) \in \mathcal{L}_{\Sigma_1}[\tau]$
- $\forall \Sigma_2 \text{ s.t. } \Sigma_2 \leq \Sigma, \forall \sigma_2 : \Gamma, x_2 : \tau_2; \Sigma_2, \hat{\sigma}_2(e_2) \in \mathcal{L}_{\Sigma_2}[\tau]$

Suppose we have $\mu : \Sigma$. Unfolding the definitions, we have

- Since $\hat{\sigma}(e) \in \mathcal{L}_{\Sigma'}[\tau]$,

$$\forall e' \in \hat{\sigma}(e). \nu \Sigma' \{e' \parallel \mu\} \Downarrow \nu \Sigma'' \{\mathbb{V}^{e'} \parallel \mu'\}$$

such that $\mu' : \Sigma''$ and $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}_{\Sigma''}[\tau]$.

- Since $\hat{\sigma}_1(e_1) \in \mathcal{L}_{\Sigma_1}[\tau]$, if $\mu_1 : \Sigma_1$, then

$$\forall e'_1 \in \hat{\sigma}_1(e_1). \nu \Sigma_1 \{e'_1 \parallel \mu_1\} \Downarrow \nu \Sigma'_1 \{\mathbb{V}_1^{e'_1} \parallel \mu'_1\}$$

such that $\mu'_1 : \Sigma'_1$ and $\bigcup_{e'_1 \in \hat{\sigma}_1(e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}_{\Sigma'_1}[\tau]$.

- Since $\hat{\sigma}_2(e_2) \in \mathcal{L}_{\Sigma_2}[\tau]$, if $\mu_2 : \Sigma_2$, then

$$\forall e'_2 \in \hat{\sigma}_2(e_2). \nu \Sigma_2 \{e'_2 \parallel \mu_2\} \Downarrow \nu \Sigma'_2 \{\mathbb{V}_2^{e'_2} \parallel \mu'_2\}$$

such that $\mu'_2 : \Sigma'_2$ and $\bigcup_{e'_2 \in \hat{\sigma}_2(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}_{\Sigma'_2}[\tau]$.

Since $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}_{\Sigma''}[\tau]$, we have that either $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} = \{1 \cdot v_1 \mid v_1 \in \mathbb{V}_1\}$ with $\mathbb{V}_1 \in \mathcal{L}_{\Sigma''}[\tau]$ or $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} = \{2 \cdot v_2 \mid v_2 \in \mathbb{V}_2\}$ with $\mathbb{V}_2 \in \mathcal{L}_{\Sigma''}[\tau]$. We case on these possibilities:

- **Case:** $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} = \{1 \cdot v_1 \mid v_1 \in \mathbb{V}_1\}$ with $\mathbb{V}_1 \in \mathcal{L}_{\Sigma''}[\tau]$

Since $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}_{\Sigma''}[\tau]$, we have that each $\mathbb{V}^{e'} \in \mathcal{L}_{\Sigma''}[\tau]$, and in particular that each $\mathbb{V}^{e'} = \{1 \cdot v_1 \mid v_1 \in \mathbb{V}_1^{e'}\}$, where $\mathbb{V}_1^{e'}$ is the subset of \mathbb{V}_1 relevant to e' . Note also that $\mathbb{V}_1^{e'} \in \mathcal{L}_{\Sigma''}[\tau]$ for each e' (Lemmas 4 and 6).

Observe that $\sigma[x_1 \mapsto \mathbb{V}_1] :_{\text{LD}} \Gamma, x_1 : \tau_1; \Sigma''$ since $\mathbb{V}_1 \in \mathcal{L}_{\Sigma''}[\tau]$, and similarly that $\sigma[x_1 \mapsto \mathbb{V}_1^{e'}] :_{\text{LD}} \Gamma, x_1 : \tau_1; \Sigma''$ for each e' (the existing maps can be extended to Σ'' by Lemma 3).

Given this, by the **IH**, we have that $\forall e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1}](e_1). \nu \Sigma'' \{e'_1 \parallel \mu'\} \Downarrow \nu \Sigma'_1 \{\mathbb{V}_1^{e'_1} \parallel \mu'_1\}$

such that $\bigcup_{e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1}](e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}_{\Sigma'_1}[\tau]$, and similarly that $\forall e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1^{e'}}](e_1). \nu \Sigma'' \{e'_1 \parallel \mu'\} \Downarrow \nu \Sigma'_1 \{\mathbb{V}_1^{e', e'_1} \parallel \mu'_1\}$ such that $\bigcup_{e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1^{e'}}](e_1)} \mathbb{V}_1^{e', e'_1} \in \mathcal{L}_{\Sigma'_1}[\tau]$.

Note that $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}_1^{e', e'_1} = \mathbb{V}_1^{e'_1}$ by definition of the sets/set union, and that since $\bigcup_{e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1}](e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau]$, we have that each set $\mathbb{V}_1^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau]$ (Lemmas 4 and 6).

Note that $\sigma[\widehat{x_1 \mapsto \mathbb{V}_1^{e'_1}}](e_1) = \{[v_1^{e'}/x_1]e''_1 \mid e''_1 \in \hat{\sigma}(e_1), v_1^{e'} \in \mathbb{V}_1^{e'_1}\}$.

Then, according to the set-lifted dynamics, we have the following for each case $e' \{x_1.e'_1 \mid x_2.e'_2\} \in \hat{\sigma}(\text{case } e \{x_1.e_1 \mid x_2.e_2\})$:

$$\frac{\nu\Sigma'\{e' \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}^{e'} \parallel \mu'\} \quad (\nu\Sigma''\{e'_1 \parallel \mu'\} \Downarrow \nu\Sigma'_1\{\mathbb{V}_{1,v_1^{e'_1}}^{e', e'_1} \parallel \mu'_1\})_{e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}^{e'}}](e_1)}}{\nu\Sigma'\{\text{case } e' \{x_1.e'_1 \mid x_2.e'_2\} \parallel \mu\} \Downarrow \nu\Sigma'_1\{\bigcup_{1.v_1^{e'} \in \mathbb{V}^{e'}} \mathbb{V}_{1,v_1^{e'_1}}^{e', e'_1} \parallel \mu'_1\}}$$

Note that the set $\bigcup_{1.v_1^{e'} \in \mathbb{V}^{e'}} \mathbb{V}_{1,v_1^{e'_1}}^{e', e'_1}$ is the set \mathbb{V}_1^{e', e'_1} , i.e. the result of evaluating each $e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1^{e'_1}}](e_1)$. We would like to show that $\bigcup_{\text{case } e' \{x_1.e'_1 \mid x_2.e'_2\} \in \hat{\sigma}(\text{case } e \{x_1.e_1 \mid x_2.e_2\})} \mathbb{V}^{e', e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau]$. First, observe that this union only depends on expressions from $\hat{\sigma}(e)$ and $\hat{\sigma}(e_1)$, since $\hat{\sigma}(e_2)$ is not involved in any evaluations. Thus, we have the following

$$\begin{aligned} & \bigcup_{\text{case } e' \{x_1.e'_1 \mid x_2.e'_2\} \in \hat{\sigma}(\text{case } e \{x_1.e_1 \mid x_2.e_2\})} \mathbb{V}^{e', e'_1} \\ &= \bigcup_{(e', e'_1) \in \hat{\sigma}(e) \times \hat{\sigma}(e_1)} \mathbb{V}^{e', e'_1} && \text{(observation)} \\ &= \bigcup_{e' \in \hat{\sigma}(e)} \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}^{e', e'_1} && \text{(definition?)} \\ &= \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}^{e'_1} && \text{(applying union over } \hat{\sigma}(e)) \end{aligned}$$

Since $e'_1 \in \hat{\sigma}(e_1)$, we have that $e'_1 = [v_1/x_1]e''_1$ for $e'_1 \in \hat{\sigma}(e_1)$ and $v_1 \in \mathbb{V}_1$. Thus, we can rewrite the set as

$$\begin{aligned} &= \bigcup_{e''_1 \in \hat{\sigma}(e_1)} \bigcup_{v_1 \in \mathbb{V}_1} \mathbb{V}^{[v_1/x_1]e''_1} \\ &= \bigcup_{e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1}](e_1)} \mathbb{V}^{e'_1} && \text{(by definition)} \end{aligned}$$

We already have from the IH that $\bigcup_{e'_1 \in \sigma[\widehat{x_1 \mapsto \mathbb{V}_1}](e_1)} \mathbb{V}^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau]$.

- $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} = \{2 \cdot v_2 \mid v_2 \in \mathbb{V}_2\}$ with $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau_2]$

This case is symmetric to the previous.

- T-LAM

WTS: $\hat{\sigma}(\lambda(x : \tau_1.e_2)) \in \mathcal{L}_{\Sigma'} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$

By definition of substitution (upto alpha-equivalence on x), we have $\hat{\sigma}(\lambda(x : \tau_1.e_2)) = \{\lambda(x : \tau_1.e'_2) \mid e'_2 \in \hat{\sigma}(e_2)\}$.

By **IH**, we have $\forall \Sigma_1$ s.t. $\Sigma_1 \leq \Sigma$, $\forall \sigma_1 : \Gamma, x_1 : \tau_1; \Sigma_1, \hat{\sigma}_1(e_2) \in \mathcal{L}_{\Sigma_1} \llbracket \tau_2 \rrbracket$. Unfolding the definition of leaf-determinism, this means

- Since $\hat{\sigma}_1(e_2) \in \mathcal{L}_{\Sigma_1} \llbracket \tau_2 \rrbracket$, if $\mu_1 : \Sigma_1$, then

$$\forall e'_2 \in \hat{\sigma}(e_2). \nu_{\Sigma_1}\{e'_2 \parallel \mu_1\} \Downarrow \nu_{\Sigma_2}\{\mathbb{V}_2^{e'_2} \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau_2 \rrbracket$.

Suppose we have $\mu : \Sigma'$. By the set-lifted dynamics, for each $\lambda(x : \tau_1.e'_2) \in \hat{\sigma}(\lambda(x : \tau_1.e_2))$, we have that

$$\overline{\nu_{\Sigma'}\{\lambda(x : \tau_1.e'_2) \parallel \mu\} \Downarrow \nu_{\Sigma'}\{\{\lambda(x : \tau_1.e'_2)\} \parallel \mu\}}$$

We then want to show that $\bigcup_{\lambda(x : \tau_1.e'_2) \in \hat{\sigma}(\lambda(x : \tau_1.e_2))} \{\lambda(x : \tau_1.e'_2)\} \in \mathcal{L}\mathcal{V}_{\Sigma'} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$, which is exactly the set $\hat{\sigma}(\lambda(x : \tau_1.e_2))$.

Suppose we have $\Sigma_1 \leq \Sigma'$ and \mathbb{V}_1 such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket \tau_1 \rrbracket$.

By the definition of $\hat{\sigma}$, we have that $\sigma[\widehat{x \mapsto \mathbb{V}_1}](e_2) = \{[v_1/x]e_2 \mid v_1 \in \mathbb{V}_1\}$. By the **IH**, we have $\sigma[\widehat{x \mapsto \mathbb{V}_1}](e_2) \in \mathcal{L}_{\Sigma_1} \llbracket \tau_2 \rrbracket$, meaning we have that the above set is in $\mathcal{L}_{\Sigma_1} \llbracket \tau_2 \rrbracket$.

- T-APP

WTS: $\hat{\sigma}(e_1(e_2)) \in \mathcal{L}_{\Sigma'} \llbracket \tau_2 \rrbracket$

By definition of substitution, we have $\hat{\sigma}(e_1(e_2)) = \{e'_1(e'_2) \mid e'_1 \in \hat{\sigma}(e_1), e'_2 \in \hat{\sigma}(e_2)\}$.

By **IH**, we have

- $\hat{\sigma}(e_1) \in \mathcal{L}_{\Sigma'} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$
- $\hat{\sigma}(e_2) \in \mathcal{L}_{\Sigma'} \llbracket \tau_1 \rrbracket$

Suppose we have $\mu : \Sigma'$. Unfolding the definitions, we have

- Since $\hat{\sigma}(e_1) \in \mathcal{L}_{\Sigma'} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$,

$$\forall e'_1 \in \hat{\sigma}(e_1). \nu_{\Sigma'}\{e'_1 \parallel \mu\} \Downarrow \nu_{\Sigma_1}\{\mathbb{V}_1^{e'_1} \parallel \mu_1\}$$

such that $\mu_1 : \Sigma_1$ and $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$.

- Since $\hat{\sigma}(e_2) \in \mathcal{L}_{\Sigma'} \llbracket \tau_1 \rrbracket$,

$$\forall e'_2 \in \hat{\sigma}(e_2). \nu_{\Sigma'}\{e'_2 \parallel \mu\} \Downarrow \nu_{\Sigma_2}\{\mathbb{V}_1^{e'_2} \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau_1 \rrbracket$.

Since $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\tau_1 \xrightarrow{\ell_k} \tau_2]$, by the definition of leaf-determinism, we have that

$$\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} = \{\lambda(x : \tau_1.e) \mid \forall \Sigma'_1 \leq \Sigma_1, \forall \mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau_1], \{[v_1/x]e \mid v_1 \in \mathbb{V}'_1\} \in \mathcal{L}_{\Sigma'_1}[\tau_2]\}$$

Since $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2}[\tau_1]$, by Lemma 2, we have that the set is in $\mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau_1]$. Since it is also the case that $\Sigma_1 \cup \Sigma_2 \leq \Sigma_1$, we have that

$$\{[v_2/x]e \mid v_2 \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2}, \lambda(x : \tau_1.e) \in \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1}\} \in \mathcal{L}_{\Sigma_1 \cup \Sigma_2}[\tau_2]$$

Define $\mathbb{E} = \{[v_2/x]e \mid v_2 \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2}, \lambda(x : \tau_1.e) \in \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1}\}$. Unrolling the definition of leaf-determinism on this set, with the fact that $\mu_1 \cup \mu_2 : \Sigma_1 \cup \Sigma_2$, this gives us

- Since $\mathbb{E} \in \mathcal{L}_{\Sigma_1 \cup \Sigma_2}[\tau_2]$, we have that exists Σ^* such that $\Sigma^* \leq \Sigma_1 \cup \Sigma_2$. Then, we have

$$\forall e' \in \mathbb{E}. \nu_{\Sigma_1 \cup \Sigma_2}\{e' \parallel \mu_1 \cup \mu_2\} \Downarrow \nu_{\Sigma^*}\{\mathbb{V}^{e'} \parallel \mu^*\}$$

such that $\mu^* : \Sigma^*$ and $\bigcup_{e' \in \mathbb{E}} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma^*}[\tau_2]$.

Note that since $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2}[\tau_1]$, we have that each $\mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2}[\tau_1]$ (and likewise that each $\mathbb{V}_1^{e'_1} \in \mathcal{L}_{\Sigma_1}[\tau_1 \xrightarrow{\ell_k} \tau_2]$), so all of the above applies to these subsets individually. Namely, we have that

$$\begin{aligned} \mathbb{V}_1^{e'_1} &= \{\lambda(x : \tau_1.e) \mid \forall \Sigma'_1 \leq \Sigma_1, \forall \mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau_1], \{[v_1^{e'_1}/x]e \mid v_1 \in \mathbb{V}'_1\} \in \mathcal{L}_{\Sigma'_1}[\tau_2]\} \\ &\quad \{[v_2^{e'_2}/x]e \mid v_2^{e'_2} \in \mathbb{V}_2^{e'_2}, \lambda(x : \tau_1.e) \in \mathbb{V}_1^{e'_1}\} \in \mathcal{L}_{\Sigma_1 \cup \Sigma_2}[\tau_2] \end{aligned}$$

Define the above set to be $\mathbb{E}^{e'_1, e'_2}$. Unrolling the definition of leaf-determinism on this set, with the fact that $\mu_1 \cup \mu_2 : \Sigma_1 \cup \Sigma_2$, this gives us

- Since $\mathbb{E}^{e'_1, e'_2} \in \mathcal{L}_{\Sigma_1 \cup \Sigma_2}[\tau_2]$, we have that exists Σ^* such that $\Sigma^* \leq \Sigma_1 \cup \Sigma_2$. Then, we have

$$\forall e^{e'_1, e'_2} \in \mathbb{E}^{e'_1, e'_2}. \nu_{\Sigma_1 \cup \Sigma_2}\{e^{e'_1, e'_2} \parallel \mu_1 \cup \mu_2\} \Downarrow \nu_{\Sigma^*}\{\mathbb{V}^{e^{e'_1, e'_2}} \parallel \mu^*\}$$

such that $\mu^* : \Sigma^*$ and $\bigcup_{e^{e'_1, e'_2} \in \mathbb{E}^{e'_1, e'_2}} \mathbb{V}^{e^{e'_1, e'_2}} \in \mathcal{L}\mathcal{V}_{\Sigma^*}[\tau_2]$.

Then, by the set-lifted dynamics, for each $e'_1(e'_2) \in \hat{\sigma}(e_1(e_2))$, we have

$$\frac{\begin{aligned} &\nu_{\Sigma}\{e'_1 \parallel \mu\} \Downarrow \nu_{\Sigma_1}\{\mathbb{V}_1^{e'_1} \parallel \mu_1\} \quad \nu_{\Sigma}\{e'_2 \parallel \mu\} \Downarrow \nu_{\Sigma_2}\{\mathbb{V}_2^{e'_2} \parallel \mu_2\} \\ &(\nu_{\Sigma_1 \cup \Sigma_2}\{[v_2^{e'_2}/x]e \parallel \mu_1 \cup \mu_2\} \Downarrow \nu_{\Sigma^*}\{\mathbb{V}^{v_1^{e'_1}, v_2^{e'_2}} \parallel \mu^*\})_{v_1^{e'_1} = \lambda(x : \tau_1.e)} \end{aligned}}{\nu_{\Sigma}\{e'_1(e'_2) \parallel \mu\} \Downarrow \nu_{\Sigma^*}\{\bigcup_{(v_1^{e'_1}, v_2^{e'_2}) \in \mathbb{V}_1^{e'_1} \times \mathbb{V}_2^{e'_2}} \mathbb{V}^{v_1^{e'_1}, v_2^{e'_2}} \parallel \mu^*\}}$$

Note that $\bigcup_{(v_1^{e'_1}, v_2^{e'_2}) \in \mathbb{V}_1^{e'_1} \times \mathbb{V}_2^{e'_2}} \mathbb{V}^{v_1^{e'_1}, v_2^{e'_2}} = \bigcup_{e^{e'_1, e'_2} \in \mathbb{E}^{e'_1, e'_2}} \mathbb{V}^{e^{e'_1, e'_2}}$ by definition.

We now show that the required set is in $\mathcal{L}_{\Sigma^*} \llbracket \tau_2 \rrbracket$:

$$\begin{aligned}
& \bigcup_{(e'_1, e'_2) \in \hat{\sigma}(e_1) \times \hat{\sigma}(e_2)} \bigcup_{e'_1, e'_2 \in \mathbb{E}^{e'_1, e'_2}} \mathbb{V}^{e'_1, e'_2} \\
&= \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \bigcup_{e'_1, e'_2 \in \mathbb{E}^{e'_1, e'_2}} \mathbb{V}^{e'_1, e'_2} \\
&= \bigcup_{e' \in \mathbb{E}} \mathbb{V}^{e'}
\end{aligned}$$

We already have that the final set is in $\mathcal{L}\mathcal{V}_{\Sigma^*} \llbracket \tau_2 \rrbracket$ from the IH.

- **Case:** T-ENC-MOBILE

$$\frac{\text{ENC-MOBILE} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau \quad \tau \blacktriangleleft \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{encrypt}_\ell(e_1; e_2) : (\text{enc}_\ell \tau)_\perp}$$

WTS: $\hat{\sigma}(\text{encrypt}_\ell(e_1; e_2)) \in \mathcal{L}_{\Sigma'} \llbracket (\text{enc}_\ell \tau)_\perp \rrbracket \xi$

By definition of substitution, we have $\hat{\sigma}(\text{encrypt}_\ell(e_1; e_2)) = \{\text{encrypt}_\ell(e'_1; e'_2) \mid e'_1 \in \hat{\sigma}(e_1), e'_2 \in \hat{\sigma}(e_2)\}$.

By **IH**, we have

- $\hat{\sigma}(e_1) \in \mathcal{L}_{\Sigma'} \llbracket \text{key}_\ell \rrbracket$
- $\hat{\sigma}(e_2) \in \mathcal{L}_{\Sigma'} \llbracket \tau \rrbracket$

Unfolding the term interpretations, we have

- Since $\hat{\sigma}(e_1) \in \mathcal{L}_{\Sigma} \llbracket \text{key}_\ell \rrbracket$,

$$\forall e'_1 \in \hat{\sigma}(e_1). \nu_{\Sigma'} \{e'_1 \parallel \mu\} \Downarrow \nu_{\Sigma_1} \{\mathbb{V}_1^{e'_1} \parallel \mu_1\}$$

such that $\mu_1 : \Sigma_1$ and $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}^{e'_1} \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket \text{key}_\ell \rrbracket$.

- Since $\hat{\sigma}(e_2) \in \mathcal{L}_{\Sigma'} \llbracket \tau \rrbracket$,

$$\forall e'_2 \in \hat{\sigma}(e_2). \nu_{\Sigma'} \{e'_2 \parallel \mu\} \Downarrow \nu_{\Sigma_2} \{\mathbb{V}_2^{e'_2} \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau \rrbracket$.

By the definition of leaf-determinism, we have that $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} = \{\text{key}\langle K \rangle\}$ for $K \sim \ell \in \Sigma_1$, and thus that each $\mathbb{V}_1^{e'_1} = \{\text{key}\langle K \rangle\}$. Since $\mu_1 : \Sigma_1$ and $K \sim \ell \in \Sigma_1$, then $\Sigma_1 = \Sigma_1^*$, $K \sim \ell$ and $\mu_1 = \mu_1^* \otimes K \hookrightarrow v_k$.

Note also that since $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau \rrbracket$, we have that each $\mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau \rrbracket$.

Then, by the set-lifted dynamics, for each $\text{encrypt}_\ell(e_1; e_2) \in \hat{\sigma}(\text{encrypt}_\ell(e_1; e_2))$, we

have

$$\frac{\nu\Sigma'\{e'_1 \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\}}{\nu\Sigma'\{e'_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2^{e'_2} \parallel \mu_2\} \quad \mathbb{U} = \{u \mid v^{e'_2} \in \mathbb{V}_2^{e'_2}, u \in \mathcal{E}_\ell(v_k, v)\}}{\nu\Sigma'\{\text{encrypt}_\ell(e'_1; e'_2) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\mathbb{U}^{e'_1, e'_2} \parallel \mu_1 \cup \mu_2\}}$$

We would like to show that $\bigcup_{\text{encrypt}_\ell(e'_1; e'_2) \in \hat{\sigma}(\text{encrypt}_\ell(e_1; e_2))} \mathbb{U}^{e'_1, e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\text{enc}_\ell \tau]$.
By Lemma 2, we have that the sets $\mathbb{V}_1^{e'_1}$ and $\mathbb{V}_2^{e'_2}$ (and their unioned version) are in the value interpretation at $\Sigma_1 \cup \Sigma_2$. Then, we have

$$\begin{aligned} & \bigcup_{\text{encrypt}_\ell(e'_1; e'_2) \in \hat{\sigma}(\text{encrypt}_\ell(e_1; e_2))} \mathbb{U}^{e'_1, e'_2} \\ &= \bigcup_{(e'_1, e'_2) \in \hat{\sigma}(e_1) \times \hat{\sigma}(e_2)} \mathbb{U}^{e'_1, e'_2} \\ &= \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{U}^{e'_1, e'_2} \\ &= \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \{u \mid v^{e'_2} \in \mathbb{V}_2^{e'_2}, u \in \mathcal{E}_\ell(v_k, v) \text{ for } \mu_1(K) = v_k\} \\ &= \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \{u \mid v \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2}, u \in \mathcal{E}_\ell(v_k, v) \text{ for } \mu_1(K) = v_k\} \\ &= \{u \mid v \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2}, u \in \mathcal{E}_\ell(v_k, v) \text{ for } \mu_1(K) = v_k\} \\ & \qquad \qquad \qquad (\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \{\text{key}\langle K \rangle\} = \{\text{key}\langle K \rangle\}) \end{aligned}$$

Since $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau]$, this set is, by definition, in $\mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\text{enc}_\ell \tau]$.

• **Case: T-ENC-STATIC**

This case is symmetric to the previous.

• **Case: T-DEC**

$$\frac{\text{T-DEC} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : (\text{enc}_\ell \tau)_\epsilon}{\Sigma; \Gamma \vdash_{\text{kc}} \text{decrypt}_\ell(e_1; e_2) : \tau \text{ result}_\epsilon}$$

WTS: $\hat{\sigma}(\text{decrypt}_\ell(e_1; e_2)) \in \mathcal{L}_{\Sigma'}[\tau \text{ result}_\epsilon]$

By definition of substitution, we have $\hat{\sigma}(\text{decrypt}_\ell(e_1; e_2)) = \{\text{decrypt}_\ell(e'_1; e'_2) \mid e'_1 \in \hat{\sigma}(e_1), e'_2 \in \hat{\sigma}(e_2)\}$.

By **IH**, we have

- $\hat{\sigma}(e_1) \in \mathcal{L}_{\Sigma'}[\text{key}_\ell]$
- $\hat{\sigma}(e_2) \in \mathcal{L}_{\Sigma'}[(\text{enc}_\ell \tau)_\epsilon]$

Unfolding the term interpretations, we have

- Since $\hat{\sigma}(e_1) \in \mathcal{L}_\Sigma[\llbracket \text{key}_\ell \rrbracket]$,

$$\forall e'_1 \in \hat{\sigma}(e_1). \nu\Sigma'\{e'_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1^{e'_1} \parallel \mu_1\}$$

such that $\mu_1 : \Sigma_1$ and $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} \in \mathcal{LV}_{\Sigma_1}[\llbracket \text{key}_\ell \rrbracket]$.

- Since $\hat{\sigma}(e_2) \in \mathcal{L}_\Sigma[\llbracket (\text{enc}_\ell \tau)_\epsilon \rrbracket]$,

$$\forall e'_2 \in \hat{\sigma}(e_2). \nu\Sigma'\{e'_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2^{e'_2} \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} \in \mathcal{LV}_{\Sigma_2}[\llbracket (\text{enc}_\ell \tau)_\epsilon \rrbracket]$.

By the definition of leaf-determinism, we have that $\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \mathbb{V}_1^{e'_1} = \{\text{key}\langle K \rangle\}$ for $K \sim \ell \in \Sigma_1$, and thus that each $\mathbb{V}_1^{e'_1} = \{\text{key}\langle K \rangle\}$. Since $\mu_1 : \Sigma_1$ and $K \sim \ell \in \Sigma_1$, then $\Sigma_1 = \Sigma_1^*$, $K \sim \ell$ and $\mu_1 = \mu_1^* \otimes K \hookrightarrow v_k$.

Similarly, by definition, we have that $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2} = \{u \mid u \in \mathcal{E}_\ell(v'_k, v), v \in \mathbb{V}\}$ such that $\mathbb{V} \in \mathcal{LV}_{\Sigma_2}[\llbracket \tau \rrbracket]$. As such, we also have that $\mathbb{V}_2^{e'_2} = \{u \mid u \in \mathcal{E}_\ell(v'_k, v), v^{e'_2} \in \mathbb{V}^{e'_2}\}$ with $v_2^{e'_2} \in \mathbb{V}^{e'_2}$.

We now case on whether $v_k = v'_k$, i.e. whether the key used to encrypt the ciphertexts is the same one being used to decrypt them:

- $v_k = v'_k$

In this case, we have that all $u \in \mathcal{E}_\ell(v_k, v)$, meaning $\mathcal{D}(v_k, u) = v$ by the determinism of decryption. Then, for each $\text{decrypt}_\ell(e'_1; e'_2) \in \hat{\sigma}(\text{decrypt}_\ell(e_1; e_2))$, we have

$$\frac{\nu\Sigma'\{e'_1 \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell \{ \{\text{key}\langle K \rangle\} \parallel \mu_1^* \otimes K \hookrightarrow v_k \} \quad \nu\Sigma'\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2^{e'_2} \parallel \mu_2\} \quad \mathbb{V}^{e'_1, e'_2} = \{\mathcal{D}(v_k, u) \mid \mu_1(K) = v_k, u^{e'_2} \in \mathbb{V}_2^{e'_2}\}}{\nu\Sigma'\{\text{decrypt}_\ell(e'_1; e'_2) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\text{Ok}(v) \mid v \in \mathbb{V}^{e'_1, e'_2}\} \parallel \mu_1 \cup \mu_2}$$

We would like to show that $\bigcup_{\text{decrypt}_\ell(e'_1; e'_2) \in \hat{\sigma}(\text{decrypt}_\ell(e_1; e_2))} \{\text{Ok}(v) \mid v \in \mathbb{V}^{e'_1, e'_2}\} \in \mathcal{LV}_{\Sigma_1 \cup \Sigma_2}[\llbracket \tau \text{ result}_\epsilon \rrbracket]$. First, by Lemma 2, we have that each of the IH results are in

$\Sigma_1 \cup \Sigma_2$. Then, we have the following:

$$\begin{aligned}
& \bigcup_{\text{decrypt}_\ell(e'_1; e'_2) \in \hat{\sigma}(\text{decrypt}_\ell(e_1; e_2))} \{\text{Ok}(v) \mid v \in \mathbb{V}^{e'_1, e'_2}\} \\
&= \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \{\text{Ok}(v) \mid v \in \mathbb{V}^{e'_1, e'_2}\} \\
&= \{\text{Ok}(v) \mid v \in \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}^{e'_1, e'_2}\} \\
&= \{\text{Ok}(v) \mid v \in \bigcup_{e'_1 \in \hat{\sigma}(e_1)} \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \{\mathcal{D}(v_k, u) \mid \mu_1(K) = v_k, u^{e'_2} \in \mathbb{V}_2^{e'_2}\}\} \\
&= \{\text{Ok}(v) \mid v \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \{\mathcal{D}(v_k, u) \mid \mu_1(K) = v_k, u^{e'_2} \in \mathbb{V}_2^{e'_2}\}\} \\
&\qquad\qquad\qquad (\bigcup_{e'_1 \in \hat{\sigma}(e_1)} \{\text{key}\langle K \rangle\} = \{\text{key}\langle K \rangle\}) \\
&= \{\text{Ok}(v) \mid v \in \{\mathcal{D}(v_k, u) \mid \mu_1(K) = v_k, u^{e'_2} \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2}\}\} \\
&= \{\text{Ok}(v) \mid v \in \{\mathcal{D}(v_k, u) \mid \mu_1(K) = v_k, u^{e'_2} \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}_2^{e'_2}\}\} \\
&= \{\text{Ok}(v) \mid v \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}^{e'_2}\}
\end{aligned}$$

Since $\bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}^{e'_2} \in \mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau]$, we have that the set $\{\text{Ok}(v) \mid v \in \bigcup_{e'_2 \in \hat{\sigma}(e_2)} \mathbb{V}^{e'_2}\} \in \mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau \text{ result}_e]$.

- $\mu(K) \neq v_k$

In this case, we have that for all $u \in \mathcal{E}_\ell(v'_k, v)$ for some mismatched key v'_k , meaning $\mathcal{D}(v_k, u) = \perp$.

We apply the following dynamics rule for each $\text{decrypt}_\ell(e'_1; e'_2) \in \hat{\sigma}(\text{decrypt}_\ell(e_1; e_2))$:

$$\frac{\nu\Sigma\{e'_1 \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma'\{e'_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2^{e'_2} \parallel \mu_2\} \quad (\mathcal{D}(v_k, u) = \perp)_{v_2^{e'_2} \in \mathbb{V}_2^{e'_2}}}{\nu\Sigma\{\text{decrypt}_\ell(e'_1; e'_2) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\{\text{Error}\}^{e'_1, e'_2} \parallel \mu_1 \cup \mu_2\}}$$

Note that the union of each set $\{\text{Error}\}^{e'_1, e'_2}$ is $\{\text{Error}\}$, which is in $\mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[\tau \text{ result}_e]$.

- **Case: T-KEY-GEN**

$$\frac{\text{T-KEY-GEN} \quad \text{kc} \sqsubseteq \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{gen}\langle \ell \rangle : \tau}$$

WTS: $\hat{\sigma}(\text{gen}\langle\ell\rangle) \in \mathcal{L}_{\Sigma'}[\tau]$

By definition of substitution (up to alpha-equivalence), we have $\hat{\sigma}(\text{gen}\langle\ell\rangle) = \{\text{gen}\langle\ell\rangle\}$.

Suppose we have $\mu : \Sigma'$. We can then apply the following dynamics rule:

$$\frac{\mathcal{G}(\ell) = v_k}{\nu\Sigma'\{\text{gen}\langle\ell\rangle \parallel \mu\} \Downarrow \nu\Sigma', K \sim \ell\{\mathbb{V}^{e'_k} \parallel \mu \otimes K \hookrightarrow v_k\}}$$

Since $K \sim \ell \in \Sigma'$, $K \sim \ell$, we have that $\{\text{key}\langle K \rangle\} \in \mathcal{L}\mathcal{V}_{\Sigma', K \sim \ell}[\text{key}\ell]$.

We then get what we want to show from the **IH**.

- **Case: T-KEY-ACCESS**

WTS: $\hat{\sigma}(\text{key}\langle K \rangle) \in \mathcal{L}_{\Sigma'}[\text{key}\ell]$

By definition of substitution, we have that $\hat{\sigma}(\text{key}\langle K \rangle) = \{\text{key}\langle K \rangle\}$.

Suppose we have $\mu : \Sigma'$. Note that since $\Sigma' \leq \Sigma$, $K \sim \ell$ and $\mu : \Sigma'$, it must be the case that $\Sigma' = \Sigma^*$, $K \sim \ell$ and $\mu = \mu^* \otimes K \hookrightarrow v_k$.

From the dynamics, we then have

$$\frac{}{\nu\Sigma^*, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu^* \otimes K \hookrightarrow v_k\} \Downarrow \nu\Sigma^*, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu^* \otimes K \hookrightarrow v_k\}}$$

We then have $\{\text{key}\langle K \rangle\} \in \mathcal{L}\mathcal{V}_{\Sigma^*, K \sim \ell}[\text{key}\ell]$ by definition.

- **Case: T-SUB**

$$\frac{\text{T-SUB} \quad \Sigma; \Gamma \vdash_{\text{kc}'} e : \tau' \quad \text{kc} \sqsubseteq \text{kc}' \quad \tau' \leq \tau}{\Sigma; \Gamma \vdash_{\text{kc}} e : \tau}$$

WTS: $\hat{\sigma}(e) \in \mathcal{L}_{\Sigma'}[\tau]$

From the **IH**, we have that $\hat{\sigma}(e) \in \mathcal{L}_{\Sigma'}[\tau']$.

Unfolding the definition of leaf-determinism, this means that

- Since $\hat{\sigma}(e) \in \mathcal{L}_{\Sigma'}[\tau']$,

$$\forall e' \in \hat{\sigma}(e). \nu\Sigma'\{e' \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}^{e'} \parallel \mu'\}$$

such that $\mu' : \Sigma''$ and $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau']$.

By Lemma 7, since $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau']$, we have that all $\bigcup_{e' \in \hat{\sigma}(e)} \mathbb{V}^{e'} \in \mathcal{L}\mathcal{V}_{\Sigma''}[\tau]$, which allows us to show that $\hat{\sigma}(e) \in \mathcal{L}_{\Sigma'}[\tau]$.

- **Omitted:** nat, ok, err, resMatch

A.2 Proof of Binary FTLR

Suppose we have Σ', Σ'' such that $\Sigma' \leq \Sigma$ and $\Sigma'' \leq \Sigma$, and suppose we have σ, σ' such that $\sigma :_{\text{LD}} \Gamma; \Sigma', \sigma' :_{\text{LD}} \Gamma; \Sigma''$, and

$$\forall \gamma \in \text{sing}(\sigma), \exists \gamma' \in \text{sing}(\sigma'). \gamma \equiv_{\xi} \gamma' : \Gamma; (\Sigma' \uplus \Sigma'')$$

$$\forall \gamma' \in \text{sing}(\sigma'), \exists \gamma \in \text{sing}(\sigma). \gamma \equiv_{\xi} \gamma' : \Gamma; (\Sigma' \uplus \Sigma'')$$

Suppose we have an arbitrary such (γ, γ') such that $\gamma \equiv_{\xi} \gamma' : \Gamma; \Sigma' \uplus \Sigma''$.

We proceed by rule induction on the typing judgment:

- **Case: T-PROD**

$$\mathbf{WTS:} (\hat{\gamma}\langle e_1, e_2 \rangle, \hat{\gamma}'\langle e_1, e_2 \rangle) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_1 \times \tau_2 \rrbracket$$

By definition of substitution, we have that $\hat{\gamma}\langle e_1, e_2 \rangle = \langle \hat{\gamma}(e_1), \hat{\gamma}(e_2) \rangle$ and $\hat{\gamma}'\langle e_1, e_2 \rangle = \langle \hat{\gamma}'(e_1), \hat{\gamma}'(e_2) \rangle$.

From the premises, we have $\Gamma; \Sigma \vdash_{\text{kc}} e_1 : \tau_1$ and $\Gamma; \Sigma \vdash_{\text{kc}} e_2 : \tau_2$.

By the **IH**, we have that $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_1 \rrbracket$ and $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_2 \rrbracket$.

Suppose we have μ, μ' such that $\mu \equiv_{\xi} \mu' : \Sigma' \uplus \Sigma''$. By the definition of the term interpretation, we have that

- Since $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket \tau_1 \rrbracket$,

$$\nu_{\Sigma'} \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V}_1 \parallel \mu_1 \}$$

and

$$\nu_{\Sigma''} \{ \hat{\gamma}'(e_1) \parallel \mu' \} \Downarrow \nu_{\Sigma'_1} \{ \mathbb{V}'_1 \parallel \mu'_1 \}$$

such that $\mu_1 \equiv_{\xi} \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and

$$\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^{\xi} \llbracket \tau_1 \rrbracket$$

$$\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^{\xi} \llbracket \tau_1 \rrbracket$$

- Since $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma''}^{\xi} \llbracket \tau_2 \rrbracket$,

$$\nu_{\Sigma''} \{ \hat{\gamma}(e_2) \parallel \mu \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}_2 \parallel \mu_2 \}$$

and

$$\nu_{\Sigma'} \{ \hat{\gamma}'(e_2) \parallel \mu' \} \Downarrow \nu_{\Sigma'_2} \{ \mathbb{V}'_2 \parallel \mu'_2 \}$$

such that $\mu_2 \equiv_{\xi} \mu'_2 : \Sigma_2 \uplus \Sigma'_2$ and

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^{\xi} \llbracket \tau_2 \rrbracket$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^{\xi} \llbracket \tau_2 \rrbracket$$

By the set-lifted dynamics rules, we have

$$\frac{\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\} \quad \nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}}{\nu\Sigma'\{\langle\hat{\gamma}(e_1), \hat{\gamma}(e_2)\rangle \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\} \parallel \mu_1 \cup \mu_2\}}$$

$$\frac{\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu'\} \Downarrow \nu\Sigma'_1\{\mathbb{V}'_1 \parallel \mu'_1\} \quad \nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma'_2\{\mathbb{V}'_2 \parallel \mu'_2\}}{\nu\Sigma''\{\langle\hat{\gamma}'(e_1), \hat{\gamma}'(e_2)\rangle \parallel \mu'\} \Downarrow \nu\Sigma'_1 \cup \Sigma'_2\{\{\langle v'_1, v'_2 \rangle \mid v'_1 \in \mathbb{V}'_1, v'_2 \in \mathbb{V}'_2\} \parallel \mu'_1 \cup \mu'_2\}}$$

Define

$$\mathbb{V}_{p1} = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\}, \quad \mathbb{V}_{p2} = \{\langle v'_1, v'_2 \rangle \mid v'_1 \in \mathbb{V}'_1, v'_2 \in \mathbb{V}'_2\}$$

First, observe the following:

1. $\forall v_1 \in \mathbb{V}_1, \exists v'_1 \in \mathbb{V}'_1, (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \tau_1 \rrbracket$
2. $\forall v'_1 \in \mathbb{V}'_1, \exists v_1 \in \mathbb{V}_1, (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \tau_1 \rrbracket$
3. $\forall v_2 \in \mathbb{V}_2, \exists v'_2 \in \mathbb{V}'_2, (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket$
4. $\forall v'_2 \in \mathbb{V}'_2, \exists v_2 \in \mathbb{V}_2, (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket$

- By Lemma 16, since $\Sigma_1 \cup \Sigma_2 \leq \Sigma_1$ and $\Sigma_1 \cup \Sigma_2 \leq \Sigma_1$ (Lemma 21) and Observation (1), we

$$\forall v_1 \in \mathbb{V}_1, \exists v'_1 \in \mathbb{V}'_1, (v_1, v'_1) \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$$

Similarly, via Lemma 16 and Observation (3), we have that

$$\forall v_2 \in \mathbb{V}_2, \exists v'_2 \in \mathbb{V}'_2, (v_2, v'_2) \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket$$

With both of these assumptions, we have that

$$\forall \langle v_1, v_2 \rangle \in \mathbb{V}_{p1}. \exists \langle v'_1, v'_2 \rangle \in \mathbb{V}_{p2}. (\langle v_1, v_2 \rangle, \langle v'_1, v'_2 \rangle) \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_1 \times \tau_2 \rrbracket$$

Since for each $\langle v_1, v_2 \rangle$, we can choose its corresponding v'_1, v'_2 such that $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$, and by the definition of the value interpretation at $\tau_1 \times \tau_2$ we have that $(\langle v_1, v_2 \rangle, \langle v'_1, v'_2 \rangle) \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_1 \times \tau_2 \rrbracket$.

- By the same reasoning as above, using Observations (2) and (4), we have

$$\forall \langle v'_1, v'_2 \rangle \in \mathbb{V}_{p2}. \exists \langle v_1, v_2 \rangle \in \mathbb{V}_{p1}. (\langle v_1, v_2 \rangle, \langle v'_1, v'_2 \rangle) \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_1 \times \tau_2 \rrbracket$$

- Since we have $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and $\mu_2 \equiv_\xi \mu'_2 : \Sigma_2 \uplus \Sigma'_2$, we have that $(\mu_1 \cup \mu_2) \equiv_\xi (\mu'_1 \cup \mu'_2) : (\Sigma_1 \cup \Sigma_2) \uplus (\Sigma'_1 \cup \Sigma'_2)$ (Lemma 20).
- Since we have all of the above, we have that $(\hat{\gamma}\langle e_1, e_2 \rangle, \hat{\gamma}'\langle e_1, e_2 \rangle) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \tau_1 \times \tau_2 \rrbracket$.

• **Case: T-PROJ-I**

WTS: $(\hat{\gamma}(e \cdot i), \hat{\gamma}'(e \cdot i)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_i \rrbracket$ for $i \in \{1, 2\}$

By definition of substitution, we have that $\hat{\gamma}(e \cdot i) = \hat{\gamma}(e) \cdot i$ and $\hat{\gamma}'(e \cdot i) = \hat{\gamma}'(e) \cdot i$.

From the premise, we have $\Gamma; \Sigma \vdash_{\text{kc}} e : \tau_1 \times \tau_2$.

By the **IH**, we have that $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_1 \times \tau_2 \rrbracket$.

Suppose we have μ, μ' such that $\mu \equiv_{\xi} \mu' : \Sigma' \uplus \Sigma''$. By the definition of the term interpretation, we have that

- Since $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma}^{\xi} \llbracket \tau_1 \times \tau_2 \rrbracket$,

$$\nu \Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu \Sigma_1 \{ \mathbb{V} \parallel \mu_1 \}$$

and

$$\nu \Sigma'' \{ \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu \Sigma_2 \{ \mathbb{V}' \parallel \mu_2 \}$$

such that $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$ and

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}' \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \times \tau_2 \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V} \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \times \tau_2 \rrbracket$$

From the **IH**, unfolding the definition of the value interpretation at $\tau_1 \times \tau_2$, we have

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}' \text{ s.t. } v = \langle v_1, v_2 \rangle, v' = \langle v'_1, v'_2 \rangle, (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \rrbracket \wedge (v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_2 \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V} \text{ s.t. } v = \langle v_1, v_2 \rangle, v' = \langle v'_1, v'_2 \rangle, (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \rrbracket \wedge (v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_2 \rrbracket$$

Note that each element in \mathbb{V} and \mathbb{V}' are of the form $\langle v_1, v_2 \rangle$ and $\langle v'_1, v'_2 \rangle$, respectively. Then, by the set-lifted dynamics rules, we have

$$\frac{\frac{\nu \Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu \Sigma_1 \{ \mathbb{V} \parallel \mu_1 \}}{\nu \Sigma' \{ \hat{\gamma}(e) \cdot i \parallel \mu \} \Downarrow \nu \Sigma_1 \{ \{ v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}, i \in \{1, 2\} \} \parallel \mu_1 \}}}{\frac{\nu \Sigma'' \{ \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu \Sigma_2 \{ \mathbb{V}' \parallel \mu_2 \}}{\nu \Sigma'' \{ \hat{\gamma}'(e) \cdot i \parallel \mu \} \Downarrow \nu \Sigma_2 \{ \{ v'_i \mid \langle v'_1, v'_2 \rangle \in \mathbb{V}', i \in \{1, 2\} \} \parallel \mu_2 \}}}$$

Since we have $\forall \langle v_1, v_2 \rangle$, we separately have $\forall v_1$ and $\forall v_2$. For all such v_1 and v_2 , there exists a choice of $\langle v'_1, v'_2 \rangle$, i.e. of two values v'_1 and v'_2 , such that they are in their respective value interpretations. Thus, we can split our assumptions into the following:

1. $\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \rrbracket$
2. $\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \rrbracket$
3. $\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_2 \rrbracket$
4. $\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_2 \rrbracket$

We also have $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$, and that (with the above) is sufficient to show $(\hat{\gamma}(e \cdot i), \hat{\gamma}'(e \cdot i)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_i \rrbracket$.

• **Case: T-INJ-1**

WTS: $(\hat{\gamma}(i \cdot e), \hat{\gamma}'(i \cdot e)) \in \mathcal{E}_{\Sigma}^{\xi} \llbracket (\tau_1 + \tau_2)_{\ell} \rrbracket$

By definition of substitution, we have that $\hat{\gamma}(i \cdot e) = i \cdot \hat{\gamma}(e)$ and $\hat{\gamma}'(i \cdot e) = i \cdot \hat{\gamma}'(e)$.

From the premise, we have $\Gamma; \Sigma \vdash_{\text{kc}} e : \tau_i$ for $i \in \{1, 2\}$.

By the **IH**, we have that $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma}^{\xi} \llbracket \tau_i \rrbracket$.

Suppose we have μ, μ' such that $\mu \equiv_{\xi} \mu' : \Sigma' \uplus \Sigma''$. By the definition of the term interpretation, we have that

- Since $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma}^{\xi} \llbracket \tau_i \rrbracket$,

$$\nu_{\Sigma'} \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V} \parallel \mu_1 \}$$

and

$$\nu_{\Sigma''} \{ \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}' \parallel \mu_2 \}$$

such that $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$ and

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}' \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_i \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V} \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_i \rrbracket$$

By the set-lifted dynamics, we have

$$\frac{\nu_{\Sigma'} \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V} \parallel \mu_1 \}}{\nu_{\Sigma'} \{ i \cdot \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \{ i \cdot v \mid v \in \mathbb{V} \} \parallel \mu_1 \}}$$

$$\frac{\nu_{\Sigma''} \{ \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}' \parallel \mu_2 \}}{\nu_{\Sigma''} \{ i \cdot \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu_{\Sigma_2} \{ \{ i \cdot v' \mid v' \in \mathbb{V}' \} \parallel \mu_2 \}}$$

Define

$$\mathbb{V}_{s1} = \{ i \cdot v \mid v \in \mathbb{V} \}$$

$$\mathbb{V}_{s2} = \{ i \cdot v' \mid v' \in \mathbb{V}' \}$$

To show $(\hat{\gamma}(i \cdot e), \hat{\gamma}'(i \cdot e)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket (\tau_1 + \tau_2)_{\ell} \rrbracket$, we must show that

$$\nu_{\Sigma'} \{ i \cdot \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V}_{s1} \parallel \mu_1 \}$$

$$\nu_{\Sigma''} \{ i \cdot \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}_{s2} \parallel \mu_2 \}$$

with $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$ and

$$\forall v_1 \in \mathbb{V}_{s1}. \exists v_2 \in \mathbb{V}_{s2} \text{ s.t. } (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket (\tau_1 + \tau_2)_{\ell} \rrbracket$$

$$\forall v_2 \in \mathbb{V}_{s2}. \exists v_1 \in \mathbb{V}_{s1} \text{ s.t. } (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket (\tau_1 + \tau_2)_{\ell} \rrbracket$$

We received $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$ from the **IH**.

We proceed by casing on $\ell \sqsubseteq \xi$:

- **Case:** $\ell \sqsubseteq \xi$

To show $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$, by the definition of the value interpretation for labeled types, we must show that

$$(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$$

From the **IH**, we have

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}' \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_i \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V} \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_i \rrbracket$$

Then, we have

$$\forall v_1 \in \mathbb{V}_{s_1}. \exists v_2 \in \mathbb{V}_{s_2} \text{ s.t. } v_1 = i \cdot v, v_2 = i \cdot v', (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_i \rrbracket$$

$$\forall v_2 \in \mathbb{V}_{s_2}. \exists v_1 \in \mathbb{V}_{s_1} \text{ s.t. } v_1 = i \cdot v, v_2 = i \cdot v', (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_i \rrbracket$$

since for all v , we can choose the corresponding v' such that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_i \rrbracket$ (and vice versa).

Then, by the definition of the value interpretation at type $\tau_1 + \tau_2$, we have

$$\forall v_1 \in \mathbb{V}_{s_1}. \exists v_2 \in \mathbb{V}_{s_2} \text{ s.t. } (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$$

$$\forall v_2 \in \mathbb{V}_{s_2}. \exists v_1 \in \mathbb{V}_{s_1} \text{ s.t. } (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$$

- **Case:** $\ell \not\sqsubseteq \xi$

To show $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$, by the definition of the value interpretation for labeled types, we must show that

$$v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_1 + \tau_2 \rrbracket \wedge v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$$

From the **IH**, we have

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}' \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_i \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V} \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_i \rrbracket$$

By Lemma 11, we have that

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_i \rrbracket$$

$$\forall v' \in \mathbb{V}'. v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_i \rrbracket$$

This gives us what we need to show that $i \cdot v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$ and $i \cdot v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$, and thus that $i \cdot v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$ and $i \cdot v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$ by the definition of the unary value interpretation.

• **Case: T-CASE**

T-CASE

$$\frac{\Sigma; \Gamma \vdash_{\text{kc}} e : (\tau_1 + \tau_2)_\ell \quad \Sigma; \Gamma, x_1 : \tau_1 \vdash_{\text{kcl}\ell} e_1 : \tau \quad \Sigma; \Gamma, x_2 : \tau_2 \vdash_{\text{kcl}\ell} e_2 : \tau \quad \ell \triangleleft \tau}{\Sigma; \Gamma \vdash_{\text{kc}} \text{case } e \{ x_1.e_1 \mid x_2.e_2 \} : \tau}$$

WTS: $(\hat{\gamma}(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}), \hat{\gamma}'(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \})) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \tau \rrbracket$

By definition of substitution (upto alpha-equivalence on x_1 and x_2), we have $\hat{\gamma}(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}) = \text{case } \hat{\gamma}(e) \{ x_1.\hat{\gamma}(e_1) \mid x_2.\hat{\gamma}(e_2) \}$ and $\hat{\gamma}'(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}) = \text{case } \hat{\gamma}'(e) \{ x_1.\hat{\gamma}'(e_1) \mid x_2.\hat{\gamma}'(e_2) \}$.

By **IH**, we have

- $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$
- $\forall \Sigma'_1, \Sigma''_1$ s.t. $\Sigma'_1 \leq \Sigma$ and $\Sigma''_1 \leq \Sigma$,
 $\forall \sigma_1, \sigma'_1$ s.t. $\sigma_1 :_{\text{LD}} \Sigma'_1, \sigma'_1 :_{\text{LD}} \Sigma''_1$, and

$$\forall \gamma_1 \in \text{sing}(\sigma_1), \exists \gamma'_1 \in \text{sing}(\sigma'_1). \gamma_1 \equiv_\xi \gamma'_1 : \Gamma, x_1 : \tau_1; (\Sigma'_1 \uplus \Sigma''_1)$$

$$\forall \gamma'_1 \in \text{sing}(\sigma'_1), \exists \gamma_1 \in \text{sing}(\sigma_1). \gamma_1 \equiv_\xi \gamma'_1 : \Gamma, x_1 : \tau_1; (\Sigma'_1 \uplus \Sigma''_1)$$

$$\forall \text{such } (\gamma_1, \gamma'_1) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma'_1). (\hat{\gamma}_1(e_1), \hat{\gamma}'_1(e_1)) \in \mathcal{E}_{\Sigma'_1, \Sigma''_1}^\xi \llbracket \tau \rrbracket$$

- $\forall \Sigma'_2, \Sigma''_2$ s.t. $\Sigma'_2 \leq \Sigma$ and $\Sigma''_2 \leq \Sigma$,
 $\forall \sigma_2, \sigma'_2$ s.t. $\sigma_2 :_{\text{LD}} \Sigma'_2, \sigma'_2 :_{\text{LD}} \Sigma''_2$, and

$$\forall \gamma_2 \in \text{sing}(\sigma_2), \gamma'_2 \in \text{sing}(\sigma'_2). \gamma_2 \equiv_\xi \gamma'_2 : \Gamma, x_2 : \tau_2; (\Sigma'_2 \uplus \Sigma''_2)$$

$$\forall \gamma'_2 \in \text{sing}(\sigma'_2), \gamma_2 \in \text{sing}(\sigma_2). \gamma_2 \equiv_\xi \gamma'_2 : \Gamma, x_2 : \tau_2; (\Sigma'_2 \uplus \Sigma''_2)$$

$$\forall \text{such } (\gamma_2, \gamma'_2) \in \text{sing}(\sigma_2) \times \text{sing}(\sigma'_2). (\hat{\gamma}_2(e_2), \hat{\gamma}'_2(e_2)) \in \mathcal{E}_{\Sigma'_2, \Sigma''_2}^\xi \llbracket \tau \rrbracket$$

Unfolding the term interpretations, we have

- Since $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$,

$$\nu \Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu \Sigma_1 \{ \mathbb{V} \parallel \mu_1 \}$$

and

$$\nu \Sigma'' \{ \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu \Sigma_2 \{ \mathbb{V}' \parallel \mu_2 \}$$

such that $\mu_1 \equiv_\xi \mu_2 : \Sigma_1 \uplus \Sigma_2$ and

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}' \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V} \text{ s.t. } (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$$

- Since $(\hat{\gamma}_1(e_1), \hat{\gamma}'_1(e_1)) \in \mathcal{E}_{\Sigma'_1, \Sigma''_1}^\xi \llbracket \mathcal{T} \rrbracket$, if $\mu'_1 \equiv_\xi \mu''_1 : \Sigma'_1 \uplus \Sigma''_1$, then

$$\nu_{\Sigma'_1} \{ \hat{\gamma}_1(e_1) \parallel \mu'_1 \} \Downarrow \nu_{\Sigma_1^*} \{ \mathbb{V}_1 \parallel \mu_1^* \}$$

and

$$\nu_{\Sigma''_1} \{ \hat{\gamma}'_1(e_1) \parallel \mu''_1 \} \Downarrow \nu_{\Sigma_1^{**}} \{ \mathbb{V}'_1 \parallel \mu_1^{**} \}$$

such that $\mu_1^* \equiv_\xi \mu_1^{**} : \Sigma_1^* \uplus \Sigma_1^{**}$ and

$$\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1^*, \Sigma_1^{**}}^\xi \llbracket \mathcal{T} \rrbracket$$

$$\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1^*, \Sigma_1^{**}}^\xi \llbracket \mathcal{T} \rrbracket$$

- Since $(\hat{\gamma}_2(e_2), \hat{\gamma}'_2(e_2)) \in \mathcal{E}_{\Sigma'_2, \Sigma''_2}^\xi \llbracket \mathcal{T} \rrbracket$, if $\mu'_2 \equiv_\xi \mu''_2 : \Sigma'_2 \uplus \Sigma''_2$, then

$$\nu_{\Sigma'_2} \{ \hat{\gamma}_2(e_2) \parallel \mu'_2 \} \Downarrow \nu_{\Sigma_2^*} \{ \mathbb{V}_2 \parallel \mu_2^* \}$$

and

$$\nu_{\Sigma''_2} \{ \hat{\gamma}'_2(e_2) \parallel \mu''_2 \} \Downarrow \nu_{\Sigma_2^{**}} \{ \mathbb{V}'_2 \parallel \mu_2^{**} \}$$

such that $\mu_2^* \equiv_\xi \mu_2^{**} : \Sigma_2^* \uplus \Sigma_2^{**}$ and

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2^*, \Sigma_2^{**}}^\xi \llbracket \mathcal{T} \rrbracket$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2^*, \Sigma_2^{**}}^\xi \llbracket \mathcal{T} \rrbracket$$

With the above, by Corollary 3 and Lemma 23, we have that $\nu_{\Sigma'} \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V} \parallel \mu_1 \}$ such that $\mathbb{V} \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$, and that $\nu_{\Sigma''} \{ \hat{\gamma}'(e) \parallel \mu \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}' \parallel \mu_2 \}$ such that $\mathbb{V}' \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$.

Since $\mathbb{V} \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$ and $\mathbb{V}' \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$, by the definition of leaf-determinism, we have that

- Either $\mathbb{V} = \{1 \cdot v_{i1} \mid v_{i1} \in \mathbb{V}_{i1}\}$ for $\mathbb{V}_{i1} \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket \tau_1 \rrbracket$ or $\mathbb{V} = \{2 \cdot v_{i2} \mid v_{i2} \in \mathbb{V}_{i2}\}$ for $\mathbb{V}_{i2} \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket \tau_2 \rrbracket$
- Either $\mathbb{V}' = \{1 \cdot v'_{i1} \mid v'_{i1} \in \mathbb{V}'_{i1}\}$ for $\mathbb{V}'_{i1} \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau_1 \rrbracket$ or $\mathbb{V}' = \{2 \cdot v'_{i2} \mid v'_{i2} \in \mathbb{V}'_{i2}\}$ for $\mathbb{V}'_{i2} \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau_2 \rrbracket$

We proceed by casing on whether $\ell \sqsubseteq \xi$:

- $\ell \sqsubseteq \xi$

This means that, according to the **IH**, we have that for each double contained pair in \mathbb{V} and \mathbb{V}' , $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$. By the definition of the binary value interpretation, either both $v = 1 \cdot v_{i1}$ and $v = 1 \cdot v'_{i1}$, or both $v = 2 \cdot v_{i2}$ and $v = 2 \cdot v'_{i2}$, which eliminates two cases from consideration in the leaf-determinism result.

We now proceed by casing on the remaining two cases:

– **All left injections**

We begin by observing that since $\Sigma_1 \leq \Sigma$ and $\Sigma_2 \leq \Sigma$ (Lemma 24).

Consider the extensions $\sigma[x_1 \mapsto \mathbb{V}_{i1}]$ and $\sigma'[x_1 \mapsto \mathbb{V}'_{i1}]$. First, observe that $\sigma[x_1 \mapsto \mathbb{V}_{i1}] :_{\text{LD}} \Gamma, x_1 : \tau_1; \Sigma_1$ and $\sigma'[x_1 \mapsto \mathbb{V}'_{i1}] :_{\text{LD}} \Gamma, x_1 : \tau_1; \Sigma_2$, since the sets are leaf-deterministic at the given signatures (and the rest follow by Lemma 18). Also, note that by definition of **sing**, we have that

$$\text{sing}(\sigma[x_1 \mapsto \mathbb{V}_{i1}]) = \{\gamma[x \mapsto v_{i1}] \mid \gamma \in \text{sing}(\sigma), v_{i1} \in \mathbb{V}_{i1}\}$$

$$\text{sing}(\sigma'[x_1 \mapsto \mathbb{V}'_{i1}]) = \{\gamma'[x \mapsto v'_{i1}] \mid \gamma' \in \text{sing}(\sigma'), v'_{i1} \in \mathbb{V}'_{i1}\}$$

Observe that $\forall \gamma[x_1 \mapsto v_{i1}] \in \text{sing}(\sigma[x_1 \mapsto \mathbb{V}_{i1}])$, $\exists \gamma'_1[x_1 \mapsto v'_{i1}] \in \text{sing}(\sigma'[x_1 \mapsto \mathbb{V}'_{i1}])$, $\gamma[x_1 \mapsto v_{i1}] \equiv_{\xi} \gamma'_1[x_1 \mapsto v'_{i1}] : \Gamma, x_1 : \tau_1; (\Sigma_1 \uplus \Sigma_2)$ (and similarly for $\forall \gamma'_1[x_1 \mapsto v'_{i1}]$, $\exists \gamma[x_1 \mapsto v_{i1}]$) for all $1 \cdot v_{i1} \in \mathbb{V}$ and $1 \cdot v'_{i1} \in \mathbb{V}'$, since we already have $\gamma \equiv_{\xi} \gamma' : \Gamma; (\Sigma' \uplus \Sigma'')$ (which we can extend to $\Sigma_1 \uplus \Sigma_2$ by Lemma 18), and the IH result gives us the $\forall \exists$ pairings for each v_{i1} and v'_{i1} .

Thus, with the **IH** result on the e_1 branch, we have the following steppings:

$$\frac{\frac{\nu \Sigma' \{\hat{\gamma}(e) \parallel \mu\} \Downarrow \nu \Sigma_1 \{\mathbb{V} \parallel \mu_1\}}{(\nu \Sigma_1 \{\widehat{\gamma[x_1 \mapsto v_{i1}]}(e_1) \parallel \mu_1\} \Downarrow \nu \Sigma_1^* \{\mathbb{V}_1^v \parallel \mu_1^*\})_{\forall v \in \mathbb{V}, v=1 \cdot v_{i1}}}}{\nu \Sigma' \{\text{case } \hat{\gamma}(e) \{x_1 \cdot \hat{\gamma}(e_1) \mid x_2 \cdot \hat{\gamma}(e_2)\} \parallel \mu\} \Downarrow \nu \Sigma_1^* \{\bigcup_{v \in \mathbb{V}} \mathbb{V}_1^v \parallel \mu_1^*\}}$$

$$\frac{\frac{\nu \Sigma'' \{\hat{\gamma}'(e) \parallel \mu'\} \Downarrow \nu \Sigma_2 \{\mathbb{V}' \parallel \mu_2\}}{(\nu \Sigma_2 \{\widehat{\gamma'[x_1 \mapsto v'_{i1}]}(e_1) \parallel \mu_2\} \Downarrow \nu \Sigma_2^{**} \{\mathbb{V}_1^{v'} \parallel \mu_2^{**}\})_{\forall v' \in \mathbb{V}', v'=1 \cdot v'_{i1}}}}{\nu \Sigma'' \{\text{case } \hat{\gamma}'(e) \{x_1 \cdot \hat{\gamma}'(e_1) \mid x_2 \cdot \hat{\gamma}'(e_2)\} \parallel \mu'\} \Downarrow \nu \Sigma_2^{**} \{\bigcup_{v' \in \mathbb{V}'} \mathbb{V}_1^{v'} \parallel \mu_2^{**}\}}$$

Since we have the **IH** result for each individual \mathbb{V}_1^v s and $\mathbb{V}_1^{v'}$ s, we also get that we have the result for all the unioned ones, as we can still match up all the original elements together in the joined sets.

Thus, we have that the results of evaluation are in value interpretations $\mathcal{V}_{\Sigma_1^*, \Sigma_2^{**}}^{\xi} \llbracket \tau \rrbracket$, and we have $\mu_1^* \equiv_{\xi} \mu_2^{**} : \Sigma_1^* \uplus \Sigma_2^{**}$ from the IH. Given all of this, we have that the expressions are in $\mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau \rrbracket$.

– **All right injections**

This case is symmetric to the previous.

▪ $\ell \not\sqsubseteq \xi$

First, observe that if $\ell \not\sqsubseteq \xi$, then $\text{kc} \sqcup \ell \not\sqsubseteq \xi$ (Lemma 25). Then, by the Lemma 13, since $\ell \triangleleft \tau$ and $\ell \not\sqsubseteq \xi$, it is sufficient to show that $\hat{\gamma}(\text{case } e \{x_1 \cdot e_1 \mid x_2 \cdot e_2\}) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket \tau \rrbracket [\text{kc} \sqcup \ell]$ and $\hat{\gamma}'(\text{case } e \{x_1 \cdot e_1 \mid x_2 \cdot e_2\}) \in \mathcal{E}_{\Sigma''}^{\xi} \llbracket \tau \rrbracket [\text{kc} \sqcup \ell]$.

Since $\gamma \equiv_{\xi} \gamma' : \Sigma' \uplus \Sigma''$, we also have that $\gamma : \Sigma'$ and $\gamma' : \Sigma''$. The proof goal then follows immediately from the Theorem 3.

• **Case: T-LAM**

WTS: $(\hat{\gamma}(\lambda(x : \tau_1.e)), \hat{\gamma}'(\lambda(x : \tau_1.e))) \in \mathcal{E}_{\Sigma}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$

By definition of substitution (upto alpha-equivalence on x), we have $\hat{\gamma}(\lambda(x : \tau_1.e)) = \lambda(x : \tau_1.\hat{\gamma}(e))$ and $\hat{\gamma}'(\lambda(x : \tau_1.e)) = \lambda(x : \tau_1.\hat{\gamma}'(e))$.

From the premise, we have $\Sigma; \Gamma, x : \tau_1 \vdash_{\ell_k} e : \tau_2$.

By the **IH**, we have for all Σ_1, Σ_2 such that $\Sigma_1 \leq \Sigma$ and $\Sigma_2 \leq \Sigma$, $\forall \sigma_1, \sigma_2$ s.t. $\sigma_1 :_{\text{LD}} \Sigma_1$, $\sigma_2 :_{\text{LD}} \Sigma_2$, and

$$\forall \gamma_1 \in \mathbf{sing}(\sigma_1), \gamma_2 \in \mathbf{sing}(\sigma_2). \gamma_1 \equiv_{\xi} \gamma_2 : \Gamma, x : \tau_1; (\Sigma_1 \uplus \Sigma_2)$$

$$\forall \gamma_2 \in \mathbf{sing}(\sigma_2), \gamma_1 \in \mathbf{sing}(\sigma_1). \gamma_1 \equiv_{\xi} \gamma_2 : \Gamma, x : \tau_1; (\Sigma_1 \uplus \Sigma_2)$$

\forall such $(\gamma_1, \gamma_2) \in \mathbf{sing}(\sigma_1) \times \mathbf{sing}(\sigma_2)$. $(\hat{\gamma}_1(e), \hat{\gamma}_2(e)) \in \mathcal{E}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_2 \rrbracket$.

By the dynamics, we have

$$\overline{\nu \Sigma' \{ \lambda(x : \tau_1.\hat{\gamma}(e)) \parallel \mu \}} \Downarrow \nu \Sigma' \{ \{ \lambda(x : \tau_1.\hat{\gamma}(e)) \} \parallel \mu \}$$

$$\overline{\nu \Sigma'' \{ \lambda(x : \tau_1.\hat{\gamma}'(e)) \parallel \mu' \}} \Downarrow \nu \Sigma'' \{ \{ \lambda(x : \tau_1.\hat{\gamma}'(e)) \} \parallel \mu' \}$$

To show this case, it is sufficient to show that $(\lambda(x : \tau_1.\hat{\gamma}(e)), \lambda(x : \tau_1.\hat{\gamma}'(e))) \in \mathcal{V}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$.

Suppose we have some Σ_1, Σ_2 such that $\Sigma_1 \leq \Sigma'$ and $\Sigma_2 \leq \Sigma''$ and sets $\mathbb{V}_1, \mathbb{V}_2$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket \tau_1 \rrbracket$, $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau_2 \rrbracket$, and $\forall v_1 \in \mathbb{V}_1, \exists v_2 \in \mathbb{V}_2. (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \rrbracket$ and $\forall v_2 \in \mathbb{V}_2, \exists v_1 \in \mathbb{V}_1. (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_1 \rrbracket$. First, observe that $\sigma[x \mapsto \mathbb{V}_1] :_{\text{LD}} \Sigma_1$ and $\sigma'[x \mapsto \mathbb{V}_2] :_{\text{LD}} \Sigma_2$ from all assumptions. Then, note that $\gamma[x \mapsto v_1] \equiv_{\xi} \gamma'[x \mapsto v_2] : \Gamma, x : \tau_1; (\Sigma_1 \uplus \Sigma_2)$, since there exist pairs (v_1, v_2) are in the value interpretation at $\Sigma_1 \uplus \Sigma_2$ for all $v_1 \in \mathbb{V}_1$ and $v_2 \in \mathbb{V}_2$, and the existing values can be extended to the future signature via Lemma 18.

By definition, $\gamma[\widehat{x \mapsto v_1}](e) = [v_1/x]\hat{\gamma}(e)$ and $\gamma'[\widehat{x \mapsto v_2}](e) = [v_2/x]\hat{\gamma}'(e)$, meaning we have that $(\gamma[\widehat{x \mapsto v_1}](e), \gamma'[\widehat{x \mapsto v_2}](e)) \in \mathcal{E}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau_2 \rrbracket$ by the **IH**.

We must also show that $\lambda(x : \tau_1.\hat{\gamma}(e)) \in \mathcal{V}_{\Sigma'}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$ and $\lambda(x : \tau_1.\hat{\gamma}'(e)) \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$. Note that since $\gamma \equiv_{\xi} \gamma' : \Sigma' \uplus \Sigma''$, we have that $\gamma : \Sigma'$ and $\gamma' : \Sigma''$ by Lemma 29. As such, we can apply the Theorem 3 to obtain that $\hat{\gamma}(\lambda(x : \tau_1.e)) \in \mathcal{E}_{\Sigma'} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket [\mathbf{kc}]$ and $\hat{\gamma}'(\lambda(x : \tau_1.e)) \in \mathcal{E}_{\Sigma''} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket [\mathbf{kc}]$.

Since we have $\mu \equiv_{\xi} \mu' : \Sigma' \uplus \Sigma''$, we also have $\mu : \Sigma'$ and $\mu' : \Sigma''$. Unfolding the term interpretations (and excluding any irrelevant parts), we have that

- If $\mu : \Sigma'$, then

$$\nu \Sigma' \{ \lambda(x : \tau_1.\hat{\gamma}(e)) \parallel \mu \} \Downarrow \nu \Sigma_1 \{ \mathbb{V}_1 \parallel \mu_1 \}$$

such that $\mu_1 : \Sigma_1$ and

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$$

▪ If $\mu' : \Sigma''$, then

$$\nu \Sigma'' \{ \lambda(x : \tau_1. \hat{\gamma}'(e)) \parallel \mu' \} \Downarrow \nu \Sigma_2 \{ \mathbb{V}_2 \parallel \mu_2 \}$$

such that $\mu_2 : \Sigma_2$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$$

By rule induction on the stepping judgments, the only non-vacuous case is that where

$$\mathbb{V}_1 = \{ \lambda(x : \tau_1. \hat{\gamma}(e)) \} \text{ and } \mathbb{V}_2 = \{ \lambda(x : \tau_1. \hat{\gamma}'(e)) \}$$

as well as $\Sigma_1 = \Sigma'$ and $\Sigma_2 = \Sigma''$. This means that we have $\lambda(x : \tau_1. \hat{\gamma}(e)) \in \mathcal{V}_{\Sigma'}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$ and $\lambda(x : \tau_1. \hat{\gamma}'(e)) \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$, which is what we want to show.

• **Case: T-APP**

$$\frac{\text{T-APP} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \tau_1 \xrightarrow{\ell_k} \tau_2 \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau_1 \quad \text{kc} \sqsubseteq \ell_k}{\Sigma; \Gamma \vdash_{\text{kc}} e_1(e_2) : \tau_2}$$

WTS: $(\hat{\gamma}(e_1(e_2)), \hat{\gamma}'(e_1(e_2))) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_2 \rrbracket$

By definition of substitution, we have $\hat{\gamma}(e_1(e_2)) = \hat{\gamma}(e_1)(\hat{\gamma}(e_2))$ and $\hat{\gamma}'(e_1(e_2)) = \hat{\gamma}'(e_1)(\hat{\gamma}'(e_2))$.

By the **IH**, we have that $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$ and $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_1 \rrbracket$.

Suppose we have μ, μ' such that $\mu \equiv_{\xi} \mu' : \Sigma' \uplus \Sigma''$. By the definition of the term interpretation, we have that

▪ Since $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$,

$$\nu \Sigma' \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu \Sigma_1 \{ \mathbb{V}_1 \parallel \mu_1 \}$$

and

$$\nu \Sigma'' \{ \hat{\gamma}'(e_1) \parallel \mu' \} \Downarrow \nu \Sigma'_1 \{ \mathbb{V}'_1 \parallel \mu'_1 \}$$

such that $\mu_1 \equiv_{\xi} \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and

$$\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$$

$$\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^{\xi} \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$$

▪ Since $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket \tau_1 \rrbracket$,

$$\nu \Sigma' \{ \hat{\gamma}(e_2) \parallel \mu \} \Downarrow \nu \Sigma_2 \{ \mathbb{V}_2 \parallel \mu_2 \}$$

and

$$\nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma'_2\{\mathbb{V}'_2 \parallel \mu'_2\}$$

such that $\mu_2 \equiv_\xi \mu'_2 : \Sigma_2 \uplus \Sigma'_2$ and

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$$

From the **IH**, we have that

$$\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$$

$$\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1 \text{ s.t. } (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$$

Unfolding the definition, this means that for all $\Sigma_1^*, \Sigma_1^{**}$ such that $\Sigma_1^* \leq \Sigma_1$ and $\Sigma_1^{**} \leq \Sigma_1'$ and for all $\mathbb{V}_i \in \mathcal{L}\mathcal{V}_{\Sigma_i^*} \llbracket \tau_1 \rrbracket, \mathbb{V}'_i \in \mathcal{L}\mathcal{V}_{\Sigma_i^{**}} \llbracket \tau_1 \rrbracket$ with $\forall (v_i, v'_i) \in \mathbb{V}_i \times \mathbb{V}'_i, (v_i, v'_i) \in \mathcal{V}_{\Sigma_1^*, \Sigma_1^{**}}^\xi \llbracket \tau_1 \rrbracket$, we have that $([v_i/x]e_1, [v'_i/x]e'_1) \in \mathcal{E}_{\Sigma_1^*, \Sigma_1^{**}}^\xi \llbracket \tau_2 \rrbracket$ for $v_1 = \lambda(x : \tau_1. e)$ and $v'_1 = \lambda(x : \tau_1. e'_1)$. Observe that this requires all elements in \mathbb{V}_1 and \mathbb{V}'_1 to be lambdas.

From the **IH**, we also have

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2 \text{ s.t. } (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$$

By Corollary 3 and Lemma 23, we have that $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_{\Sigma_2} \llbracket \tau_1 \rrbracket$ and $\mathcal{L}\mathcal{V}_{\Sigma'_2} \llbracket \tau_1 \rrbracket$.

By Lemma 16, we have that they are all in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$, since $\Sigma_1 \cup \Sigma_2 \leq \Sigma_2$ and $\Sigma'_1 \cup \Sigma'_2 \leq \Sigma'_2$. We also have that $\Sigma_1 \cup \Sigma_2 \leq \Sigma_1$ and $\Sigma'_1 \cup \Sigma'_2 \leq \Sigma'_1$, which means that, for each pair $(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2$ and $(v'_1, v'_2) \in \mathbb{V}'_1 \times \mathbb{V}'_2$, we have

$$\forall v_1, v_2. \exists v'_1, v'_2. ([v_2/x]e_1, [v'_2/x]e'_1) \in \mathcal{E}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket \text{ with } v_1 = \lambda(x : \tau_1. e_1), v'_1 = \lambda(x : \tau_1. e'_1)$$

$$\forall v'_1, v'_2. \exists v_1, v_2. ([v_2/x]e_1, [v'_2/x]e'_1) \in \mathcal{E}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket \text{ with } v_1 = \lambda(x : \tau_1. e_1), v'_1 = \lambda(x : \tau_1. e'_1)$$

(for each v_1, v_2 , we chose the corresponding v'_1 and v'_2 which is in the binary value interpretation, and vice versa).

From the **IHs** and Lemma 20, we have that $\mu_1 \cup \mu_2 \equiv_\xi \mu'_1 \cup \mu'_2 : (\Sigma_1 \cup \Sigma_2) \uplus (\Sigma'_1 \cup \Sigma'_2)$. Unfolding the definition of the term interpretation, we have that

- Since $([v_2/x]e_1, [v'_2/x]e'_1) \in \mathcal{E}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket$,

$$\nu\Sigma_1 \cup \Sigma_2 \{ [v_2/x]e_1 \parallel \mu_1 \cup \mu_2 \} \Downarrow \nu\Sigma^* \{ \mathbb{V} \parallel \mu^* \}$$

$$\nu\Sigma'_1 \cup \Sigma'_2 \{ [v'_2/x]e'_1 \parallel \mu'_1 \cup \mu'_2 \} \Downarrow \nu\Sigma^{**} \{ \mathbb{V} \parallel \mu^{**} \}$$

such that $\mu^* \equiv_\xi \mu^{**} : \Sigma^* \uplus \Sigma^{**}$ and

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}'. (v, v') \in \mathcal{V}_{\Sigma^*, \Sigma^{**}}^\xi \llbracket \tau_2 \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V}. (v, v') \in \mathcal{V}_{\Sigma^*, \Sigma^{**}}^\xi \llbracket \tau_2 \rrbracket$$

Given all of these, we are able to apply the following set-lifted dynamics rules:

$$\frac{\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\} \quad \nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}}{(\nu\Sigma_1 \cup \Sigma_2\{[v_2/x]e_1 \parallel \mu_1 \cup \mu_2\} \Downarrow \nu\Sigma^*\{\mathbb{V}^{v_1, v_2} \parallel \mu^*\})_{v_1=\lambda(x:\tau_1.e_1)}} \\ \nu\Sigma'\{\hat{\gamma}(e_1)(\hat{\gamma}(e_2)) \parallel \mu\} \Downarrow \nu\Sigma^*\left\{ \bigcup_{(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2} \mathbb{V}^{v_1, v_2} \parallel \mu^* \right\}$$

$$\frac{\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu'\} \Downarrow \nu\Sigma'_1\{\mathbb{V}'_1 \parallel \mu'_1\} \quad \nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma'_2\{\mathbb{V}'_2 \parallel \mu'_2\}}{(\nu\Sigma'_1 \cup \Sigma'_2\{[v'_2/x]e'_1 \parallel \mu'_1 \cup \mu'_2\} \Downarrow \nu\Sigma^{**}\{\mathbb{V}^{v'_1, v'_2} \parallel \mu^{**}\})_{v'_1=\lambda(x:\tau_1.e'_1)}} \\ \nu\Sigma''\{\hat{\gamma}'(e_1)(\hat{\gamma}'(e_2)) \parallel \mu\} \Downarrow \nu\Sigma^{**}\left\{ \bigcup_{(v'_1, v'_2) \in \mathbb{V}'_1 \times \mathbb{V}'_2} \mathbb{V}^{v'_1, v'_2} \parallel \mu^{**} \right\}$$

Ultimately, what we need to show is that $\forall v \in \bigcup_{(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2} \mathbb{V}^{v_1, v_2}. \exists v' \in \bigcup_{(v'_1, v'_2) \in \mathbb{V}'_1 \times \mathbb{V}'_2} \mathbb{V}^{v'_1, v'_2}. (v, v') \in \mathcal{V}_{\Sigma^*, \Sigma^{**}}^\xi[\tau_2]$. Note that the sets \mathbb{V}^{v_1, v_2} and $\mathbb{V}^{v'_1, v'_2}$ are exactly the sets \mathbb{V} and \mathbb{V}' (respectively) that we got from unfolding the term interpretation on $([v_2/x]e_1, [v'_2/x]e'_1)$, so this holds immediately, and continues to hold when we take the union of each of these sets, since we can still match up the original pairs in the new joint sets.

• **Case: T-ENC-MOBILE**

$$\frac{\text{ENC-MOBILE} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau \quad \tau \blacktriangleleft \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{encrypt}_\ell(e_1; e_2) : (\text{enc}_\ell \tau)_\perp}$$

WTS: $(\hat{\gamma}(\text{encrypt}_\ell(e_1; e_2)), \hat{\gamma}'(\text{encrypt}_\ell(e_1; e_2))) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi[(\text{enc}_\ell \tau)_\perp]$

By definition of substitution, we have $\hat{\gamma}(\text{encrypt}_\ell(e_1; e_2)) = \text{encrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2))$ and $\hat{\gamma}'(\text{encrypt}_\ell(e_1; e_2)) = \text{encrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2))$.

By **IH**, we have

- $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi[\text{key}_\ell]$
- $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi[\tau]$

Suppose we have μ, μ' such that $\mu \equiv_\xi \mu' : \Sigma' \uplus \Sigma''$. By the definition of the term interpretation, we have that

- Since $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi[\text{key}_\ell]$,

$$\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$$

$$\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu'\} \Downarrow \nu\Sigma'_1\{\mathbb{V}'_1 \parallel \mu'_1\}$$

such that $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and

$$\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi[\text{key}_\ell]$$

$$\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi[\text{key}_\ell]$$

- Since $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_\Sigma^\xi[\tau]$,

$$\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}$$

$$\nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma_2'\{\mathbb{V}'_2 \parallel \mu'_2\}$$

such that $\mu_2 \equiv_\xi \mu'_2 : \Sigma_2 \uplus \Sigma_2'$ and

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma_2'}^\xi[\tau]$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma_2'}^\xi[\tau]$$

With the above, by Corollary 3 and Lemma 23, we have that $\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\text{key}_\ell]$, and we have that $\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1'\{\mathbb{V}'_1 \parallel \mu'_1\}$ such that $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1'}[\text{key}_\ell]$.

Unfolding the definition of leaf-determinism, this means that $\mathbb{V}_1 = \{\text{key}\langle K \rangle\}$ and $\mathbb{V}'_1 = \{\text{key}\langle K' \rangle\}$ for some $K \sim \ell \in \Sigma_1, K' \sim \ell \in \Sigma_1'$. From the **IH** result, this must mean that $(\text{key}\langle K \rangle, \text{key}\langle K' \rangle) \in \mathcal{V}_{\Sigma_1, \Sigma_1'}^\xi[\text{key}_\ell]$.

Since $K \sim \ell \in \Sigma_1$ and $K' \sim \ell \in \Sigma_1'$, then the signatures must be of the form $\Sigma_1 = \Sigma_1^*, K \sim \ell$ and $\Sigma_1' = \Sigma_1'^*, K' \sim \ell$. Additionally, since we have $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma_1'$, by definition, it must be the case that $\mu_1 = \mu_1^* \otimes K \hookrightarrow v_k$ and $\mu'_1 = \mu_1'^* \otimes K' \hookrightarrow v'_k$.

With all of that, we can then apply the following set-lifted dynamics rule, after defining the set \mathbb{U} in the required manner:

$$\frac{\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell \{ \{\text{key}\langle K \rangle\} \parallel \mu_1^* \otimes K \hookrightarrow v_k \}}{\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\} \quad \mathbb{U} = \{u \mid v \in \mathbb{V}_2, u \in \mathcal{E}_\ell(v_k, v)\}}{\nu\Sigma'\{\text{encrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2)) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\mathbb{U} \parallel \mu_1 \cup \mu_2\}}$$

$$\frac{\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu'\} \Downarrow \nu\Sigma_1'^*, K' \sim \ell \{ \{\text{key}\langle K' \rangle\} \parallel \mu_1'^* \otimes K' \hookrightarrow v'_k \}}{\nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma_2'\{\mathbb{V}'_2 \parallel \mu'_2\} \quad \mathbb{U}' = \{u' \mid v' \in \mathbb{V}'_2, u' \in \mathcal{E}_\ell(v'_k, v')\}}{\nu\Sigma''\{\text{encrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2)) \parallel \mu'\} \Downarrow \nu\Sigma_1' \cup \Sigma_2'\{\mathbb{U}' \parallel \mu'_1 \cup \mu'_2\}}$$

Since the label of $(\text{enc}_\ell \tau)_\perp$ is \perp (and thus it must be that $\perp \sqsubseteq \xi$), it is sufficient to show that

$$\forall u \in \mathbb{U}. \exists u' \in \mathbb{U}'. (u, u') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma_1' \cup \Sigma_2'}^\xi[\text{enc}_\ell \tau]$$

$$\forall u' \in \mathbb{U}'. \exists u \in \mathbb{U}. (u, u') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma_1' \cup \Sigma_2'}^\xi[\text{enc}_\ell \tau]$$

First, we need to show that $\exists v, v_k. v = \mathcal{D}(v_k, u)$ and $\exists v', v'_k. v' = \mathcal{D}(v'_k, u')$. By set construction, we know that each $u \in \mathbb{U}$ is the product of $\mathcal{E}_\ell(v_k, v)$ for $v \in \mathbb{V}_2$, and similarly we know that each $u' \in \mathbb{U}'$ is the product of $\mathcal{E}_\ell(v'_k, v')$, so we can take v, v_k and v', v'_k to be such values by the definition of the encryption scheme (decryption is deterministic).

We proceed by casing on whether $\ell \sqsubseteq \xi$:

- $\ell \sqsubseteq \xi$:

This means that we must show that $v_k = v'_k$ and $(v, v') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$.

For the first proof goal, since $\ell \sqsubseteq \xi$ and $(\text{key}_Y \langle K \rangle, \text{key}_Y \langle K' \rangle) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \text{key}_Y \ell \rrbracket$, we have that $K = K'$. Since we also have that $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$, we have that $\mu_1(K) = \mu'_1(K')$, meaning that the corresponding values v_k and v'_k are equal.

For the second proof goal, we have from the **IH** that each double contained pair of values (v, v') is in $\mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau \rrbracket$. By Lemma 16, we have that they are in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$.

- $\ell \not\sqsubseteq \xi$:

This means that we must show that each $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \rrbracket$, $v' \in \mathcal{V}_{\Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$, and $u \doteq u'$.

For the first two proof goals, we have from the **IH** that each double contained pair of values (v, v') is in $\mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau \rrbracket$. By Lemma 16, we have that they are in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$, and by Lemma 11, we have that individually $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \rrbracket$ and $v' \in \mathcal{V}_{\Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$.

By Equation 1 in Definition 3, we have that for each $u \in \mathcal{E}_\ell(v_k, v)$, there exists $u' \in \mathcal{E}_\ell(v'_k, v')$ such that $u \doteq u'$. Thus, when showing that $\forall u \in \mathbb{U}. \exists u' \in \mathbb{U}. (u, u') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket$, we choose the u' for each u that satisfies the above property, giving us that $u \doteq u'$ (and vice versa).

• **Case: T-ENC-STATIC**

$$\frac{\text{T-ENC-STATIC} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau \quad \tau \blacktriangleleft \ell' \quad \ell' \not\sqsubseteq \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{encrypt}_\ell(e_1; e_2) : (\text{enc}_\ell \tau)_{\ell'}}$$

WTS: $(\hat{\gamma}(\text{encrypt}_\ell(e_1; e_2)), \hat{\gamma}'(\text{encrypt}_\ell(e_1; e_2))) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket (\text{enc}_\ell \tau)_{\ell'} \rrbracket$

By definition of substitution, we have $\hat{\gamma}(\text{encrypt}_\ell(e_1; e_2)) = \text{encrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2))$ and $\hat{\gamma}'(\text{encrypt}_\ell(e_1; e_2)) = \text{encrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2))$.

By **IH**, we have

- $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \text{key}_\ell \rrbracket$
- $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \tau \rrbracket$

Suppose we have μ, μ' such that $\mu \equiv_\xi \mu' : \Sigma' \uplus \Sigma''$. By the definition of the term interpretation, we have that

- Since $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \text{key}_\ell \rrbracket$,

$$\nu \Sigma' \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu \Sigma_1 \{ \mathbb{V}_1 \parallel \mu_1 \}$$

$$\nu \Sigma'' \{ \hat{\gamma}'(e_1) \parallel \mu' \} \Downarrow \nu \Sigma'_1 \{ \mathbb{V}'_1 \parallel \mu'_1 \}$$

such that $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and

$$\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \text{key}_\ell \rrbracket$$

$$\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi[\text{key}_\ell]$$

- Since $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_\Sigma^\xi[\tau]$,

$$\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}$$

$$\nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma'_2\{\mathbb{V}'_2 \parallel \mu'_2\}$$

such that $\mu_2 \equiv_\xi \mu'_2 : \Sigma_2 \uplus \Sigma'_2$ and

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi[\tau]$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi[\tau]$$

With the above, by Corollary 3 and Lemma 23, we have that $\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\text{key}_\ell]$, and we have that $\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu\} \Downarrow \nu\Sigma'_1\{\mathbb{V}'_1 \parallel \mu'_1\}$ such that $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\text{key}_\ell]$.

Unfolding the definition of leaf-determinism, this means that $\mathbb{V}_1 = \{\text{key}\langle K \rangle\}$ and $\mathbb{V}'_1 = \{\text{key}\langle K' \rangle\}$ for some $K \sim \ell \in \Sigma_1, K' \sim \ell \in \Sigma'_1$. From the **IH** result, this must mean that $(\text{key}\langle K \rangle, \text{key}\langle K' \rangle) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi[\text{key}_\ell]$.

Since $K \sim \ell \in \Sigma_1$ and $K' \sim \ell \in \Sigma'_1$, then the signatures must be of the form $\Sigma_1 = \Sigma_1^*, K \sim \ell$ and $\Sigma'_1 = \Sigma_1^*, K' \sim \ell$. Additionally, since we have $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$, by definition, it must be the case that $\mu_1 = \mu_1^* \otimes K \hookrightarrow v_k$ and $\mu'_1 = \mu_1^* \otimes K' \hookrightarrow v'_k$.

With all of that, we can then apply the following set-lifted dynamics rule, after defining the set \mathbb{U} in the required manner:

$$\frac{\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell \{ \{\text{key}\langle K \rangle\} \parallel \mu_1^* \otimes K \hookrightarrow v_k \}}{\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\} \quad \mathbb{U} = \{u \mid v \in \mathbb{V}_2, u \in \mathcal{E}_\ell(v_k, v)\}}{\nu\Sigma'\{\text{encrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2)) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\mathbb{U} \parallel \mu_1 \cup \mu_2\}}$$

$$\frac{\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu'\} \Downarrow \nu\Sigma_1^*, K' \sim \ell \{ \{\text{key}\langle K' \rangle\} \parallel \mu_1^* \otimes K' \hookrightarrow v'_k \}}{\nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma'_2\{\mathbb{V}'_2 \parallel \mu'_2\} \quad \mathbb{U}' = \{u' \mid v' \in \mathbb{V}'_2, u' \in \mathcal{E}_\ell(v'_k, v')\}}{\nu\Sigma''\{\text{encrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2)) \parallel \mu\} \Downarrow \nu\Sigma'_1 \cup \Sigma'_2\{\mathbb{U}' \parallel \mu'_1 \cup \mu'_2\}}$$

We proceed by casing on whether $\ell' \sqsubseteq \xi$:

- $\ell' \sqsubseteq \xi$:

In this case, we must show that

$$\forall u \in \mathbb{U}. \exists u' \in \mathbb{U}'. (u, u') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi[\text{enc}_\ell \tau]$$

$$\forall u' \in \mathbb{U}'. \exists u \in \mathbb{U}. (u, u') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi[\text{enc}_\ell \tau]$$

First, we need to show that $\exists v, v_k. v = \mathcal{D}(v_k, u)$ and $\exists v', v'_k. v' = \mathcal{D}(v'_k, u')$. By set construction, we know that each $u \in \mathbb{U}$ is the product of $\mathcal{E}_\ell(v_k, v)$ for $v \in \mathbb{V}_2$, and

similarly we know that each $u' \in \mathbb{U}'$ is the product of $\mathcal{E}_\ell(v'_k, v')$, so we can take v, v_k and v', v'_k to be such values by the definition of the encryption scheme (decryption is deterministic)..

We proceed by casing on whether $\ell \sqsubseteq \xi$:

– $\ell \sqsubseteq \xi$:

This means that we must show that $v_k = v'_k$ and $(v, v') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$.

For the first proof goal, since $\ell \sqsubseteq \xi$ and $(\text{key}_Y \langle K \rangle, \text{key}_Y \langle K' \rangle) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \text{key}_Y \ell \rrbracket$, we have that $K = K'$. Since we also have that $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$, we have that $\mu_1(K) = \mu'_1(K')$, meaning that the corresponding values v_k and v'_k are equal.

For the second proof goal, we have from the **IH** that each double contained pair of values (v, v') is in $\mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau \rrbracket$. By Lemma 16, we have that they are in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$.

– $\ell \not\sqsubseteq \xi$:

This means that we must show that each $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \rrbracket$, $v' \in \mathcal{V}_{\Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$, and $u \doteq u'$.

For the first two proof goals, we have from the **IH** that each double contained pair of values (v, v') is in $\mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau \rrbracket$. By Lemma 16, we have that they are in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$, and by Lemma 11, we have that individually $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \rrbracket$ and $v' \in \mathcal{V}_{\Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$.

By Equation 1 in Definition 3, we have that for each $u \in \mathcal{E}_\ell(v_k, v)$, there exists $u' \in \mathcal{E}_\ell(v'_k, v')$ such that $u \doteq u'$. Thus, when showing that $\forall u \in \mathbb{U}. \exists u' \in \mathbb{U}'. (u, u') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket$, we choose the u' for each u that satisfies the above property, giving us that $u \doteq u'$ (and vice versa).

▪ $\ell' \not\sqsubseteq \xi$:

In this case, it's sufficient to show

$$\begin{aligned} \forall u \in \mathbb{U}. u \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket \\ \forall u' \in \mathbb{U}'. u' \in \mathcal{V}_{\Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket \end{aligned}$$

The only obligation left to show for this is that $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \rrbracket$ and $v' \in \mathcal{V}_{\Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \rrbracket$, which follows from the **IH** (to get that they are binary-related), Lemma 11, and Lemma 15.

• **Case: T-DEC**

$$\frac{\text{T-DEC} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : (\text{enc}_\ell \tau)_\epsilon}{\Sigma; \Gamma \vdash_{\text{kc}} \text{decrypt}_\ell(e_1; e_2) : \tau \text{ result}_\epsilon}$$

WTS: $(\hat{\gamma}(\text{decrypt}_\ell(e_1; e_2)), \hat{\gamma}'(\text{decrypt}_\ell(e_1; e_2))) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \tau \text{ result}_\ell \rrbracket$

By definition of substitution, we have $\hat{\gamma}(\text{decrypt}_\ell(e_1; e_2)) = \text{decrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2))$ and $\hat{\gamma}'(\text{decrypt}_\ell(e_1; e_2)) = \text{decrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2))$.

By **IH**, we have

- $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \text{key}_\ell \rrbracket$
- $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket (\text{enc}_\ell \tau)_\ell \rrbracket$

Suppose we have μ, μ' such that $\mu \equiv_\xi \mu' : \Sigma' \uplus \Sigma''$. By the definition of the term interpretation, we have that

- Since $(\hat{\gamma}(e_1), \hat{\gamma}'(e_1)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \text{key}_\ell \rrbracket$,

$$\nu_{\Sigma'} \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V}_1 \parallel \mu_1 \}$$

$$\nu_{\Sigma''} \{ \hat{\gamma}'(e_1) \parallel \mu' \} \Downarrow \nu_{\Sigma'_1} \{ \mathbb{V}'_1 \parallel \mu'_1 \}$$

such that $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and

$$\forall v_1 \in \mathbb{V}_1. \exists v'_1 \in \mathbb{V}'_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \text{key}_\ell \rrbracket$$

$$\forall v'_1 \in \mathbb{V}'_1. \exists v_1 \in \mathbb{V}_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \text{key}_\ell \rrbracket$$

- Since $(\hat{\gamma}(e_2), \hat{\gamma}'(e_2)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket (\text{enc}_\ell \tau)_\ell \rrbracket$,

$$\nu_{\Sigma'} \{ \hat{\gamma}(e_2) \parallel \mu \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}_2 \parallel \mu_2 \}$$

$$\nu_{\Sigma''} \{ \hat{\gamma}'(e_2) \parallel \mu' \} \Downarrow \nu_{\Sigma'_2} \{ \mathbb{V}'_2 \parallel \mu'_2 \}$$

such that $\mu_2 \equiv_\xi \mu'_2 : \Sigma_2 \uplus \Sigma'_2$ and

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket (\text{enc}_\ell \tau)_\ell \rrbracket$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket (\text{enc}_\ell \tau)_\ell \rrbracket$$

With the above, by Corollary 3 and Lemma 23, we have that $\nu_{\Sigma'} \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V}_1 \parallel \mu_1 \}$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1} \llbracket \text{key}_\ell \rrbracket$, and we have that $\nu_{\Sigma''} \{ \hat{\gamma}'(e_1) \parallel \mu' \} \Downarrow \nu_{\Sigma'_1} \{ \mathbb{V}'_1 \parallel \mu'_1 \}$ such that $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1} \llbracket \text{key}_\ell \rrbracket$.

Unfolding the definition of leaf-determinism, this means that $\mathbb{V}_1 = \{ \text{key} \langle K \rangle \}$ and $\mathbb{V}'_1 = \{ \text{key} \langle K' \rangle \}$ for some $K \sim \ell \in \Sigma_1, K' \sim \ell \in \Sigma'_1$. From the **IH** result, this must mean that $(\text{key} \langle K \rangle, \text{key} \langle K' \rangle) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \text{key}_\ell \rrbracket$.

Since $K \sim \ell \in \Sigma_1$ and $K' \sim \ell \in \Sigma'_1$, then the signatures must be of the form $\Sigma_1 = \Sigma_1^*, K \sim \ell$ and $\Sigma'_1 = \Sigma_1'^*, K' \sim \ell$. Additionally, since we have $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$, by definition, it must be the case that $\mu_1 = \mu_1^* \otimes K \hookrightarrow v_k$ and $\mu'_1 = \mu_1'^* \otimes K' \hookrightarrow v'_k$.

We proceed by casing on whether $\epsilon \sqsubseteq \xi$:

- $\epsilon \sqsubseteq \xi$:

In this case, we have that

$$\begin{aligned} \forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket \\ \forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket \end{aligned}$$

By the definition of the binary value interpretation, this means that, for each pair (v_2, v'_2) , we have

- $\exists k, p. p = \mathcal{D}(k, v_2)$
- $\exists k', p'. p' = \mathcal{D}(k', v'_2)$

By Corollary 3 and Lemma 23, we have that $\nu \Sigma' \{ \hat{\gamma}(e_2) \parallel \mu \} \Downarrow \nu \Sigma_2 \{ \mathbb{V}_2 \parallel \mu_2 \}$ such that $\mathbb{V}_2 \in \mathcal{L} \mathcal{V}_{\Sigma_2} \llbracket (\text{enc}_\ell \tau)_\epsilon \rrbracket$, and we have that $\nu \Sigma'' \{ \hat{\gamma}'(e_2) \parallel \mu' \} \Downarrow \nu \Sigma'_2 \{ \mathbb{V}'_2 \parallel \mu'_2 \}$ such that $\mathbb{V}'_2 \in \mathcal{L} \mathcal{V}_{\Sigma'_2} \llbracket (\text{enc}_\ell \tau)_\epsilon \rrbracket$.

Unfolding the definition of leaf-determinism, this means that

$$\begin{aligned} \forall v_2 \in \mathbb{V}_2, v_2 \in \mathcal{E}_\ell(k, p) \\ \forall v'_2 \in \mathbb{V}'_2, v'_2 \in \mathcal{E}_\ell(k', p') \end{aligned}$$

Since decryption is deterministic, it must be that the k, k', p, p' are the same ones obtained in the binary value interpretation.

We proceed by casing on whether $\ell \sqsubseteq \xi$:

- $\ell \sqsubseteq \xi$:

This means that $k = k'$ and $(p, p') \in \mathcal{V}_{\Sigma_2, \Sigma'_2}^\xi \llbracket \tau \rrbracket$.

Similarly, since $\ell \sqsubseteq \xi$ and $(\text{key}\langle K \rangle, \text{key}\langle K' \rangle) \in \mathcal{V}_{\Sigma_1, \Sigma'_1}^\xi \llbracket \text{key}_\ell \rrbracket$, we have that $K = K'$. Since we also have that $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$, we have that $\mu_1(K) = \mu'_1(K')$, meaning that the corresponding values v_k and v'_k are equal.

We case on whether $k = v_k$. That is, whether the key used to decrypt the ciphertexts is the same as the one used to encrypt them:

$$\star \quad k = v_k$$

If this is the case, then it must be that $\forall v_2 \in \mathbb{V}_2. \mathcal{D}(k, v_2) = p$ and $\forall v'_2 \in \mathbb{V}'_2. \mathcal{D}(k, v'_2) = p'$.

This means that we can apply the following set-lifted dynamics rule:

$$\frac{\begin{array}{l} \nu \Sigma' \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu \Sigma_1^*, K \sim \ell \{ \{ \text{key}\langle K \rangle \} \parallel \mu_1^* \otimes K \leftrightarrow v_k \} \\ \nu \Sigma' \{ \hat{\gamma}(e_2) \parallel \mu \} \Downarrow \nu \Sigma_2 \{ \mathbb{V}_2 \parallel \mu_2 \} \quad \mathbb{V} = \{ \mathcal{D}(v_k, v_2) \mid v_2 \in \mathbb{V}_2 \} \end{array}}{\nu \Sigma' \{ \text{decrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2)) \parallel \mu \} \Downarrow \nu \Sigma_1 \cup \Sigma_2 \{ \{ \text{Ok}(p) \mid p \in \mathbb{V} \} \parallel \mu_1 \cup \mu_2 \}}$$

$$\frac{\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1^*, K' \sim \ell\{\{\text{key}\langle K'\rangle\} \parallel \mu'_1 \otimes K' \hookrightarrow v'_k\}}{\nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2'\{\mathbb{V}'_2 \parallel \mu'_2\} \quad \mathbb{V}' = \{\mathcal{D}(v'_k, v'_2) \mid v'_2 \in \mathbb{V}'_2\}} \nu\Sigma''\{\text{decrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2)) \parallel \mu\} \Downarrow \nu\Sigma_1' \cup \Sigma_2'\{\{\text{Ok}(p') \mid p' \in \mathbb{V}'\} \parallel \mu'_1 \cup \mu'_2\}$$

All that's left to show is that

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}'. (v, v') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma_1' \cup \Sigma_2'}^\xi \llbracket \tau \text{ result}_\epsilon \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V}. (v, v') \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma_1' \cup \Sigma_2'}^\xi \llbracket \tau \text{ result}_\epsilon \rrbracket$$

Since $\epsilon \sqsubseteq \xi$ and $\ell \sqsubseteq \xi$, this mean that $\epsilon \sqcup \ell \sqsubseteq \xi$ (Lemma 26), this means we need to show each double contained pair is in the binary value interpretation at $\mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma_1' \cup \Sigma_2'}^\xi \llbracket \tau \text{ result} \rrbracket$. This should follow from the fact that $(p, p') \in \mathcal{V}_{\Sigma_2, \Sigma_2'}^\xi \llbracket \tau \rrbracket$ and Lemma 16.

★ $k \neq v_k$

In this case, it must be that $\mathcal{D}(k, v_2) = \perp$ and $\mathcal{D}(k, v'_2) = \perp$ for all $v_2 \in \mathbb{V}_2$ and $v'_2 \in \mathbb{V}'_2$.

This means that we can apply the following set-lifted dynamics rule:

$$\frac{\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell\{\{\text{key}\langle K\rangle\} \parallel \mu^* \otimes K \hookrightarrow v_k\}}{\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\} \quad (\mathcal{D}(v_k, v_2) = \perp)_{v_2 \in \mathbb{V}_2}} \nu\Sigma'\{\text{decrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2)) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\{\text{Error}\} \parallel \mu_1 \cup \mu_2\}$$

$$\frac{\nu\Sigma''\{\hat{\gamma}'(e_1) \parallel \mu'\} \Downarrow \nu\Sigma_1^*, K' \sim \ell\{\{\text{key}\langle K'\rangle\} \parallel \mu_1^* \otimes K' \hookrightarrow v'_k\}}{\nu\Sigma''\{\hat{\gamma}'(e_2) \parallel \mu'\} \Downarrow \nu\Sigma_2'\{\mathbb{V}'_2 \parallel \mu'_2\} \quad (\mathcal{D}(v'_k, v'_2) = \perp)_{v'_2 \in \mathbb{V}'_2}} \nu\Sigma''\{\text{decrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2)) \parallel \mu\} \Downarrow \nu\Sigma_1' \cup \Sigma_2'\{\{\text{Error}\} \parallel \mu'_1 \cup \mu'_2\}$$

We immediately have that $(\text{Error}, \text{Error}) \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2, \Sigma_1' \cup \Sigma_2'}^\xi \llbracket \tau \text{ result}_{\epsilon \cup \ell} \rrbracket$.

○ $\ell \not\sqsubseteq \xi$:

This means that $p \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau \rrbracket$, $p' \in \mathcal{V}_{\Sigma_2'}^\xi \llbracket \tau \rrbracket$, and $v_2 \doteq v'_2$.

Observe that if $\epsilon \sqsubseteq \xi$ and $\ell \not\sqsubseteq \xi$, then $\epsilon \sqcup \ell \not\sqsubseteq \xi$ (Lemma 26). This means that for any sets \mathbb{V}, \mathbb{V}' which result from the stepping of $\text{decrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2))$ and $\text{decrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2))$, respectively, we only need to show that

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \text{ result} \rrbracket$$

$$\forall v' \in \mathbb{V}'. v' \in \mathcal{V}_{\Sigma_1' \cup \Sigma_2'}^\xi \llbracket \tau \text{ result} \rrbracket$$

This follows by the Theorem 3 on $\hat{\gamma}(\text{decrypt}_\ell(e_1; e_2))$ and $\hat{\gamma}'(\text{decrypt}_\ell(e_1; e_2))$.

- $\epsilon \not\sqsubseteq \xi$:

In this case, we have that

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket$$

$$\forall v'_2 \in \mathbb{V}'_2. v'_2 \in \mathcal{V}_{\Sigma'_2}^\xi \llbracket \text{enc}_\ell \tau \rrbracket$$

Since $\epsilon \not\sqsubseteq \xi$, then for all ℓ , it must also be that $\epsilon \sqcup \ell \not\sqsubseteq \xi$ (Lemma 25). This means that for any sets \mathbb{V}, \mathbb{V}' which result from the stepping of $\text{decrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2))$ and $\text{decrypt}_\ell(\hat{\gamma}'(e_1); \hat{\gamma}'(e_2))$, respectively, we only need to show that

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \text{ result} \rrbracket$$

$$\forall v' \in \mathbb{V}'. v' \in \mathcal{V}_{\Sigma'_1 \cup \Sigma'_2}^\xi \llbracket \tau \text{ result} \rrbracket$$

This follows by the Theorem 3 on $\hat{\gamma}(\text{decrypt}_\ell(e_1; e_2))$ and $\hat{\gamma}'(\text{decrypt}_\ell(e_1; e_2))$.

- **Case: T-KEY-GEN**

$$\frac{\text{T-KEY-GEN} \quad \text{kc} \sqsubseteq \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{gen}\langle \ell \rangle : \tau}$$

$$\text{WTS: } (\hat{\gamma}(\text{gen}\langle \ell \rangle), \hat{\gamma}'(\text{gen}\langle \ell \rangle)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi \llbracket \tau \rrbracket$$

By definition of substitution, we have $\hat{\gamma}(\text{gen}\langle \ell \rangle) = \text{gen}\langle \ell \rangle$ and $\hat{\gamma}'(\text{gen}\langle \ell \rangle) = \text{gen}\langle \ell \rangle$.

Suppose we have μ, μ' such that $\mu \equiv_\xi \mu' : \Sigma' \uplus \Sigma''$, and suppose we have $(\mathcal{G}_1, \mathcal{K}_1) \equiv_\xi (\mathcal{G}_2, \mathcal{K}_2)$. By the dynamics, we have

$$\frac{\mathcal{G}_1 = \mathcal{G}'_1[\ell \mapsto v_k :: v_k s] \quad \mathcal{K}_1 = \mathcal{K}'_1[\ell \mapsto K :: K s]}{(\mathcal{G}_1, \mathcal{K}_1, \nu \Sigma' \{ \text{gen}\langle \ell \rangle \parallel \mu \}) \Downarrow (\mathcal{G}'_1[\ell \mapsto v_k s], \mathcal{K}'_1[\ell \mapsto K s], \nu \Sigma', K \sim \ell \{ \{ \text{key}\langle K \rangle \} \parallel \mu \otimes K \hookrightarrow v_k \})}$$

$$\frac{\mathcal{G}_2 = \mathcal{G}'_2[\ell \mapsto v'_k :: v'_k s'] \quad \mathcal{K}_1 = \mathcal{K}'_2[\ell \mapsto K' :: K' s']}{(\mathcal{G}_2, \mathcal{K}_2, \nu \Sigma'' \{ \text{gen}\langle \ell \rangle \parallel \mu' \}) \Downarrow (\mathcal{G}'_2[\ell \mapsto v'_k s'], \mathcal{K}'_2[\ell \mapsto K' s'], \nu \Sigma'', K' \sim \ell \{ \{ \text{key}\langle K' \rangle \} \parallel \mu' \otimes K' \hookrightarrow v'_k \})}$$

To show this case, we need to show that $(\text{key}\langle K \rangle, \text{key}\langle K' \rangle) \in \mathcal{V}_{(\Sigma', K \sim \ell), (\Sigma'', K' \sim \ell)} \llbracket \text{key}_\ell \rrbracket$ and that $(\mu \otimes K \hookrightarrow v_k) \equiv_\xi (\mu' \otimes K' \hookrightarrow v'_k) : (\Sigma', K \sim \ell) \uplus (\Sigma'', K' \sim \ell)$.

We proceed by casing on whether $\ell \sqsubseteq \xi$:

- $\ell \sqsubseteq \xi$:

Since we had $(\mathcal{G}_1, \mathcal{K}_1) \equiv_\xi (\mathcal{G}_2, \mathcal{K}_2)$, we know that $v_k = v'_k, v_k s \approx v'_k s', K = K',$ and $K s \approx K' s'.$

The fact that $K = K'$ gives us immediately what we want to show for the value interpretation.

For the memory compliance, we must show that $(\mu \otimes K \hookrightarrow v_k)(K) = (\mu' \otimes K' \hookrightarrow v'_k)(K')$, which is also immediate by the respective memory contents at K (since the symbols are equal) being v_k (since the key values are equal).

We also have that $(\mathcal{G}'_1[\ell \mapsto v_k s], \mathcal{K}_1[\ell \mapsto K s]) \equiv_\xi (\mathcal{G}'_2[\ell \mapsto v_k s'], \mathcal{K}'_2[\ell \mapsto K s'])$ since $v_k s \approx v_k s'$ and $K s \approx K s'$.

- $\ell \not\sqsubseteq \xi$:

In this case, it's sufficient to show that $\text{key}\langle K \rangle \in \mathcal{V}_{\Sigma', K \sim \ell}[\text{key}_\ell]$ and $\text{key}\langle K' \rangle \in \mathcal{V}_{\Sigma'', K' \sim \ell}[\text{key}_\ell]$. This holds immediately by the definition of the unary value interpretation.

For the memory compliance, since the keys are unobservable, we only need to show that the keys are in memory, which is immediate by the structure of the memory.

Similarly, since the keys are unobservable, we have that the resultant $(\mathcal{G}'_1[\ell \mapsto v_k s], \mathcal{K}'_1[\ell \mapsto K s])$ and $(\mathcal{G}'_2[\ell \mapsto v_k s'], \mathcal{K}'_2[\ell \mapsto K s'])$ stream maps are trivially related.

- **T-KEY-ACCESS**

WTS: $(\hat{\gamma}(\text{key}\langle K \rangle), \hat{\gamma}'(\text{key}\langle K \rangle)) \in \mathcal{E}_{\Sigma', \Sigma''}^\xi[\text{key}_\ell]$

Note that in this case, $\Sigma' \leq \Sigma, K \sim \ell$ and $\Sigma'' \leq \Sigma, K \sim \ell$, since that is the current signature. Since they're in the future, by definition, they must be of the form $\Sigma' = \Sigma^*, K \sim \ell$ and $\Sigma'' = \Sigma^{**}, K \sim \ell$.

Suppose we have $\mu \equiv_\xi \mu' : \Sigma' \uplus \Sigma''$. Given this, it must be the case that $\mu = \mu^* \otimes K \hookrightarrow v_k$ and $\mu' = \mu^{**} \otimes K \hookrightarrow v'_k$.

From the dynamics, we then have

$$\overline{\nu\Sigma^*, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu^* \otimes K \hookrightarrow v_k\} \Downarrow \nu\Sigma^*, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu^* \otimes K \hookrightarrow v_k\}}$$

$$\overline{\nu\Sigma^{**}, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu^{**} \otimes K \hookrightarrow v'_k\} \Downarrow \nu\Sigma^{**}, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu^{**} \otimes K \hookrightarrow v'_k\}}$$

It suffices to show that $(\text{key}\langle K \rangle, \text{key}\langle K \rangle) \in \mathcal{V}_{(\Sigma^*, K \sim \ell), (\Sigma^{**}, K \sim \ell)}^\xi[\text{key}_\ell]$. We proceed by casing on whether $\ell \sqsubseteq \xi$:

- $\ell \sqsubseteq \xi$:

In this case, we must show $K = K$, which is immediate.

- $\ell \not\sqsubseteq \xi$:

In this case, it's sufficient to show that $\text{key}\langle K \rangle \in \mathcal{V}_{\Sigma^*, K \sim \ell}[\text{key}_\ell]$ and $\text{key}\langle K \rangle \in \mathcal{V}_{\Sigma^{**}, K \sim \ell}[\text{key}_\ell]$. This holds immediately by the definition of the unary value interpretation.

- **Case: T-SUB**

$$\frac{\text{T-SUB} \quad \Sigma; \Gamma \vdash_{\text{kc}'} e : \tau' \quad \text{kc} \sqsubseteq \text{kc}' \quad \tau' \leq \tau}{\Sigma; \Gamma \vdash_{\text{kc}} e : \tau}$$

WTS: $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau \rrbracket$

From the **IH**, we have that $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau' \rrbracket$.

Suppose we have $\mu \equiv_{\xi} \mu' : \Sigma' \uplus \Sigma''$. Unfolding the term interpretation, this means that

- Since $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau' \rrbracket$,

$$\nu_{\Sigma'} \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V} \parallel \mu_1 \}$$

$$\nu_{\Sigma''} \{ \hat{\gamma}'(e) \parallel \mu' \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}' \parallel \mu_2 \}$$

such that $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$ and

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}'. (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V}. (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau \rrbracket$$

By Lemma 31, since

$$\forall v \in \mathbb{V}. \exists v' \in \mathbb{V}'. (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau' \rrbracket$$

$$\forall v' \in \mathbb{V}'. \exists v \in \mathbb{V}. (v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau' \rrbracket$$

, we have the above double containment for $\mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi} \llbracket \tau \rrbracket$, which allows us to show that $(\hat{\gamma}(e), \hat{\gamma}'(e)) \in \mathcal{E}_{\Sigma', \Sigma''}^{\xi} \llbracket \tau \rrbracket$.

- **Omitted:** nat, resMatch, ok, err

A.3 Proof of Unary FTLR

Suppose Σ' such that $\Sigma' \leq \Sigma$, and σ such that $\sigma :_{\text{LD}} \Gamma; \Sigma'$ and $\forall \gamma \in \text{sing}(\sigma). \gamma : \Gamma; \Sigma'$.

Suppose we have an arbitrary such γ . We proceed by rule induction on the typing judgment:

- **Case: T-PROD**

WTS: $\hat{\gamma} \langle e_1, e_2 \rangle \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket \tau_1 \times \tau_2 \rrbracket [\text{kc}]$

By definition of substitution, we have that $\hat{\gamma} \langle e_1, e_2 \rangle = \langle \hat{\gamma}(e_1), \hat{\gamma}(e_2) \rangle$.

From the premises, we have $\Gamma; \Sigma \vdash_{\text{kc}} e_1 : \tau_1$ and $\Gamma; \Sigma \vdash_{\text{kc}} e_2 : \tau_2$.

By the **IH**, we have that $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket \tau_1 \rrbracket [\text{kc}]$ and $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket \tau_2 \rrbracket [\text{kc}]$.

Suppose we have μ such that $\mu : \Sigma'$. By the definition of the term interpretation, we have that

- Since $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_1]][\mathbf{kc}]$,

$$\nu_{\Sigma'}\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu_{\Sigma_1}\{\mathbb{V}_1 \parallel \mu_1\}$$

such that $\mu_1 : \Sigma_1$ and

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}^{\xi}[[\tau_1]]$$

and $\forall K_1 \sim \ell_1 \in (\Sigma_1 \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell_1$

- Since $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_2]][\mathbf{kc}]$,

$$\nu_{\Sigma'}\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu_{\Sigma_2}\{\mathbb{V}_2 \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}^{\xi}[[\tau_2]]$$

and $\forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell_2$

By the set-lifted dynamics rules, we have

$$\frac{\nu_{\Sigma'}\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu_{\Sigma_1}\{\mathbb{V}_1 \parallel \mu_1\} \quad \nu_{\Sigma'}\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu_{\Sigma_2}\{\mathbb{V}_2 \parallel \mu_2\}}{\nu_{\Sigma'}\{\langle \hat{\gamma}(e_1), \hat{\gamma}(e_2) \rangle \parallel \mu\} \Downarrow \nu_{\Sigma_1 \cup \Sigma_2}\{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\} \parallel \mu_1 \cup \mu_2\}}$$

Define

$$\mathbb{V}_p = \{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\}$$

- By Lemma 15, since $\Sigma_1 \cup \Sigma_2 \leq \Sigma_1$ (Lemma 21), we have

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[[\tau_1]]$$

Similarly, via Lemma 15, we have that

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[[\tau_2]]$$

With both of these assumptions, we have that

$$\forall \langle v_1, v_2 \rangle \in \mathbb{V}_p. \langle v_1, v_2 \rangle \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[[\tau_1 \times \tau_2]]$$

- Since we have $\mu_1 : \Sigma_1$ and $\mu_2 : \Sigma_2$, we have that $\mu_1 \cup \mu_2 : \Sigma_1 \cup \Sigma_2$ (Lemma 19).
- Since we have $\forall K_1 \sim \ell_1 \in (\Sigma_1 \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell_1$ and $\forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell_2$, then we have that

$$\forall k \sim \ell \in ((\Sigma_1 \cup \Sigma_2) \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell$$

since the elements of $(\Sigma_1 \cup \Sigma_2) \setminus \Sigma'$ are exactly the elements in $\Sigma_1 \setminus \Sigma'$ and $\Sigma_2 \setminus \Sigma'$ by definition of union and difference.

- Since we have all of the above, we have that $(\hat{\gamma}\langle e_1, e_2 \rangle) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_1 \times \tau_2]]$.

• **Case: T-PROJ-I**

WTS: $\hat{\gamma}(e \cdot i) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_i]][\mathbf{kc}]$ for $i \in \{1, 2\}$

By definition of substitution, we have that $\hat{\gamma}(e \cdot i) = \hat{\gamma}(e) \cdot i$.

From the premise, we have $\Gamma; \Sigma \vdash_{\mathbf{kc}} e : \tau_1 \times \tau_2$.

By the **IH**, we have that $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_1 \times \tau_2]][\mathbf{kc}]$.

Suppose we have μ such that $\mu : \Sigma'$. By the definition of the term interpretation, we have that

- Since $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_1 \times \tau_2]][\mathbf{kc}]$,

$$\nu\Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu\Sigma'' \{ \mathbb{V} \parallel \mu' \}$$

such that $\mu' : \Sigma''$ and

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma''}^{\xi}[[\tau_1 \times \tau_2]]$$

and $\forall K \sim \ell \in (\Sigma'' \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell$.

From the **IH**, unfolding the definition of the value interpretation at $\tau_1 \times \tau_2$, we have

$$\forall v \in \mathbb{V}. v = \langle v_1, v_2 \rangle, v_1 \in \mathcal{V}_{\Sigma''}^{\xi}[[\tau_1]] \wedge v_2 \in \mathcal{V}_{\Sigma''}^{\xi}[[\tau_2]]$$

By the set-lifted dynamics rules, we have

$$\frac{\nu\Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu\Sigma'' \{ \mathbb{V} \parallel \mu' \}}{\nu\Sigma' \{ \hat{\gamma}(e) \cdot i \parallel \mu \} \Downarrow \nu\Sigma'' \{ \{ v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}, i \in \{1, 2\} \} \parallel \mu' \}}$$

Since we have $\forall \langle v_1, v_2 \rangle$, we separately have $\forall v_1$ and $\forall v_2$. Thus, we can split our assumptions into the following:

1. $\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma''}^{\xi}[[\tau_1]]$
2. $\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma''}^{\xi}[[\tau_2]]$

We also have $\mu' : \Sigma''$ and $\forall K \sim \ell \in (\Sigma'' \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell$ from the **IH**, and that (with the above) is sufficient to show $\hat{\gamma}(e \cdot i) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_i]][\mathbf{kc}]$.

• **Case: T-INJ-I**

WTS: $\hat{\gamma}(i \cdot e) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_1 + \tau_2]_{\ell}][\mathbf{kc}]$

By definition of substitution, we have that $\hat{\gamma}(i \cdot e) = i \cdot \hat{\gamma}(e)$.

From the premise, we have $\Gamma; \Sigma \vdash_{\mathbf{kc}} e : \tau_i$ for $i \in \{1, 2\}$.

By the **IH**, we have that $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_i]][\mathbf{kc}]$.

Suppose we have μ such that $\mu : \Sigma'$. By the definition of the term interpretation, we have that

- Since $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^{\xi}[[\tau_i]][\mathbf{kc}]$,

$$\nu\Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu\Sigma'' \{ \mathbb{V} \parallel \mu' \}$$

such that $\mu' : \Sigma''$ and

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket \tau_i \rrbracket$$

and $\forall K \sim \ell' \in (\Sigma'' \setminus \Sigma'). \text{kc} \sqsubseteq \ell'$.

By the set-lifted dynamics, we have

$$\frac{\nu\Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu\Sigma'' \{ \mathbb{V} \parallel \mu' \}}{\nu\Sigma' \{ i \cdot \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu\Sigma'' \{ \{ i \cdot v \mid v \in \mathbb{V} \} \parallel \mu' \}}$$

Define

$$\mathbb{V}_s = \{ i \cdot v \mid v \in \mathbb{V} \}$$

To show $\hat{\gamma}(i \cdot e) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket (\tau_1 + \tau_2)_{\ell} \rrbracket [\text{kc}]$, we must show that

$$\nu\Sigma' \{ i \cdot \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu\Sigma'' \{ \mathbb{V}_s \parallel \mu' \}$$

with $\mu' : \Sigma''$ and

$$\forall v_s \in \mathbb{V}_s. v_s \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket (\tau_1 + \tau_2)_{\ell} \rrbracket$$

and $\forall K \sim \ell' \in (\Sigma'' \setminus \Sigma'). \text{kc} \sqsubseteq \ell'$

We received $\mu' : \Sigma''$ and the condition on effects from the **IH**.

According to the unary logical relation, to show a value $v \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket t_{\ell} \rrbracket$, it is sufficient to show that $v \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket t \rrbracket$.

From the **IH**, we have

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket \tau_i \rrbracket$$

Then, we have

$$\forall v_s \in \mathbb{V}_s. v_s = i \cdot v, v \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket \tau_i \rrbracket$$

Then, by the definition of the value interpretation at type $\tau_1 + \tau_2$, we have

$$\forall v_s \in \mathbb{V}_s. v_s \in \mathcal{V}_{\Sigma''}^{\xi} \llbracket \tau_1 + \tau_2 \rrbracket$$

• **Case: T-CASE**

T-CASE

$$\frac{\begin{array}{c} \Sigma; \Gamma \vdash_{\text{kc}} e : (\tau_1 + \tau_2)_{\ell} \\ \Sigma; \Gamma, x_1 : \tau_1 \vdash_{\text{kc} \sqcup \ell} e_1 : \tau \quad \Sigma; \Gamma, x_2 : \tau_2 \vdash_{\text{kc} \sqcup \ell} e_2 : \tau \quad \ell \triangleleft \tau \end{array}}{\Sigma; \Gamma \vdash_{\text{kc}} \text{case } e \{ x_1.e_1 \mid x_2.e_2 \} : \tau}$$

WTS: $\hat{\gamma}(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket \tau \rrbracket [\text{kc}]$

By definition of substitution (upto alpha-equivalence on x_1 and x_2), we have $\hat{\gamma}(\text{case } e \{ x_1.e_1 \mid x_2.e_2 \}) = \text{case } \hat{\gamma}(e) \{ x_1.\hat{\gamma}(e_1) \mid x_2.\hat{\gamma}(e_2) \}$.

By **IH**, we have

$$\begin{array}{l} \blacksquare \hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^{\xi} \llbracket (\tau_1 + \tau_2)_{\ell} \rrbracket [\text{kc}] \end{array}$$

- $\forall \Sigma_1, \Sigma_1 \leq \Sigma, \forall \sigma_1$ such that $\sigma_1 :_{\text{LD}} \Gamma, x_1 : \tau_1; \Sigma_1$ and $\forall \gamma_1 \in \mathbf{sing}(\sigma_1). \gamma_1 : \Gamma, x_1 : \tau_1; \Sigma_1,$
 $\forall \gamma_1 \in \mathbf{sing}(\sigma_1), \hat{\gamma}_1(e_1) \in \mathcal{E}_\Sigma^\xi \llbracket \tau \rrbracket [\mathbf{kc} \sqcup \ell].$
- $\forall \Sigma_2, \Sigma_2 \leq \Sigma, \forall \sigma_2$ such that $\sigma_2 :_{\text{LD}} \Gamma, x_2 : \tau_2; \Sigma_2$ and $\forall \gamma_2 \in \mathbf{sing}(\sigma_2). \gamma_2 : \Gamma, x_2 : \tau_2; \Sigma_2,$
 $\forall \gamma_2 \in \mathbf{sing}(\sigma_2), \hat{\gamma}_2(e_2) \in \mathcal{E}_\Sigma^\xi \llbracket \tau \rrbracket [\mathbf{kc} \sqcup \ell].$

Unfolding the term interpretations, we have

- Since $\hat{\gamma}(e) \in \mathcal{E}_\Sigma^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket [\mathbf{kc}],$

$$\nu \Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu \Sigma'' \{ \mathbb{V} \parallel \mu' \}$$

such that $\mu' : \Sigma''$ and

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma''}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$$

and $\forall K \sim \ell' \in (\Sigma'' \setminus \Sigma'). \mathbf{kc} \sqsubseteq \ell'.$

- Since $\hat{\gamma}_1(e_1) \in \mathcal{E}_\Sigma^\xi \llbracket \tau \rrbracket [\mathbf{kc} \sqcup \ell],$ if *isOf* * $\mu_1 \Sigma_1,$ then

$$\nu \Sigma_1 \{ \hat{\gamma}_1(e_1) \parallel \mu_1 \} \Downarrow \nu \Sigma'_1 \{ \mathbb{V}_1 \parallel \mu'_1 \}$$

such that $\mu'_1 : \Sigma'_1$ and

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma'_1}^\xi \llbracket \tau \rrbracket$$

and $\forall K_1 \sim \ell_1 \in (\Sigma'_1 \setminus \Sigma_1). \mathbf{kc} \sqcup \ell \sqsubseteq \ell_1.$

- Since $\hat{\gamma}_2(e_2) \in \mathcal{E}_\Sigma^\xi \llbracket \tau \rrbracket [\mathbf{kc} \sqcup \ell],$ if $\mu_2 : \Sigma_2,$ then

$$\nu \Sigma_2 \{ \hat{\gamma}_2(e_2) \parallel \mu_2 \} \Downarrow \nu \Sigma'_2 \{ \mathbb{V}_2 \parallel \mu'_2 \}$$

such that $\mu'_2 : \Sigma'_2$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma'_2}^\xi \llbracket \tau \rrbracket$$

and $\forall K_2 \sim \ell_2 \in (\Sigma'_2 \setminus \Sigma_2). \mathbf{kc} \sqcup \ell \sqsubseteq \ell_2.$

By Corollary 2 and Lemma 23, we have that $\nu \Sigma' \{ \hat{\gamma}(e) \parallel \mu \} \Downarrow \nu \Sigma'' \{ \mathbb{V} \parallel \mu' \}$ such that $\mathbb{V} \in \mathcal{L} \mathcal{V}_{\Sigma''} \llbracket (\tau_1 + \tau_2)_\ell \rrbracket.$

Unfolding the definition of leaf-determinism, this means that either $\mathbb{V} = \{ 1 \cdot v_{i1} \mid v_{i1} \in \mathbb{V}_{i1} \}$ with $\mathbb{V}_{i1} \in \mathcal{L} \mathcal{V}_{\Sigma''} \llbracket \tau_1 \rrbracket$ or $\mathbb{V} = \{ 2 \cdot v_{i2} \mid v_{i2} \in \mathbb{V}_{i2} \}$ with $\mathbb{V}_{i2} \in \mathcal{L} \mathcal{V}_{\Sigma''} \llbracket \tau_2 \rrbracket.$

We proceed by casing on these two possibilities:

- $\mathbb{V} = \{ 1 \cdot v_{i1} \mid v_{i1} \in \mathbb{V}_{i1} \}$

Consider the extension $\sigma[x_1 \mapsto \mathbb{V}_{i1}].$ First, observe that $\sigma[x_1 \mapsto \mathbb{V}_{i1}] :_{\text{LD}} \Gamma, x_1 : \tau_1; \Sigma'',$ since $\mathbb{V}_{i1} \in \mathcal{L} \mathcal{V}_{\Sigma''} \llbracket \tau_1 \rrbracket$ (and the signature of all other values in the map can be extended by Lemma 17). Then, by definition of $\mathbf{sing}(\sigma[x_1 \mapsto \mathbb{V}_{i1}]),$ we have

$$\mathbf{sing}(\sigma[x_1 \mapsto \mathbb{V}_{i1}]) = \{ \gamma[x_1 \mapsto v_{i1}] \mid \gamma \in \mathbf{sing}(\sigma), v_{i1} \in \mathbb{V}_{i1} \}$$

First, observe that $\forall \gamma[x_1 \mapsto v_{i1}] \in \mathbf{sing}(\sigma[x_1 \mapsto \mathbb{V}_{i1}]). \gamma[x_1 \mapsto v_{i1}] : \Gamma, x_1 : \tau_1; \Sigma''$ for all $1 \cdot v_1 \in \mathbb{V}$ due to **IH** (and existing values can be extended to future signature by Lemma 17).

Then, according to the **IH** (since $\Sigma'' \leq \Sigma$) and set-lifted dynamics, we have the following:

$$\frac{\nu\Sigma'\{\hat{\gamma}(e) \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V} \parallel \mu'\} \quad (\nu\Sigma''\{\widehat{\gamma[x_1 \mapsto v_{i1}]}(e_1) \parallel \mu'\} \Downarrow \nu\Sigma'_1\{\mathbb{V}^v \parallel \mu'_1\})_{\forall v \in \mathbb{V}, v=1 \cdot v_{i1}}}{\nu\Sigma'\{\text{case } \hat{\gamma}(e) \{x_1 \cdot \hat{\gamma}(e_1) \mid x_2 \cdot \hat{\gamma}(e_2)\} \parallel \mu\} \Downarrow \nu\Sigma'_1\{\bigcup_{v \in \mathbb{V}} \mathbb{V}_1^v \parallel \mu'_1\}}$$

Since we have the **IH** result for each individual \mathbb{V}_1^v , we also get that we have the result for all the unioned ones.

Thus, we have that the results of evaluation are in value interpretations $\mathcal{V}_{\Sigma'_1}^\xi \llbracket \tau \rrbracket$.

By the **IH**, we have that $\forall K \sim \ell' \in (\Sigma'' \setminus \Sigma')$. $\text{kc} \sqsubseteq \ell'$ and $\forall K_1 \sim \ell_1 \in (\Sigma'_1 \setminus \Sigma'')$. $\text{kc} \sqcup \ell \sqsubseteq \ell_1$.

We would like to show that $\forall K'_1 \sim \ell'_1 \in (\Sigma'_1 \setminus \Sigma')$. $\text{kc} \sqsubseteq \ell'_1$. Since $\Sigma'_1 \leq \Sigma''$, observe that the set $\Sigma'_1 \setminus \Sigma'$ is equal to $(\Sigma'' \setminus \Sigma') \cup (\Sigma'_1 \setminus \Sigma'')$ (Lemma 22). We then have $\text{kc} \sqsubseteq \ell'_1$, immediately for $K'_1 \sim \ell'_1 \in (\Sigma'' \setminus \Sigma')$, and otherwise, we have that $\text{kc} \sqcup \ell \sqsubseteq \ell'_1$ implies $\text{kc} \sqsubseteq \ell'_1$ (Lemma 27).

Given all of this, we have that the expressions are in $\mathcal{E}_{\Sigma'}^\xi \llbracket \tau \rrbracket [\text{kc}]$.

- $\forall v \in \mathbb{V}, v = 2 \cdot v_2$

This case is symmetric.

• **Case: T-LAM**

WTS: $\hat{\gamma}(\lambda(x : \tau_1 \cdot e)) \in \mathcal{E}_{\Sigma'}^\xi \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket [\text{kc}]$

By definition of substitution (upto alpha-equivalence on x), we have $\hat{\gamma}(\lambda(x : \tau_1 \cdot e)) = \lambda(x : \tau_1 \cdot \hat{\gamma}(e))$.

From the premise, we have $\Sigma; \Gamma, x : \tau_1 \vdash_{\ell_k} e : \tau_2$.

By the **IH**, we have $\forall \Sigma_1, \Sigma_1 \leq \Sigma, \forall \sigma_1$ such that $\sigma_1 :_{\text{LD}} \Gamma, x : \tau_1; \Sigma_1$ and $\forall \gamma_1 \in \mathbf{sing}(\sigma_1)$. $\gamma_1 : \Gamma, x : \tau_1; \Sigma_1$,

$\forall \gamma_1 \in \mathbf{sing}(\sigma_1)$. $\hat{\gamma}_1(e) \in \mathcal{E}_{\Sigma_1}^\xi \llbracket \tau_2 \rrbracket [\ell_k]$.

By the dynamics, we have

$$\overline{\nu\Sigma'\{\lambda(x : \tau_1 \cdot \hat{\gamma}(e)) \parallel \mu\} \Downarrow \nu\Sigma'\{\{\lambda(x : \tau_1 \cdot \hat{\gamma}(e))\} \parallel \mu\}}$$

To show this case, it is sufficient to show that $\lambda(x : \tau_1 \cdot \hat{\gamma}(e)) \in \mathcal{V}_{\Sigma'}^\xi \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$.

Suppose we have some Σ_1 such that $\Sigma_1 \leq \Sigma$ and set \mathbb{V}_1 such that $\forall v_1 \in \mathbb{V}_1$. $v_1 \in \mathcal{V}_{\Sigma_1} \llbracket \tau_1 \rrbracket$. First, observe that $\sigma[x \mapsto \mathbb{V}_1] :_{\text{LD}} \Sigma_1$ by all assumptions. By the definition of **sing**, we have that

$$\mathbf{sing}(\sigma[x \mapsto \mathbb{V}_1]) = \{\gamma[x \mapsto v_1] \mid \gamma \in \mathbf{sing}(\sigma), v_1 \in \mathbb{V}_1\}$$

Then, observe that $\gamma[x \mapsto v_1] : \Gamma, x : \tau_1; \Sigma_1$, since $\gamma : \Sigma_1$ for all $\gamma \in \mathbf{sing}(\sigma)$ (extended to Σ_1 by Lemma 17) and each $v_1 \in \mathcal{V}_{\Sigma_1} \llbracket \tau_1 \rrbracket$.

By definition, $\gamma[\widehat{x \mapsto v_1}](e) = [v_1/x]\hat{\gamma}(e)$, meaning we have that $\gamma[\widehat{x \mapsto v_1}](e) \in \mathcal{E}_{\Sigma_1}^\xi[[\tau_2]][\ell_k]$ by the **IH**.

We must also show that $\forall K \sim \ell \in (\Sigma' \setminus \Sigma)$. $\text{kc} \sqsubseteq \ell$. Since $\Sigma' \setminus \Sigma = \emptyset$, this holds vacuously.

- **Case: T-APP**

$$\frac{\text{T-APP} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \tau_1 \xrightarrow{\ell_k} \tau_2 \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau_1 \quad \text{kc} \sqsubseteq \ell_k}{\Sigma; \Gamma \vdash_{\text{kc}} e_1(e_2) : \tau_2}$$

WTS: $\hat{\gamma}(e_1(e_2)) \in \mathcal{E}_{\Sigma'}^\xi[[\tau_2]][\text{kc}]$

By definition of substitution, we have $\hat{\gamma}(e_1(e_2)) = \hat{\gamma}(e_1)(\hat{\gamma}(e_2))$.

By **IH**, we have

- $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^\xi[[\tau_1 \xrightarrow{\ell_k} \tau_2]][\text{kc}]$
- $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma'}^\xi[[\tau_1]][\text{kc}]$

Unfolding the term interpretations, we have

- Since $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^\xi[[\tau_1 \xrightarrow{\ell_k} \tau_2]][\text{kc}]$,

$$\nu_{\Sigma'}\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu_{\Sigma_1}\{\mathbb{V}_1 \parallel \mu_1\}$$

such that $\mu_1 : \Sigma_1$ and

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}^\xi[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$$

and $\forall K_1 \sim \ell_1 \in (\Sigma_1 \setminus \Sigma)$. $\text{kc} \sqsubseteq \ell_1$

- Since $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma'}^\xi[[\tau_1]][\text{kc}]$, we have that exists Σ_2 such that $\Sigma_2 \leq \Sigma$. Then, we have

$$\nu_{\Sigma'}\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu_{\Sigma_2}\{\mathbb{V}_2 \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}^\xi[[\tau_1]]$$

and $\forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma)$. $\text{kc} \sqsubseteq \ell_2$

From the **IH**, we have that $\forall v_1 \in \mathbb{V}_1, v_1 \in \mathcal{V}_{\Sigma_1}^\xi[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$. Unfolding the definition, this means that for all Σ'_1 such that $\Sigma'_1 \leq \Sigma_1$ and for all $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[[\tau_1]]$ with $\forall v_1 \in \mathbb{V}_1, v_1 \in \mathcal{V}_{\Sigma'_1}^\xi[[\tau_1]]$, we have that $[v_1/x]e \in \mathcal{E}_{\Sigma'_1}^\xi[[\tau_2]][\ell_k]$ for $v_1 = \lambda(x : \tau_1.e)$.

From the **IH**, we also have $\forall v_2 \in \mathbb{V}_2, v_2 \in \mathcal{V}_{\Sigma_2}^\xi[[\tau_1]]$. By Corollary 2 and Lemma 23, we have that $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_{\Sigma_1}[[\tau_1]]$. By Lemma 15, we have that they are all in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi[[\tau_1]]$ (and $\mathcal{L}\mathcal{V}_{\Sigma_1 \cup \Sigma_2}[[\tau_1]]$), since $\Sigma_1 \cup \Sigma_2 \leq \Sigma_2$. We also have that $\Sigma_1 \cup \Sigma_2 \leq \Sigma_1$, which means that, for each pair $(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2$, we have

$$[v_2/x]e \in \mathcal{E}_{\Sigma_1 \cup \Sigma_2}^\xi[[\tau_2]][\ell_k] \text{ with each } v_1 = \lambda(x : \tau_1.e)$$

From the **IHs** and Lemma 19, we have that $\mu_1 \cup \mu_2 : \Sigma_1 \cup \Sigma_2$. Unfolding the definition of the term interpretation, we have that

- Since $[v_2/x]e \in \mathcal{E}_{\Sigma_1 \cup \Sigma_2}^\xi[[\tau_2]][\ell_k]$,

$$\nu_{\Sigma_1 \cup \Sigma_2} \{ [v_2/x]e \parallel \mu_1 \cup \mu_2 \} \Downarrow \nu_{\Sigma^*} \{ \mathbb{V} \parallel \mu^* \}$$

such that $\mu^* : \Sigma^*$ and

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma^*}^\xi[[\tau_2]]$$

and $\forall K \sim \ell \in (\Sigma^* \setminus (\Sigma_1 \cup \Sigma_2)). \ell_k \sqsubseteq \ell$

Given all of these, we are able to apply the following set-lifted dynamics rule:

$$\frac{\nu_{\Sigma'} \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V}_1 \parallel \mu_1 \} \quad \nu_{\Sigma'} \{ \hat{\gamma}(e_2) \parallel \mu \} \Downarrow \nu_{\Sigma_2} \{ \mathbb{V}_2 \parallel \mu_2 \} \quad (\nu_{\Sigma_1 \cup \Sigma_2} \{ [v_2/x]e \parallel \mu_1 \cup \mu_2 \} \Downarrow \nu_{\Sigma^*} \{ \mathbb{V}^{v_1, v_2} \parallel \mu^* \})_{v_1 = \lambda(x: \tau_1.e)}}{\nu_{\Sigma'} \{ \hat{\gamma}(e_1)(\hat{\gamma}(e_2)) \parallel \mu \} \Downarrow \nu_{\Sigma^*} \left\{ \bigcup_{(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2} \mathbb{V}^{v_1, v_2} \parallel \mu^* \right\}}$$

Since we have that each individual $v \in \mathbb{V}^{v_1, v_2}$ for $(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2$ is in $\mathcal{V}_{\Sigma^*}^\xi[[\tau_2]]$ by the above reasoning, it should also be the case that all the values in the Union of all these sets are in the value interpretation.

The only thing left to show for the term interpretation is that $\forall K^* \sim \ell^* \in (\Sigma^* \setminus \Sigma'). \text{kc} \sqsubseteq \ell^*$. This should follow from the premise $\text{kc} \sqsubseteq \ell_k$, as well as all the facts learned from unfolding **IHs** and term interps.

- **Case: T-ENC-MOBILE**

$$\frac{\text{ENC-MOBILE} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_\ell \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : \tau \quad \tau \blacktriangleleft \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{encrypt}_\ell(e_1; e_2) : (\text{enc}_\ell \tau)_\perp}$$

WTS: $\hat{\gamma}(\text{encrypt}_\ell(e_1; e_2)) \in \mathcal{E}_{\Sigma'}^\xi[[\text{enc}_\ell \tau)_\perp][\text{kc}]$

By definition of substitution, we have $\hat{\gamma}(\text{encrypt}_\ell(e_1; e_2)) = \text{encrypt}_\ell(\hat{\gamma}(e_1); \hat{\gamma}(e_2))$.

By **IH**, we have

- $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^\xi[[\text{key}_\ell][\text{kc}]$
- $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma'}^\xi[[\tau][\text{kc}]$

Unfolding the term interpretations, we have

- Since $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^\xi[[\text{key}_\ell][\text{kc}]$,

$$\nu_{\Sigma'} \{ \hat{\gamma}(e_1) \parallel \mu \} \Downarrow \nu_{\Sigma_1} \{ \mathbb{V}_1 \parallel \mu_1 \}$$

such that $\mu_1 : \Sigma_1$ and

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}^\xi[[\text{key}_\ell]]$$

and $\forall K_1 \sim \ell_1 \in (\Sigma_1 \setminus \Sigma'). \text{kc} \sqsubseteq \ell_1$

- Since $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma}^{\xi}[\tau][\text{kc}]$,

$$\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}^{\xi}[\tau]$$

and $\forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma')$. $\text{kc} \sqsubseteq \ell_2$

By Corollary 2 and Lemma 23, we have that $\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\text{key}_{\ell}]$. Unfolding the definition of leaf-determinism, this means that $\mathbb{V}_1 = \{\text{key}\langle K \rangle\}$ for some $K \sim \ell \in \Sigma_1$.

Since $K \sim \ell \in \Sigma_1$, then the signature must be of the form $\Sigma_1 = \Sigma_1^*$, $K \sim \ell$. Additionally, since we have $\mu_1 : \Sigma_1$, by definition, it must be the case that $\mu_1 = \mu_1^* \otimes K \hookrightarrow v_k$

We can then apply the following set-lifted dynamics rule, after defining the set \mathbb{U} in the required manner:

$$\frac{\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell \{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\} \quad \nu\Sigma\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\} \quad \mathbb{U} = \{u \mid v \in \mathbb{V}_2, u \in \mathcal{E}_{\ell}(v_k, v)\}}{\nu\Sigma'\{\text{encrypt}_{\ell}(\hat{\gamma}(e_1); \hat{\gamma}(e_2)) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\mathbb{U} \parallel \mu_1 \cup \mu_2\}}$$

We must now show that all $u \in \mathbb{U}$ are in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[(\text{enc}_{\ell} \tau)_{\perp}]$. This is equivalent to showing that they are all in $\mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[\text{enc}_{\ell} \tau]$.

By the definition of the value interpretation, we would need to show that $\exists v, v_k$ such that $v = \mathcal{D}(v_k, u)$ and $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[\tau]$. By set construction, we know that each $u \in \mathbb{U}$ is the product of $\mathcal{E}_{\ell}(v_k, v)$ for $v \in \mathbb{V}_2$, so we can take v_k, v to be such values by the definition of the encryption scheme (decryption is deterministic).

The only thing left to show is that $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[\tau]$. From the **IH**, we have that each $v \in \mathbb{V}_2$ is in $\mathcal{V}_{\Sigma_2}^{\xi}[\tau]$, which means that by Lemma 15, we have that $v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[\tau]$ since $\Sigma_1 \cup \Sigma_2 \leq \Sigma_2$.

The final thing to show is that $\forall K \sim \ell' \in ((\Sigma_1 \cup \Sigma_2) \setminus \Sigma')$. $\text{kc} \sqsubseteq \ell'$. This follows immediately from the results from the **IH** on Σ_1 and Σ_2 .

- **Case: T-ENC-STATIC**

This case is symmetric to **ENC-MOBILE**, since the unary relation is agnostic to any outer labels or the relationship between the level of the plaintext and the key.

- **Case: T-DEC**

$$\frac{\text{T-DEC} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_1 : \text{key}_{\ell} \quad \Sigma; \Gamma \vdash_{\text{kc}} e_2 : (\text{enc}_{\ell} \tau)_{\epsilon}}{\Sigma; \Gamma \vdash_{\text{kc}} \text{decrypt}_{\ell}(e_1; e_2) : \tau \text{ result}_{\epsilon}}$$

WTS: $\hat{\gamma}(\text{decrypt}_{\ell}(e_1; e_2)) \in \mathcal{E}_{\Sigma'}^{\xi}[\tau \text{ result}_{\epsilon}][\text{kc}]$

By definition of substitution, we have $\hat{\gamma}(\text{decrypt}_{\ell}(e_1; e_2)) = \text{decrypt}_{\ell}(\hat{\gamma}(e_1); \hat{\gamma}(e_2))$.

By **IH**, we have

- $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^{\xi}[\llbracket \text{key}_{\ell} \rrbracket][\text{kc}]$
- $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma'}^{\xi}[\llbracket (\text{enc}_{\ell} \tau)_{\epsilon} \rrbracket][\text{kc}]$

Unfolding the term interpretations, we have

- Since $\hat{\gamma}(e_1) \in \mathcal{E}_{\Sigma'}^{\xi}[\llbracket \text{key}_{\ell} \rrbracket][\text{kc}]$,

$$\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$$

such that $\mu_1 : \Sigma_1$ and

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}^{\xi}[\llbracket \text{key}_{\ell} \rrbracket]$$

and $\forall K_1 \sim \ell_1 \in (\Sigma_1 \setminus \Sigma'). \text{kc} \sqsubseteq \ell_1$.

- Since $\hat{\gamma}(e_2) \in \mathcal{E}_{\Sigma'}^{\xi}[\llbracket (\text{enc}_{\ell} \tau)_{\epsilon} \rrbracket][\text{kc}]$,

$$\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}^{\xi}[\llbracket (\text{enc}_{\ell} \tau)_{\epsilon} \rrbracket]$$

and $\forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma'). \text{kc} \sqsubseteq \ell_2$.

Since each $u \in \mathcal{V}_{\Sigma_2}^{\xi}[\llbracket (\text{enc}_{\ell} \tau)_{\epsilon} \rrbracket]$ (and therefore, by definition, are in $\mathcal{V}_{\Sigma_2}^{\xi}[\llbracket \text{enc}_{\ell} \tau \rrbracket]$), by the definition of the value interpretation, we have v'_k, v such that $v = \mathcal{D}(v'_k, v)$ and $v \in \mathcal{V}_{\Sigma_2}^{\xi}[\llbracket \tau \rrbracket]$. Furthermore, by Corollary 3 and Lemma 23, we have that $\nu\Sigma'\{\hat{\gamma}(e_2) \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}$ such that $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_{\Sigma_2}[\llbracket (\text{enc}_{\ell} \tau)_{\epsilon} \rrbracket]$. Unfolding the definition of leaf-determinism, this means that $\mathbb{V}_2 = \{u \mid u \in \mathcal{E}_{\ell}(v'_k, v), v \in \mathbb{V}\}$ for $\mathbb{V} \in \mathcal{L}\mathcal{V}_{\Sigma_2}[\llbracket \tau \rrbracket]$. That is, each value in \mathbb{V}_2 is the product of one call to \mathcal{E}_{ℓ} with the same plaintext v and key v'_k .

Also by Corollary 2 and Lemma 23, we have that $\nu\Sigma'\{\hat{\gamma}(e_1) \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\llbracket \text{key}_{\ell} \rrbracket]$. Unfolding the definition of leaf-determinism, this means that $\mathbb{V}_1 = \{\text{key}\langle K \rangle\}$ for some $K \sim \ell \in \Sigma_1$.

Since $K \sim \ell \in \Sigma_1$, then the signature must be of the form $\Sigma_1 = \Sigma_1^*, K \sim \ell$. Additionally, since we have $\mu_1 : \Sigma_1$, by definition, it must be the case that $\mu_1 = \mu_1^* \otimes K \hookrightarrow v_k$.

We proceed by casing on whether $v_k = v'_k$ (i.e. whether the key used to decrypt is the same as the one used to encrypt):

- $v_k = v'_k$

In this case, we have that all $u \in \mathcal{E}_{\ell}(v_k, v)$, meaning $\mathcal{D}(v_k, u) = v$ by the determinism of decryption. We can then apply the following dynamics rule:

$$\frac{\nu\Sigma'\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1^*, K \sim \ell \{ \{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k \} \quad \nu\Sigma'\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\} \quad \mathbb{V} = \{ \mathcal{D}(v_k, u) \mid u \in \mathbb{U} \}}{\nu\Sigma'\{\text{decrypt}_{\ell}(e_1; e_2) \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2 \{ \{\text{ok}(v) \mid v \in \mathbb{V} \} \parallel \mu_1 \cup \mu_2 \}}$$

To show that all $v' \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[\llbracket \tau \text{ result}_{\ell} \rrbracket]$, it is sufficient to show $v' \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^{\xi}[\llbracket \tau \text{ result} \rrbracket]$. To show this, since we know that each $v' = \text{ok}(v)$, we would only need to show that

$v \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \rrbracket$. This follows from the previous fact that $v \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau \rrbracket$ and Lemma 15.

- $v_k \neq v'_k$

In this case, we have that for all $u \in \mathcal{E}_\ell(v'_k, v)$ for some mismatched key v'_k , meaning $\mathcal{D}(v_k, u) = \perp$.

We apply the following dynamics rule:

$$\frac{\nu \Sigma' \{e_1 \parallel \mu\} \Downarrow \nu \Sigma_1 \{\{\text{key}\langle K \rangle\} \parallel \mu_1\} \quad \nu \Sigma' \{e_2 \parallel \mu\} \Downarrow \nu \Sigma_2 \{\mathbb{V}_2 \parallel \mu_2\} \quad (\mathcal{D}(v_k, u) = \perp)_{u \in \mathbb{U}}}{\nu \Sigma' \{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu \Sigma_1 \cup \Sigma_2 \{\{\text{Error}\} \parallel \mu_1 \cup \mu_2\}}$$

Since each v' in the resulting set is `Error`, we immediately have that $\forall v'. v' \in \mathcal{V}_{\Sigma_1 \cup \Sigma_2}^\xi \llbracket \tau \text{ result}_\epsilon \rrbracket$.

The final thing to show is that $\forall K \sim \ell' \in ((\Sigma_1 \cup \Sigma_2) \setminus \Sigma')$. $\text{kc} \sqsubseteq \ell'$. This follows immediately from the results from the IH on Σ_1 and Σ_2 .

- **Case: T-KEY-GEN**

$$\frac{\text{T-KEY-GEN} \quad \text{kc} \sqsubseteq \ell}{\Sigma; \Gamma \vdash_{\text{kc}} \text{gen}\langle \ell \rangle : \tau}$$

WTS: $\hat{\gamma}(\text{gen}\langle \ell \rangle) \in \mathcal{E}_{\Sigma'}^\xi \llbracket \tau \rrbracket \llbracket \text{kc} \rrbracket$

By definition of substitution, we have $\hat{\gamma}(\text{gen}\langle \ell \rangle) = \text{gen}\langle \ell \rangle$.

Suppose $\mu : \Sigma'$. Then, we can apply the following dynamics rules:

$$\frac{\mathcal{G} = \mathcal{G}'[\ell \mapsto v_k :: v_k s] \quad \mathcal{K} = \mathcal{K}'[\ell \mapsto K :: K s]}{(\mathcal{G}, \mathcal{K}, \nu \Sigma' \{\text{gen}\langle \ell \rangle \parallel \mu\}) \Downarrow (\mathcal{G}'[\ell \mapsto v_k s], \mathcal{K}'[\ell \mapsto K s], \nu \Sigma', K \sim \ell \{\{\text{key}\langle K \rangle\} \parallel \mu \otimes K \hookrightarrow v_k\})}$$

First, we need to show that $\{\text{key}\langle K \rangle\} \in \mathcal{V}_{\Sigma', K \sim \ell} \llbracket \text{key}_\ell \rrbracket$, this is immediate from the fact that $K \sim \ell \in \Sigma', K \sim \ell$.

We'd also like to show that $\forall K' \sim \ell \in (\Sigma', K \sim \ell) \setminus \Sigma'$. $\text{kc} \sqsubseteq \ell$. This follows from the premise.

- **Case: T-KEY-ACCESS**

WTS: $\hat{\gamma}(\text{key}\langle K \rangle) \in \mathcal{E}_{\Sigma'}^\xi \llbracket \text{key}_\ell \rrbracket \llbracket \text{kc} \rrbracket$

Suppose we have $\mu : \Sigma'$. Note that since $\Sigma' \leq \Sigma, K \sim \ell$, Σ' must be of the form $\Sigma' = \Sigma^*, K \sim \ell$. With $\mu : \Sigma^*, K \sim \ell$, it must be the case that $\mu = \mu^* \otimes K \hookrightarrow v_k$.

From the dynamics, we then have

$$\overline{\nu\Sigma^*, K \sim \ell\{\text{key}\langle K \rangle \parallel \mu^* \otimes K \leftrightarrow v_k\} \Downarrow \nu\Sigma^*, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu^* \otimes K \leftrightarrow v_k\}}$$

Also note that $(\Sigma^*, K \sim \ell) \setminus (\Sigma^*, K \sim \ell) = \emptyset$, so the effect condition is proven vacuously. It suffices to show that $\text{key}\langle K \rangle \in \mathcal{V}_{\Sigma^*, K \sim \ell}^\xi[\text{key}\ell]$, since that is the only element in the set. This reduces to showing that $K \sim \ell \in \Sigma^*, K \sim \ell$, which is immediate.

- **Case: T-SUB**

$$\frac{\text{T-SUB} \quad \Sigma; \Gamma \vdash_{\text{kc}'} e : \tau' \quad \text{kc} \sqsubseteq \text{kc}' \quad \tau' \leq \tau}{\Sigma; \Gamma \vdash_{\text{kc}} e : \tau}$$

WTS: $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^\xi[\llbracket \tau \rrbracket][\text{kc}]$

From the **IH**, we have that $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^\xi[\llbracket \tau' \rrbracket][\text{kc}']$.

Unfolding the term interpretation, this means that

- Since $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^\xi[\llbracket \tau' \rrbracket][\text{kc}']$,

$$\nu\Sigma'\{\hat{\gamma}(e) \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V} \parallel \mu'\}$$

such that $\mu' : \Sigma''$ and

$$\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma''}^\xi[\llbracket \tau' \rrbracket]$$

and $\forall K \sim \ell \in (\Sigma'' \setminus \Sigma'). \text{kc}' \sqsubseteq \ell$

First, observe that since $\text{kc} \sqsubseteq \text{kc}'$, then for all keys in $\Sigma'' \setminus \Sigma'$, the levels being greater than or equal to kc' implies they are greater than or equal to kc .

By Lemma 30, since $\forall v \in \mathbb{V}. v \in \mathcal{V}_{\Sigma''}^\xi[\llbracket \tau' \rrbracket]$, we have that all $v \in \mathcal{V}_{\Sigma''}^\xi[\llbracket \tau \rrbracket]$, which allows us to show that $\hat{\gamma}(e) \in \mathcal{E}_{\Sigma'}^\xi[\llbracket \tau \rrbracket][\text{kc}]$.

- **Omitted:** nat, unit, error, ok, resmatch

A.4 Proofs of Remaining Lemmas

We have the following corollaries of the Theorem 1, one for the binary and one for the unary:

Corollary 4. *If $\Sigma; \Gamma \vdash_{\text{kc}} e : \tau$, and*

- $\forall \Sigma'$ such that $\Sigma' \leq \Sigma$,
- $\forall \sigma$ such that $\sigma :_{\text{LD}} \Gamma; \Sigma'$ and $\forall \gamma \in \text{sing}(\sigma). \gamma : \Gamma; \Sigma'$,
- $\mu : \Sigma'$,

we have $\forall \gamma \in \text{sing}(\sigma)$,

$$\nu\Sigma'\{\hat{\gamma}(e) \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V} \parallel \mu'\}$$

with $\mathbb{V} \in \mathcal{LV}_{\Sigma''}[\llbracket \tau \rrbracket]$.

Proof. Suppose $\Sigma; \Gamma \vdash_{\text{kc}} e : \tau$, Σ' such that $\Sigma' \leq \Sigma$, σ such that $\sigma :_{\text{LD}} \Gamma; \Sigma$ and $\forall \gamma \in \text{sing}(\sigma)$. $\gamma : \Gamma; \Sigma$, and $\mu : \Sigma'$.

Given this σ , by Lemma 8, we have that $\text{set}(\gamma) :_{\text{LD}} \Gamma; \Sigma$ for all $\gamma \in \text{sing}(\sigma)$.

By Theorem 1, we have that $\widehat{\text{set}(\gamma)}(e) \in \mathcal{L}_{\Sigma'}[\tau]$. Unrolling the definition, we have

$$\forall e' \in \widehat{\text{set}(\gamma)}(e). \nu_{\Sigma'}\{e' \parallel \mu\} \Downarrow \nu_{\Sigma''}\{\mathbb{V}^{e'} \parallel \mu'\}$$

with $\mu' : \Sigma''$ and $\bigcup_{e' \in \widehat{\text{set}(\gamma)}(e)} \mathbb{V}^{e'} \in \mathcal{L}_{\Sigma''}[\tau]$.

By Lemma 10, we know that $\widehat{\text{set}(\gamma)}(e) = \{\hat{\gamma}(e)\}$. Applying this to the above unfolding, this gives us that

$$\nu_{\Sigma'}\{\hat{\gamma}(e) \parallel \mu\} \Downarrow \nu_{\Sigma''}\{\mathbb{V} \parallel \mu'\}$$

with $\mathbb{V} \in \mathcal{L}_{\Sigma''}[\tau]$, as required. \square

Corollary 5. *If $\Sigma; \Gamma \vdash_{\text{kc}} e : \tau$, and*

- $\forall \Sigma_1, \Sigma_2$ such that $\Sigma_1 \leq \Sigma$ and $\Sigma_2 \leq \Sigma$,
- $\forall \sigma_1, \sigma_2$ such that $\sigma_1 :_{\text{LD}} \Gamma; \Sigma_1$, $\sigma_2 :_{\text{LD}} \Gamma; \Sigma_2$, and $\forall (\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2)$. $\gamma_1 \equiv_{\xi} \gamma_2 : \Gamma; (\Sigma_1 \uplus \Sigma_2)$, and
- $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$,

we have $\forall (\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2)$,

$$\nu_{\Sigma_1}\{\hat{\gamma}_1(e) \parallel \mu_1\} \Downarrow \nu_{\Sigma'_1}\{\mathbb{V}_1 \parallel \mu'_1\}$$

$$\nu_{\Sigma_2}\{\hat{\gamma}_2(e) \parallel \mu_2\} \Downarrow \nu_{\Sigma'_2}\{\mathbb{V}_2 \parallel \mu'_2\}$$

with $\mathbb{V}_1 \in \mathcal{L}_{\Sigma'_1}[\tau]$ and $\mathbb{V}_2 \in \mathcal{L}_{\Sigma'_2}[\tau]$.

Proof. Suppose we have the above assumptions.

By Lemma 9, we have that $\text{set}(\gamma_1) :_{\text{LD}} \Gamma; \Sigma_1$ and $\text{set}(\gamma_2) :_{\text{LD}} \Gamma; \Sigma_2$ for all $(\gamma_1, \gamma_2) \in \text{sing}(\sigma_1) \times \text{sing}(\sigma_2)$.

By definition of $\mu_1 \equiv_{\xi} \mu_2 : \Sigma_1 \uplus \Sigma_2$, we have that separately $\mu_1 : \Sigma_1$ and $\mu_2 : \Sigma_2$. By Theorem 1, we have that $\widehat{\text{set}(\gamma_1)}(e) \in \mathcal{L}_{\Sigma_1}[\tau]$ and $\widehat{\text{set}(\gamma_2)}(e) \in \mathcal{L}_{\Sigma_2}[\tau]$. Unrolling the definition, we have

- For $\widehat{\text{set}(\gamma_1)}(e) \in \mathcal{L}_{\Sigma_1}[\tau]$, we get

$$\forall e'_1 \in \widehat{\text{set}(\gamma_1)}(e). \nu_{\Sigma_1}\{e'_1 \parallel \mu_1\} \Downarrow \nu_{\Sigma'_1}\{\mathbb{V}_1^{e'_1} \parallel \mu'_1\}$$

with $\mu'_1 : \Sigma'_1$ and $\bigcup_{e'_1 \in \widehat{\text{set}(\gamma_1)}(e)} \mathbb{V}_1^{e'_1} \in \mathcal{L}_{\Sigma'_1}[\tau]$.

- For $\widehat{\text{set}(\gamma_2)}(e) \in \mathcal{L}_{\Sigma_2}[\tau]$, we get

$$\forall e'_2 \in \widehat{\text{set}(\gamma_2)}(e). \nu_{\Sigma_2}\{e'_2 \parallel \mu_2\} \Downarrow \nu_{\Sigma'_2}\{\mathbb{V}_2^{e'_2} \parallel \mu'_2\}$$

with $\mu'_2 : \Sigma'_2$ and $\bigcup_{e'_2 \in \widehat{\text{set}(\gamma_2)}(e)} \mathbb{V}_2^{e'_2} \in \mathcal{L}_{\Sigma'_2}[\tau]$.

By Lemma 10, we know that $\widehat{\text{set}(\gamma_1)}(e) = \{\hat{\gamma}_1(e)\}$ and $\widehat{\text{set}(\gamma_2)}(e) = \{\hat{\gamma}_2(e)\}$. Applying this to the above unfolding, this gives us that

$$\nu_{\Sigma_1}\{\hat{\gamma}_1(e) \parallel \mu_1\} \Downarrow \nu_{\Sigma'_1}\{\mathbb{V}_1 \parallel \mu'_1\}$$

$$\nu_{\Sigma_2}\{\hat{\gamma}_2(e) \parallel \mu_2\} \Downarrow \nu_{\Sigma'_2}\{\mathbb{V}_1 \parallel \mu'_2\}$$

with $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau]$ and $\mathbb{V}_2 \in \mathcal{L}\mathcal{V}_{\Sigma'_2}[\tau]$, as required. \square

Lemma 41 (Transitivity). *If $\Sigma_2 \leq \Sigma_1$ and $\Sigma_3 \leq \Sigma_2$, then $\Sigma_3 \leq \Sigma_1$.*

Proof. Suppose $\Sigma_2 \leq \Sigma_1$ and $\Sigma_3 \leq \Sigma_2$.

We would like to show that $\forall K \sim \ell \in \Sigma_1, K \sim \ell \in \Sigma_3$. From the first assumption, we have that $\forall K \sim \ell \in \Sigma_1, K \sim \ell \in \Sigma_2$, and then from the second assumption we have $\forall K \sim \ell \in \Sigma_2, K \sim \ell \in \Sigma_3$. Therefore, since all elements in Σ_1 are contained in Σ_2 and all elements in Σ_2 are contained in Σ_3 , we get that all elements in Σ_1 are contained in Σ_3 . \square

Lemma 42 (Unary Anti-Monotonicity). *If $v \in \mathcal{V}_{\Sigma}[\tau]$ and $\Sigma' \leq \Sigma$, then $v \in \mathcal{V}_{\Sigma'}[\tau]$.*

Proof. We proceed by induction on the type τ :

- **Case:** $\tau = \text{unit}$
Since $v \in \mathcal{V}_{\Sigma}[\text{unit}]$, we have that $v = \langle \rangle$. We immediately have that $v \in \mathcal{V}_{\Sigma'}[\text{unit}]$ for any signature Σ' .
- **Case:** $\tau = \text{key}_{\ell}$
Since $v \in \mathcal{V}_{\Sigma}[\text{key}_{\ell}]$, we have that $v = \text{key}\langle K \rangle$ with $K \sim \ell \in \Sigma$.
Since $\Sigma' \leq \Sigma$, we have that $\forall K' \sim \ell' \in \Sigma, K' \sim \ell' \in \Sigma'$. Thus, we have that $K \sim \ell \in \Sigma'$, which gives us what we need to show $\text{key}\langle K \rangle \in \mathcal{V}_{\Sigma'}[\text{key}_{\ell}]$.
- **Case:** $\tau = \tau_1 \times \tau_2$
By the definition of the value interpretation, we have that $v = \langle v_1, v_2 \rangle$ with $v_1 \in \mathcal{V}_{\Sigma}[\tau_1]$ and $v_2 \in \mathcal{V}_{\Sigma}[\tau_2]$. By the **IH**, we have that $v_1 \in \mathcal{V}_{\Sigma'}[\tau_1]$ and $v_2 \in \mathcal{V}_{\Sigma'}[\tau_2]$, which gives us what we want to show for $\langle v_1, v_2 \rangle \in \mathcal{V}_{\Sigma'}[\tau_1 \times \tau_2]$.
- **Case:** $\tau = (\tau_1 + \tau_2)_{\ell}$
By the definition of the value interpretation, we have that either $v = 1 \cdot v_1$ with $v_1 \in \mathcal{V}_{\Sigma}[\tau_1]$ or $v = 2 \cdot v_2$ with $v_2 \in \mathcal{V}_{\Sigma}[\tau_2]$. By the **IH**, we have that $v_i \in \mathcal{V}_{\Sigma'}[\tau_i]$, which gives us what we want to show for $i \cdot v_i \in \mathcal{V}_{\Sigma'}[(\tau_1 + \tau_2)_{\ell}]$.
- **Case:** $\tau = \tau_1 \xrightarrow{\ell_k} \tau_2$
By the definition of the value interpretation, we have that $v = \lambda(x.e)$ such that $\forall \Sigma_1$ such that $\Sigma_1 \leq \Sigma$ and $\forall \mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1}[\tau_1]$ with $\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}[\tau_1]$, we have $[v_1/x]e \in \mathcal{E}_{\Sigma_1}[\tau_2]$.
Suppose we have Σ'_1 such that $\Sigma'_1 \leq \Sigma'$ and $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[\tau_1]$ such that $\forall v'_1 \in \mathbb{V}'_1. v'_1 \in \mathcal{V}_{\Sigma'_1}[\tau_1]$.
By Lemma 14, observe that $\Sigma'_1 \leq \Sigma$, since $\Sigma' \leq \Sigma$ and $\Sigma'_1 \leq \Sigma'$. This means we can apply the result from the value interpretation to obtain $[v'_1/x]e \in \mathcal{E}_{\Sigma'_1}[\tau_2]$, as required.

- **Case:** $\tau = (\text{enc}_\ell \tau')_\epsilon$
By the definition of the value interpretation, we have that $\exists v_k, v'. v' = \mathcal{D}_\ell(v_k, v)$ such that $v' \in \mathcal{V}_\Sigma \llbracket \tau' \rrbracket$.
By the **IH**, we have that $v' \in \mathcal{V}_{\Sigma'} \llbracket \tau' \rrbracket$, which gives us what we need to show $v \in \mathcal{V}_{\Sigma'} \llbracket (\text{enc}_\ell \tau')_\epsilon \rrbracket$.
- **Case:** $\tau = \tau' \text{ result}_\ell$
By the definition of the value interpretation, we have that either $v = \text{Error}$ or $v = \text{Ok}(v')$ with $v' \in \mathcal{V}_\Sigma \llbracket \tau' \rrbracket$.
In the former case, we immediately have that $\text{Error} \in \mathcal{V}_{\Sigma'} \llbracket \tau' \text{ result}_\ell \rrbracket$. In the latter case, we have by the **IH** that $v' \in \mathcal{V}_{\Sigma'} \llbracket \tau' \rrbracket$, which gives us that $\text{Ok}(v') \in \mathcal{V}_{\Sigma'} \llbracket \tau' \text{ result}_\ell \rrbracket$.
□

Lemma 43 (Binary Anti-Monotonicity). *If $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau \rrbracket$ and $\Sigma'_1 \leq \Sigma_1$ and $\Sigma'_2 \leq \Sigma_2$, then $(v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau \rrbracket$.*

Proof. We proceed by induction on the type τ :

- **Case:** $\tau = \text{unit}$
In this case, we have that $v_1 = v_2 = \langle \rangle$ by the definition of the value interpretation. This immediately gives us that $(v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \text{unit} \rrbracket$.
- **Case:** $\tau = \text{key}_\ell$
In this case, we have that $v_1 = \text{key}\langle K_1 \rangle$ and $v_2 = \text{key}\langle K_2 \rangle$ for $K_1 \sim \ell_1$
- **Case:** $\tau = t_\ell$
We proceed by casing on whether $\ell \sqsubseteq \xi$:
 - $\ell \sqsubseteq \xi$:
In this case, we have that $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket t \rrbracket$. We proceed by casing on t :
 - **Case:** $t = \tau_1 + \tau_2$
In this case, we have that either $v_1 = 1 \cdot v'_1$ and $v_2 = 1 \cdot v'_2$ with $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 \rrbracket$ or $v_1 = 2 \cdot v'_1$ and $v_2 = 2 \cdot v'_2$ with $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_2 \rrbracket$.
By the **IH**, we have that $(v'_1, v'_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau_i \rrbracket$, which gives us what we need to show $(i \cdot v'_1, i \cdot v'_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket (\tau_1 + \tau_2)_\ell \rrbracket$.
 - **Case:** $t = \text{enc}_{\ell'} \tau'$
In this case, we have that $\exists v_{ki}, v'_i. v'_i = \mathcal{D}_\ell(v_{ki}, v_i)$ for $i \in \{1, 2\}$.
We proceed by casing on whether $\ell' \sqsubseteq \xi$:
 - $\ell' \sqsubseteq \xi$:
In this case, we have that $v_{k1} = v_{k2}$ and $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau' \rrbracket$. By the **IH**, we have that $(v'_1, v'_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau' \rrbracket$, which then gives us what we need to show for $(v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket (\text{enc}_{\ell'} \tau')_\ell \rrbracket$.
 - $\ell' \not\sqsubseteq \xi$:
In this case, we have that $v'_1 \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau' \rrbracket$, $v'_2 \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau' \rrbracket$, and $v_1 \doteq v_2$.
By Lemma 15, we have that $v'_1 \in \mathcal{V}_{\Sigma'_1}^\xi \llbracket \tau' \rrbracket$ and $v'_2 \in \mathcal{V}_{\Sigma'_2}^\xi \llbracket \tau' \rrbracket$, which gives us what we need to show $(v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket (\text{enc}_{\ell'} \tau')_\ell \rrbracket$.

– **Case:** $\tau = \tau'$ result

In this case, we have that either $v_1 = v_2 = \text{Error}$ or $v_1 = \text{Ok}(v'_1)$ and $v_2 = \text{Ok}(v'_2)$ with $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau' \rrbracket$.

In the former case, we immediately have that $(\text{Error}, \text{Error}) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau' \text{ result}_\ell \rrbracket$.

In the latter, from the **IH**, we have that $(v'_1, v'_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau' \rrbracket$, which gives us what we need to show for $(\text{Ok}(v'_1), \text{Ok}(v'_2)) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau' \text{ result}_\ell \rrbracket$.

▪ $\ell \not\subseteq \xi$:

In this case, we have that $v_1 \in \mathcal{V}_{\Sigma_1} \llbracket t \rrbracket$ and $v_2 \in \mathcal{V}_{\Sigma_2} \llbracket t \rrbracket$. By Lemma 15, we have that $v_1 \in \mathcal{V}_{\Sigma'_1} \llbracket t \rrbracket$ and $v_2 \in \mathcal{V}_{\Sigma'_2} \llbracket t \rrbracket$, which then gives us $(v_1, v_2) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket t_\ell \rrbracket$ by definition.

• **Case:** $\tau = \tau_1 \xrightarrow{\ell_k} \tau_2$

By definition, this means we have $v_1 =_\alpha \lambda(x.e_1)$ and $v_2 =_\alpha \lambda(x.e_2)$ such that $\forall \Sigma'_1, \Sigma'_2$ such that $\Sigma'_1 \leq \Sigma_1$ and $\Sigma'_1 \leq \Sigma_2$ and $\forall \mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1} \llbracket \tau_1 \rrbracket, \mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_2} \llbracket \tau_1 \rrbracket$, with $\forall (v_1, v'_1) \in \mathbb{V}_1 \times \mathbb{V}'_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$, we have $([v_1/x]e_1, [v'_1/x]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket$.

Suppose we have Σ_1^*, Σ_2^* such that $\Sigma_1^* \leq \Sigma'_1$ and $\Sigma_2^* \leq \Sigma'_2$. Suppose also that we have $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma_1^*} \llbracket \tau_1 \rrbracket, \mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma_2^*} \llbracket \tau_1 \rrbracket$ with $\forall (v_1, v'_1) \in \mathbb{V}_1 \times \mathbb{V}'_1. (v_1, v'_1) \in \mathcal{V}_{\Sigma_1^*, \Sigma_2^*}^\xi \llbracket \tau_1 \rrbracket$.

By Lemma 14, observe that $\Sigma_1^* \leq \Sigma_1$ and $\Sigma_2^* \leq \Sigma_2$, since we have $\Sigma'_1 \leq \Sigma_1$ and $\Sigma'_2 \leq \Sigma_2$. We then have $([v_1/x]e_1, [v'_1/x]e_2) \in \mathcal{E}_{\Sigma_1^*, \Sigma_2^*}^\xi \llbracket \tau_2 \rrbracket$ from the value interpretation result. □

Lemma 44. *If $\gamma : \Gamma; \Sigma$ and $\Sigma' \leq \Sigma$, then $\gamma : \Gamma; \Sigma'$.*

Proof. By definition of $\gamma : \Gamma; \Sigma$, we have that $\forall x : \tau \in \Gamma, \gamma(x) \in \mathcal{V}_\Sigma \llbracket \tau \rrbracket$. By Lemma 15, we have that $\gamma(x) \in \mathcal{V}_{\Sigma'} \llbracket \tau \rrbracket$ for each x , which gives us that $\gamma : \Gamma; \Sigma'$. □

Lemma 45. *If $\gamma \equiv_\xi \gamma' : \Gamma; \Sigma_1 \uplus \Sigma_2$ and $\Sigma'_1 \leq \Sigma_1, \Sigma'_2 \leq \Sigma_2$, then $\gamma : \Gamma; \Sigma'_1 \uplus \Sigma'_2$.*

Proof. By definition of $\gamma \equiv_\xi \gamma' : \Gamma; \Sigma_1 \uplus \Sigma_2$, we have that $\forall x : \tau \in \Gamma. (\gamma(x), \gamma'(x)) \in \mathcal{V}_{\Sigma_1, \Sigma_2} \llbracket \tau \rrbracket$. By Lemma 16, we have that $(\gamma(x), \gamma'(x)) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2} \llbracket \tau \rrbracket$ for all x , which gives us that $\gamma \equiv_\xi \gamma' : \Sigma'_1 \uplus \Sigma'_2$. □

Lemma 46. *If $\mu_1 : \Sigma_1$ and $\mu_2 : \Sigma_2$, then $\mu_1 \cup \mu_2 : \Sigma_1 \cup \Sigma_2$.*

Proof. (Outline) This should follow from the definition of memory well-formedness, since individually each of μ_1 and μ_2 are well-formed against Σ_1 and Σ_2 , together they continue to well-formed, the union does not induce any elements that are unaccounted for. □

Lemma 47. *If $\mu_1 \equiv_\xi \mu'_1 : \Sigma_1 \uplus \Sigma'_1$ and $\mu_2 \equiv_\xi \mu'_2 : \Sigma_2 \uplus \Sigma'_2$, then $\mu_1 \cup \mu_2 \equiv_\xi \mu'_1 \cup \mu'_2 : (\Sigma_1 \cup \Sigma_2) \uplus (\Sigma'_1 \cup \Sigma'_2)$*

Proof. (Outline) From the previous lemma, we can obtain that $\mu_1 \cup \mu_2 : \Sigma_1 \cup \Sigma_2$ and $\mu'_1 \cup \mu'_2 : \Sigma'_1 \cup \Sigma'_2$. To show the equivalence of the two joint memories, we can simply choose the pairs from the original μ_1, μ'_1 and μ_2, μ'_2 to show the equivalence for, since we know it held originally and not additional elements need to be accounted for. □

Lemma 48. *For all $\Sigma_1, \Sigma_2, \Sigma_1 \cup \Sigma_2 \leq \Sigma_1$.*

Proof. We would like to show that $\forall K \sim \ell \in \Sigma_1. K \sim \ell \in \Sigma_1 \cup \Sigma_2$. This follows from the fact that, by definition, $\Sigma_1 \cup \Sigma_2$ contains all of the elements in Σ_1 . \square

Lemma 49. For all $\Sigma_1, \Sigma_2, \Sigma_3$, if $\Sigma_1 \leq \Sigma_2$, then $\Sigma_1 \setminus \Sigma_3 = (\Sigma_1 \setminus \Sigma_2) \cup (\Sigma_2 \setminus \Sigma_3)$.

Proof. (Outline) Observe that $(\Sigma_1 \setminus \Sigma_2) \cup \Sigma_2 = \Sigma_1$, which means that the RHS is equivalent to $\Sigma_1 \setminus \Sigma_3$. \square

Lemma 50. If $(\mathcal{G}, \mathcal{K}, \nu\Sigma\{e \parallel \mu\}) \Downarrow (\mathcal{G}_1, \mathcal{K}_1, \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\})$ and $(\mathcal{G}, \mathcal{K}, \nu\Sigma\{e \parallel \mu\}) \Downarrow (\mathcal{G}_2, \mathcal{K}_2, \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\})$, then $\mathbb{V}_1 = \mathbb{V}_2$, $\Sigma_1 = \Sigma_2$, and $\mu_1 = \mu_2$ (and $\mathcal{G}_1 = \mathcal{G}_2$, $\mathcal{K}_1 = \mathcal{K}_2$).

Proof. We proceed by rule induction on the first stepping judgment:

- **Case:**
$$\frac{}{\nu\Sigma\{\langle \rangle \parallel \mu\} \Downarrow \nu\Sigma\{\{\langle \rangle\} \parallel \mu\}}$$

Proceeding by rule induction on the other judgment, the only non-vacuous case is

$$\frac{}{\nu\Sigma\{\langle \rangle \parallel \mu\} \Downarrow \nu\Sigma\{\{\langle \rangle\} \parallel \mu\}}$$
, which immediately gives us what we want to show since $\{\langle \rangle\} = \{\langle \rangle\}$, $\Sigma = \Sigma$, and $\mu = \mu$.

- **Case:**
$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_2\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}}{\nu\Sigma\{\langle e_1, e_2 \rangle \parallel \mu\} \Downarrow \nu\Sigma_1 \cup \Sigma_2\{\{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\} \parallel \mu_1 \cup \mu_2\}}$$

Proceeding by rule induction on the other judgment, the only non-vacuous case is

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma'_1\{\mathbb{V}'_1 \parallel \mu'_2\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma'_2\{\mathbb{V}'_2 \parallel \mu'_2\}}{\nu\Sigma\{\langle e_1, e_2 \rangle \parallel \mu\} \Downarrow \nu\Sigma'_1 \cup \Sigma'_2\{\{\langle v'_1, v'_2 \rangle \mid v'_1 \in \mathbb{V}'_1, v'_2 \in \mathbb{V}'_2\} \parallel \mu'_1 \cup \mu'_2\}}$$

By the **IH**, we have that

- $\Sigma_1 = \Sigma'_1$, $\mathbb{V}_1 = \mathbb{V}'_1$, $\mu_1 = \mu'_1$
- $\Sigma_2 = \Sigma'_2$, $\mathbb{V}_2 = \mathbb{V}'_2$, $\mu_2 = \mu'_2$

This then gives us that $\Sigma_1 \cup \Sigma_2 = \Sigma'_1 \cup \Sigma'_2$, $\mu_1 \cup \mu_2 = \mu'_1 \cup \mu'_2$, and the sets

$$\{\langle v_1, v_2 \rangle \mid v_1 \in \mathbb{V}_1, v_2 \in \mathbb{V}_2\} = \{\langle v'_1, v'_2 \rangle \mid v'_1 \in \mathbb{V}'_1, v'_2 \in \mathbb{V}'_2\}$$

as required.

- **Case:**
$$\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (i \in \{1, 2\})}{\nu\Sigma\{e \cdot i \parallel \mu\} \Downarrow \nu\Sigma'\{\{v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}\} \parallel \mu'\}}$$

Proceeding by rule induction on the other judgment, the only non-vacuous case is

$$\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}' \parallel \mu''\} \quad (i \in \{1, 2\})}{\nu\Sigma\{e \cdot i \parallel \mu\} \Downarrow \nu\Sigma''\{\{v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}'\} \parallel \mu''\}}$$

By the **IH**, we have that $\Sigma' = \Sigma''$, $\mathbb{V} = \mathbb{V}'$, $\mu' = \mu''$.

Since $\mathbb{V} = \mathbb{V}'$, we have that $\forall v \in \mathbb{V}$ and $\forall v \in \mathbb{V}'$, $v = \langle v_1, v_2 \rangle$. As such, we get that the resultant sets $\{v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}\}$ and $\{v_i \mid \langle v_1, v_2 \rangle \in \mathbb{V}'\}$ are equal.

- **Case:**
$$\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (i \in \{1, 2\})}{\nu\Sigma\{i \cdot e \parallel \mu\} \Downarrow \nu\Sigma'\{\{i \cdot v \mid v \in \mathbb{V}\} \parallel \mu'\}}$$

Proceeding by rule induction on the other judgment, the only non-vacuous case is

$$\frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}' \parallel \mu''\} \quad (i \in \{1, 2\})}{\nu\Sigma\{i \cdot e \parallel \mu\} \Downarrow \nu\Sigma''\{\{i \cdot v \mid v \in \mathbb{V}'\} \parallel \mu''\}}$$

By the **IH**, we have that $\Sigma' = \Sigma''$, $\mathbb{V} = \mathbb{V}'$, $\mu' = \mu''$. Since $\mathbb{V} = \mathbb{V}'$, we then have by set construction that $\{i \cdot v \mid v \in \mathbb{V}\} = \{i \cdot e \mid v \in \mathbb{V}'\}$.

$$\bullet \text{ Case: } \frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (\nu\Sigma'\{[v'/x_1]e_1 \parallel \mu'\} \Downarrow \nu\Sigma_1\{\mathbb{V}^v \parallel \mu_1\})_{v=1 \cdot v'}}{\nu\Sigma\{\text{case } e \{x_1.e_1 \mid x_2.e_2\} \parallel \mu\} \Downarrow \nu\Sigma_1\{\bigcup_{v \in \mathbb{V}} \mathbb{V}^v \parallel \mu_1\}}$$

Proceeding by rule induction on the other judgment, we have the two following non-vacuous cases:

$$\bullet \text{ Case: } \frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}' \parallel \mu''\} \quad (\nu\Sigma''\{[v'/x_1]e_1 \parallel \mu''\} \Downarrow \nu\Sigma_1'\{\mathbb{V}'^v \parallel \mu_1'\})_{v=1 \cdot v'}}{\nu\Sigma\{\text{case } e \{x_1.e_1 \mid x_2.e_2\} \parallel \mu\} \Downarrow \nu\Sigma_1'\{\bigcup_{v \in \mathbb{V}'} \mathbb{V}'^v \parallel \mu_1'\}}$$

By the **IH**, we have that $\Sigma' = \Sigma''$, $\mathbb{V} = \mathbb{V}'$, $\mu' = \mu''$. In this case, we have that $\forall v \in \mathbb{V}$ and $\forall v \in \mathbb{V}'$, $v = 1 \cdot v'$.

We also have from the **IH** that $\Sigma_1 = \Sigma_1'$, $\mathbb{V}^v = \mathbb{V}'^v$ for each $v \in \mathbb{V}$, and $\mu_1 = \mu_1'$. Since $\mathbb{V}^v = \mathbb{V}'^v$ and $\mathbb{V} = \mathbb{V}'$, we have that $\bigcup_{v \in \mathbb{V}} \mathbb{V}^v = \bigcup_{v \in \mathbb{V}'} \mathbb{V}'^v$, as required.

$$\bullet \text{ Case: } \frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma''\{\mathbb{V}' \parallel \mu''\} \quad (\nu\Sigma''\{[v'/x_2]e_2 \parallel \mu''\} \Downarrow \nu\Sigma_2\{\mathbb{V}'^v \parallel \mu_2\})_{v=2 \cdot v'}}{\nu\Sigma\{\text{case } e \{x_1.e_1 \mid x_2.e_2\} \parallel \mu\} \Downarrow \nu\Sigma_2\{\bigcup_{v \in \mathbb{V}} \mathbb{V}^v \parallel \mu_2\}}$$

By the **IH**, we have that $\Sigma' = \Sigma''$, $\mathbb{V} = \mathbb{V}'$, $\mu' = \mu''$. However, in this case, we have that $\forall v \in \mathbb{V}$, $v = 1 \cdot v'$ and $\forall v' \in \mathbb{V}'$, $v' = 2 \cdot v''$, which is a contradiction with the **IH** result. Thus, this case is vacuous.

$$\bullet \text{ Case: } \frac{\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\} \quad (\nu\Sigma'\{[v'/x_2]e_2 \parallel \mu'\} \Downarrow \nu\Sigma_2\{\mathbb{V}^v \parallel \mu_2\})_{v=2 \cdot v'}}{\nu\Sigma\{\text{case } e \{x_1.e_1 \mid x_2.e_2\} \parallel \mu\} \Downarrow \nu\Sigma_2\{\bigcup_{v \in \mathbb{V}} \mathbb{V}^v \parallel \mu_2\}}$$

This case is symmetric to the previous.

$$\bullet \text{ Case: } \frac{\nu\Sigma\{\lambda(x : \tau_1.e) \parallel \mu\} \Downarrow \nu\Sigma\{\{\lambda(x : \tau_1.e)\} \parallel \mu\}}{\nu\Sigma\{\lambda(x : \tau_1.e) \parallel \mu\} \Downarrow \nu\Sigma\{\{\lambda(x : \tau_1.e)\} \parallel \mu\}}$$

Proceeding by rule induction on the other judgment, the only non-vacuous case is

$$\frac{\nu\Sigma\{\lambda(x : \tau_1.e) \parallel \mu\} \Downarrow \nu\Sigma\{\{\lambda(x : \tau_1.e)\} \parallel \mu\}}{\nu\Sigma\{\lambda(x : \tau_1.e) \parallel \mu\} \Downarrow \nu\Sigma\{\{\lambda(x : \tau_1.e)\} \parallel \mu\}}$$

This immediately gives us what we want to show, since $\Sigma = \Sigma$, $\{1 \text{ am}[\tau_1; \tau_2](x : \tau_1.e)\} = \{\lambda(x : \tau_1.e)\}$, and $\mu = \mu$.

$$\bullet \text{ Case: } \frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\} \quad (\nu\Sigma_1 \cup \Sigma_2\{[v_2/x]e \parallel \mu_1 \cup \mu_2\} \Downarrow \nu\Sigma^*\{\mathbb{V}^{v_1, v_2} \parallel \mu^*\})_{v_1 = \lambda(x : \tau_1.e)}}{\nu\Sigma\{e_1(e_2) \parallel \mu\} \Downarrow \nu\Sigma^*\{\bigcup_{(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2} \mathbb{V}^{v_1, v_2} \parallel \mu^*\}}$$

Proceeding my rule induction on the other judgment, the only non-vacuous case is

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1'\{\mathbb{V}'_1 \parallel \mu'_1\} \quad \nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2'\{\mathbb{V}'_2 \parallel \mu'_2\} \quad (\nu\Sigma_1' \cup \Sigma_2'\{[v_2/x]e \parallel \mu'_1 \cup \mu'_2\} \Downarrow \nu\Sigma^{**}\{\mathbb{V}'^{v_1, v_2} \parallel \mu^{**}\})_{v_1 = \lambda(x : \tau_1.e)}}{\nu\Sigma\{e_1(e_2) \parallel \mu\} \Downarrow \nu\Sigma^{**}\{\bigcup_{(v_1, v_2) \in \mathbb{V}'_1 \times \mathbb{V}'_2} \mathbb{V}'^{v_1, v_2} \parallel \mu^{**}\}}$$

By the **IH**, we have

$$\bullet \Sigma_1 = \Sigma_1', \mathbb{V}_1 = \mathbb{V}'_1, \text{ and } \mu_1 = \mu'_1$$

- $\Sigma_2 = \Sigma'_2$, $\mathbb{V}_2 = \mathbb{V}'_2$, and $\mu_2 = \mu'_2$

This gives us that $\Sigma_1 \cup \Sigma_2 = \Sigma'_1 \cup \Sigma'_2$ and $\mu_1 \cup \mu_2 = \mu'_1 \cup \mu'_2$. As such, by the **IH** on the third premise, we have that $\Sigma^* = \Sigma^{**}$, $\mathbb{V}^{v_1, v_2} = \mathbb{V}'^{v_1, v_2}$ for all $(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2$, and $\mu^* = \mu^{**}$.

Finally, since $\mathbb{V}^{v_1, v_2} = \mathbb{V}'^{v_1, v_2}$, we get that $\bigcup_{(v_1, v_2) \in \mathbb{V}_1 \times \mathbb{V}_2} \mathbb{V}^{v_1, v_2} = \bigcup_{(v_1, v_2) \in \mathbb{V}'_1 \times \mathbb{V}'_2} \mathbb{V}'^{v_1, v_2}$.

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\}}{\nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{V} \parallel \mu_2\}} \quad \mathbb{U} = \{u \mid v \in \mathbb{V}, u \in \mathcal{E}_\ell(v_k, v)\}$$

- **Case:** $\frac{\nu\Sigma\{\text{encrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\mathbb{U} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma'_1, K' \sim \ell\{\{\text{key}\langle K' \rangle\} \parallel \mu'_1 \otimes K \hookrightarrow v'_k\}}$

Proceeding by rule induction on the other judgment, the only non-vacuous case is

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma'_1, K' \sim \ell\{\{\text{key}\langle K' \rangle\} \parallel \mu'_1 \otimes K \hookrightarrow v'_k\}}{\nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma'_2\{\mathbb{V}' \parallel \mu'_2\}} \quad \mathbb{U}' = \{u \mid v \in \mathbb{V}', u \in \mathcal{E}_\ell(v'_k, v)\}$$

$$\nu\Sigma\{\text{encrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma'_1, K' \sim \ell) \cup \Sigma'_2\{\mathbb{U}' \parallel (\mu'_1 \otimes K' \hookrightarrow v'_k) \cup \mu'_2\}$$

By the **IH**, we have that

- $\Sigma_1, K \sim \ell = \Sigma'_1, K' \sim \ell$, $\{\text{key}\langle K \rangle\} = \{\text{key}\langle K' \rangle\}$, and $\mu_1 \otimes K \hookrightarrow v_k = \mu'_1 \otimes K' \hookrightarrow v'_k$.
- $\Sigma_2 = \Sigma'_2$, $\mathbb{V} = \mathbb{V}'$, $\mu_2 = \mu'_2$

Note that this means $\text{key}\langle K \rangle = \text{key}\langle K' \rangle$ (i.e. the strings K and K' are equal) and $v_k = v'_k$.

The above results give us that $(\Sigma_1, K \sim \ell) \cup \Sigma_2 = (\Sigma'_1, K' \sim \ell) \cup \Sigma'_2$, $\{u \mid v \in \mathbb{V}, u \in \mathcal{E}_\ell(v_k, v)\} = \{u \mid v \in \mathbb{V}', u \in \mathcal{E}_\ell(v'_k, v)\}$, and $(\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2 = (\mu'_1 \otimes K' \hookrightarrow v'_k) \cup \mu'_2$.

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\}}{\nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{U} \parallel \mu_2\}} \quad \mathbb{V} = \{\mathcal{D}(v_k, u) \mid u \in \mathbb{U}\}$$

- **Case:** $\frac{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\{\text{ok}(v) \mid v \in \mathbb{V}\} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma'_1, K' \sim \ell'\{\{\text{key}\langle K' \rangle\} \parallel \mu'_1 \otimes K \hookrightarrow v'_k\}}$

Proceeding by rule induction on the other judgment, we have two non-vacuous cases:

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma'_1, K' \sim \ell'\{\{\text{key}\langle K' \rangle\} \parallel \mu'_1 \otimes K \hookrightarrow v'_k\}}{\nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma'_2\{\mathbb{U}' \parallel \mu'_2\}} \quad \mathbb{V}' = \{\mathcal{D}(v'_k, u) \mid u \in \mathbb{U}'\}$$

- **Case:** $\frac{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma'_1, K' \sim \ell) \cup \Sigma'_2\{\{\text{ok}(v) \mid v \in \mathbb{V}'\} \parallel (\mu'_1 \otimes K' \hookrightarrow v'_k) \cup \mu'_2\}}{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\{\text{ok}(v) \mid v \in \mathbb{V}\} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}$

In this case, by the **IH**, we have that

- $\Sigma_1, K \sim \ell = \Sigma'_1, K' \sim \ell$, $\{\text{key}\langle K \rangle\} = \{\text{key}\langle K' \rangle\}$, and $\mu_1 \otimes K \hookrightarrow v_k = \mu'_1 \otimes K' \hookrightarrow v'_k$.
- $\Sigma_2 = \Sigma'_2$, $\mathbb{U} = \mathbb{U}'$, $\mu_2 = \mu'_2$

Note that this means $\text{key}\langle K \rangle = \text{key}\langle K' \rangle$ (i.e. the strings K and K' are equal) and $v_k = v'_k$. Similarly, since $\mathbb{U} = \mathbb{U}'$, we have that $\{\mathcal{D}_\ell(v_k, u) \mid u \in \mathbb{U}\} = \{\mathcal{D}_\ell(v_k, u') \mid u' \in \mathbb{U}'\}$.

The above results give us that $(\Sigma_1, K \sim \ell) \cup \Sigma_2 = (\Sigma'_1, K' \sim \ell) \cup \Sigma'_2$, $\{\text{ok}(v) \mid v \in \mathbb{V}\} = \{\text{ok}(v) \mid v \in \mathbb{V}'\}$, and $(\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2 = (\mu'_1 \otimes K' \hookrightarrow v'_k) \cup \mu'_2$.

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\}}{\nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{U} \parallel \mu_2\}} \quad (\mathcal{D}(v_k, u) = \perp)_{\forall u \in \mathbb{U}}$$

- **Case:** $\frac{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\{\text{Error}\} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma'_1, K' \sim \ell) \cup \Sigma'_2\{\{\text{Error}\} \parallel (\mu'_1 \otimes K' \hookrightarrow v'_k) \cup \mu'_2\}}$

In this case, by the **IH**, we have that

- $\Sigma_1, K \sim \ell = \Sigma'_1, K' \sim \ell$, $\{\text{key}\langle K \rangle\} = \{\text{key}\langle K' \rangle\}$, and $\mu_1 \otimes K \hookrightarrow v_k = \mu'_1 \otimes K' \hookrightarrow v'_k$.

$$- \Sigma_2 = \Sigma'_2, \mathbb{U} = \mathbb{U}', \mu_2 = \mu'_2$$

However, note that in this case, the decryption of each of the ciphertexts in \mathbb{U}' fails, whereas all of the ciphertexts in \mathbb{U} succeed, which is a contradiction. Thus, this case is vacuous.

$$\frac{\nu\Sigma\{e_1 \parallel \mu\} \Downarrow \nu\Sigma_1, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu_1 \otimes K \hookrightarrow v_k\}}{\nu\Sigma\{e_2 \parallel \mu\} \Downarrow \nu\Sigma_2\{\mathbb{U} \parallel \mu_2\} \quad (\mathcal{D}(v_k, u) = \perp)_{\forall u \in \mathbb{U}}}$$

- **Case:** $\frac{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\{\text{Error}\} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}{\nu\Sigma\{\text{decrypt}_\ell(e_1; e_2) \parallel \mu\} \Downarrow \nu(\Sigma_1, K \sim \ell) \cup \Sigma_2\{\{\text{Error}\} \parallel (\mu_1 \otimes K \hookrightarrow v_k) \cup \mu_2\}}$

This case is symmetric to the previous.

$$\mathcal{G} = \mathcal{G}'[\ell \mapsto v_k :: v_k s] \quad \mathcal{K} = \mathcal{K}'[\ell \mapsto K :: K s]$$

- **Case:** $\frac{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{\text{gen}\langle \ell \rangle \parallel \mu\}) \Downarrow (\mathcal{G}'[\ell \mapsto v_k s], \mathcal{K}'[\ell \mapsto K s], \nu\Sigma, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu \otimes K \hookrightarrow v_k\})}{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{\text{gen}\langle \ell \rangle \parallel \mu\}) \Downarrow (\mathcal{G}'[\ell \mapsto v_k s], \mathcal{K}'[\ell \mapsto K s], \nu\Sigma, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu \otimes K \hookrightarrow v_k\})}$

Proceeding by rule induction on the other judgment, the only non-vacuous case is

$$\mathcal{G} = \mathcal{G}'[\ell \mapsto v_k :: v_k s] \quad \mathcal{K} = \mathcal{K}'[\ell \mapsto K :: K s]$$

$$\frac{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{\text{gen}\langle \ell \rangle \parallel \mu\}) \Downarrow (\mathcal{G}'[\ell \mapsto v_k s], \mathcal{K}'[\ell \mapsto K s], \nu\Sigma, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu \otimes K \hookrightarrow v_k\})}{(\mathcal{G}, \mathcal{K}, \nu\Sigma\{\text{gen}\langle \ell \rangle \parallel \mu\}) \Downarrow (\mathcal{G}'[\ell \mapsto v_k s], \mathcal{K}'[\ell \mapsto K s], \nu\Sigma, K \sim \ell\{\{\text{key}\langle K \rangle\} \parallel \mu \otimes K \hookrightarrow v_k\})}$$

Note that since the expressions are being evaluated in the same environment, we have that the key string K and key value v_k produced in both runs is the same. Thus, we have what we want to show.

- Omitted: err, ok, resmatch, key

□

Lemma 51. *If $\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma'\{\mathbb{V} \parallel \mu'\}$, then $\Sigma' \leq \Sigma$.*

Proof. (Outline) Proceed by induction on the stepping judgment, the signature always grows. □

Lemma 52. *If $\ell_1 \not\sqsubseteq \ell_2$, then for all ℓ , we have that $\ell_1 \sqcup \ell \not\sqsubseteq \ell_2$.*

Proof. Suppose it is the case that $\ell_1 \sqcup \ell \sqsubseteq \ell_2$. By the definition of least upper bound, this means that ℓ_2 is the lowest such label that $\ell_1 \sqsubseteq \ell_2$ and $\ell \sqsubseteq \ell_2$. However, we already have that $\ell_1 \not\sqsubseteq \ell_2$, so this is impossible. □

Lemma 53. *If $\ell_1 \sqsubseteq \ell$ and $\ell_2 \sqsubseteq \ell$, then $\ell_1 \sqcup \ell_2 \sqsubseteq \ell$.*

Proof. In a lattice, by definition, there must exist a least upper bound between two elements. In this case, suppose $\ell_1 \sqcup \ell_2 = \ell'$. We consider whether $\ell' = \ell$:

- $\ell' = \ell$

In this case, we immediately have what we want to show by the definition of least upper bound.

- $\ell' \neq \ell$

By the definition of least upper bound, we have that ℓ' is the lowest element such that $\ell_1 \sqsubseteq \ell'$ and $\ell_2 \sqsubseteq \ell'$. Since ℓ' is the least upper bound, it cannot be the case that $\ell \sqsubseteq \ell'$, since that would make ℓ the lowest element satisfying the bound. It also cannot be the case that $\ell' \not\sqsubseteq \ell$ or $\ell \not\sqsubseteq \ell'$ —in the former case, this would contradict that $\ell_1 \sqsubseteq \ell$ and $\ell_2 \sqsubseteq \ell$ by transitivity, and in the latter case, it would contradict the fact that $\ell_1 \sqsubseteq \ell'$ and $\ell_2 \sqsubseteq \ell'$ by

the least upper bound (again by transitivity). Thus, we must have $\ell' \sqsubseteq \ell$, which gives us $\ell_1 \sqcup \ell_2 \sqsubseteq \ell$ by transitivity. □

Lemma 54. *If $\ell_1 \sqcup \ell_2 \sqsubseteq \ell$, then $\ell_1 \sqsubseteq \ell$ and $\ell_2 \sqsubseteq \ell$.*

Proof. This follows directly from the definition of least upper bound. □

Lemma 55. *If $\ell_1 \sqsubseteq \ell_2$ and $\ell_1 \not\sqsubseteq \ell_3$, then $\ell_2 \not\sqsubseteq \ell_3$.*

Proof. Suppose it is the case that $\ell_2 \sqsubseteq \ell_3$, then, it must be the case that $\ell_1 \sqsubseteq \ell_3$, since we have that $\ell_1 \sqsubseteq \ell_2$ and we can apply transitivity. However, we have that $\ell_1 \not\sqsubseteq \ell_3$, so this is a contradiction and thus we must have $\ell_2 \not\sqsubseteq \ell_3$. □

Lemma 56 (Binary-Unary Subsumption). *If $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau]$, then $v_1 \in \mathcal{V}_{\Sigma_1}[\tau]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[\tau]$.*

Proof. Suppose we have $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau]$. We proceed by induction on the type τ :

- **Case:** $\tau = \text{unit}$

In this case, we have that $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\text{unit}]$. By definition, this means that $v_1 = v_2 = \langle \rangle$, and this immediately gives us that $v_1 \in \mathcal{V}_{\Sigma_1}[\text{unit}]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[\text{unit}]$ by definition of the unary value interpretation.

- **Case:** $\tau = \tau_1 \times \tau_2$

In this case, we have that $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1 \times \tau_2]$. By definition, this means that $v_1 = \langle v'_1, v''_1 \rangle$ and $v_2 = \langle v'_2, v''_2 \rangle$ with $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1]$ and $(v''_1, v''_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_2]$. By the **IH**, we have that $v'_1 \in \mathcal{V}_{\Sigma_1}[\tau_1]$, $v'_2 \in \mathcal{V}_{\Sigma_2}[\tau_1]$, $v''_1 \in \mathcal{V}_{\Sigma_1}[\tau_2]$, and $v''_2 \in \mathcal{V}_{\Sigma_2}[\tau_2]$.

Then, by the definition of the unary interpretation, we have that $\langle v'_1, v''_1 \rangle \in \mathcal{V}_{\Sigma_1}[\tau_1 \times \tau_2]$ and $\langle v'_2, v''_2 \rangle \in \mathcal{V}_{\Sigma_2}[\tau_1 \times \tau_2]$, as required.

- **Case:** $\tau = t_\ell$

We proceed by casing on whether $\ell \sqsubseteq \xi$:

- $\ell \sqsubseteq \xi$:

In this case, by the definition of the binary interpretation, we have that $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[t]$. We proceed by casing on t :

- **Case:** $t = \tau_1 + \tau_2$

By the definition of the binary interpretation, we have that either $v_1 = 1 \cdot v'_1, v_2 = 1 \cdot v'_2 \wedge (v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1]$ or $v_1 = 2 \cdot v'_1, v_2 = 2 \cdot v'_2 \wedge (v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_2]$.

WLOG, suppose it is the case that $v_1 = 1 \cdot v'_1$ and $v_2 = 1 \cdot v'_2$. In this case, we have $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau_1]$. By the **IH**, we have that $v'_1 \in \mathcal{V}_{\Sigma_1}[\tau_1]$ and $v'_2 \in \mathcal{V}_{\Sigma_2}[\tau_1]$, which gives us that $1 \cdot v'_1 \in \mathcal{V}_{\Sigma_1}[(\tau_1 + \tau_2)_\ell]$ and $1 \cdot v'_2 \in \mathcal{V}_{\Sigma_2}[(\tau_1 + \tau_2)_\ell]$ by definition of the unary value interp.

– **Case:** $t = \tau'$ result

By the definition of the binary interpretation, we have that either $v_1 = v_2 = \text{Error}$ or $v_1 = \text{Ok}(v'_1), v_2 = \text{Ok}(v'_2)$ and $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau']$.

In the former case, we immediately have that $v_1 \in \mathcal{V}_{\Sigma_1}[\tau' \text{ result}_\ell]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[\tau' \text{ result}_\ell]$.

In the latter case, by the **IH** we have that $v'_1 \in \mathcal{V}_{\Sigma_1}[\tau']$ and $v'_2 \in \mathcal{V}_{\Sigma_2}[\tau']$, which gives us that $\text{Ok}(v'_1) \in \mathcal{V}_{\Sigma_1}[\tau' \text{ result}_\ell]$ and $\text{Ok}(v'_2) \in \mathcal{V}_{\Sigma_2}[\tau' \text{ result}_\ell]$.

– **Case:** $t = \text{enc}_{\ell'} \tau$

By the definition of the binary value interpretation, we have that $\exists v'_1, v_{k1}. v'_1 = \mathcal{D}(v_{k1}, v_1)$ and $\exists v'_2, v_{k2}. v'_2 = \mathcal{D}(v_{k2}, v_2)$.

We proceed by casing on whether $\ell' \sqsubseteq \xi$:

• $\ell' \sqsubseteq \xi$:

In this case, we have that $(v'_1, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau]$. By the **IH**, we have that $v'_1 \in \mathcal{V}_{\Sigma_1}[\tau]$ and $v'_2 \in \mathcal{V}_{\Sigma_2}[\tau]$, which gives us what we need to show for $v_1 \in \mathcal{V}_{\Sigma_1}[(\text{enc}_{\ell'} \tau)_\ell]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[(\text{enc}_{\ell'} \tau)_\ell]$.

• $\ell' \not\sqsubseteq \xi$:

In this case, we have that $v'_1 \in \mathcal{V}_{\Sigma_1}[\tau]$ and $v'_2 \in \mathcal{V}_{\Sigma_2}[\tau]$, which immediately gives us that $v_1 \in \mathcal{V}_{\Sigma_1}[(\text{enc}_{\ell'} \tau)_\ell]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[(\text{enc}_{\ell'} \tau)_\ell]$.

• $\ell \not\sqsubseteq \xi$:

In this case, by the definition of the binary interpretation, we have that $v_1 \in \mathcal{V}_{\Sigma_1}[t]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[t]$. By the definition of the unary interpretation, we then have $v_1 \in \mathcal{V}_{\Sigma_1}[t_\ell]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[t_\ell]$, as required.

• **Case:** $\tau = \tau_1 \xrightarrow{\ell_k} \tau_2$

By the definition of the binary interpretation, we immediately have that $v_1 \in \mathcal{V}_{\Sigma_1}[\tau_1 \xrightarrow{\ell_k} \tau_2]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[\tau_1 \xrightarrow{\ell_k} \tau_2]$.

• **Case:** $\tau = \text{key}_\ell$

By the definition of the binary value interpretation, we have $v_1 = \text{key}\langle K_2 \rangle$ and $v_2 = \text{key}\langle K_2 \rangle$ for $K_1 \sim \ell \in \Sigma_1$ and $K_2 \sim \ell \in \Sigma_2$. This immediately gives that $\text{key}\langle K_1 \rangle \in \mathcal{V}_{\Sigma_1}[\text{key}_\ell]$ and $\text{key}\langle K_2 \rangle \in \mathcal{V}_{\Sigma_2}[\text{key}_\ell]$ by the definition of the unary value interp. □

Lemma 57. *If $\gamma \equiv_\xi \gamma' : \Gamma; \Sigma \uplus \Sigma'$, then $\gamma : \Gamma; \Sigma$ and $\gamma' : \Gamma; \Sigma'$.*

Proof. Suppose we have $\gamma \equiv_\xi \gamma' : \Gamma; \Sigma \uplus \Sigma'$. By definition, this means that $\forall x : \tau_1 \in \Gamma$, we have that $(\gamma(x), \gamma'(x)) \in \mathcal{V}_{\Sigma, \Sigma'}^\xi[\tau]$, $\gamma :_{\text{LD}} \Gamma; \Sigma$, and $\gamma' :_{\text{LD}} \Gamma; \Sigma'$.

By Lemma 11, we have that $\gamma(x) \in \mathcal{V}_\Sigma[\tau]$ and $\gamma'(x) \in \mathcal{V}_{\Sigma'}[\tau]$. With the leaf-determinism conditions that we already have, we get that $\gamma : \Gamma; \Sigma$ and $\gamma' : \Gamma; \Sigma'$. □

Lemma 58 (Value Splitting Lemma). *If $\ell \triangleleft \tau$ and $\ell \not\sqsubseteq \xi$, then if $v \in \mathcal{V}_{\Sigma_1}[\tau]$ and $v' \in \mathcal{V}_{\Sigma_2}[\tau]$, then $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[\tau]$.*

Proof. We proceed by rule induction on the judgment $\ell \triangleleft \tau$:

- **Case:** $\frac{\ell \sqsubseteq \ell'}{\ell \triangleleft t_{\ell'}}$

Since $\ell \sqsubseteq \ell'$ and $\ell \not\sqsubseteq \xi$, it must be the case that $\ell' \not\sqsubseteq \xi$ (Lemma 28).

By the definition of the binary value interpretation, to show $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[t_{\ell'}]]$, we need to show that $v \in \mathcal{V}_{\Sigma_1}[[t]]$ and $v \in \mathcal{V}_{\Sigma_2}[[t]]$. This is immediate from our assumptions.

- **Cases:** $\frac{}{\ell \triangleleft \text{unit}}$

To show that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[\text{unit}]]$, we must show that $v = v' = \langle \rangle$.

From the unary term interpretation, we already have that $v = \langle \rangle$ and $v' = \langle \rangle$, which gives us what we want to show.

- **Case:** $\frac{\ell \triangleleft \tau_1 \quad \ell \triangleleft \tau_2}{\ell \triangleleft \tau_1 \times \tau_2}$

To show that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[\tau_1 \times \tau_2]]$, we must show that $v = \langle v_1, v_2 \rangle$, $v' = \langle v'_1, v'_2 \rangle$ such that $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[\tau_1]]$ and $(v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[\tau_2]]$.

From our assumptions, since $v \in \mathcal{V}_{\Sigma_1}[[\tau_1 \times \tau_2]]$ and $v' \in \mathcal{V}_{\Sigma_2}[[\tau_1 \times \tau_2]]$, we have that

- $v = \langle v_1, v_2 \rangle$ with $v_1 \in \mathcal{V}_{\Sigma_1}[[\tau_1]]$ and $v_2 \in \mathcal{V}_{\Sigma_2}[[\tau_2]]$
- $v' = \langle v'_1, v'_2 \rangle$ with $v'_1 \in \mathcal{V}_{\Sigma_2}[[\tau_1]]$ and $v'_2 \in \mathcal{V}_{\Sigma_2}[[\tau_2]]$

From the premises, we have that $\ell \triangleleft \tau_1$ and $\ell \triangleleft \tau_2$, alongside $\ell \not\sqsubseteq \xi$ from our assumptions.

Given that, by the **IH**, we have that $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[\tau_1]]$ and $(v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[\tau_2]]$, which is precisely what we want to show.

- **Case:** $\frac{\ell \sqsubseteq \ell_k \quad \ell \triangleleft \tau_2}{\ell \triangleleft \tau_1 \xrightarrow{\ell_k} \tau_2}$

To show that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^{\xi}[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$, we must show that $v = \lambda(x_1 : \tau_1.e_1)$, $v' = \lambda(x_2 : \tau_2.e_2)$ such that for all $\Sigma'_1 \leq \Sigma_1$ and $\Sigma'_2 \leq \Sigma_2$, if $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[[\tau_1]]$ and $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_2}[[\tau_1]]$ such that $\forall (v_1, v'_1) \in \mathbb{V}_1 \times \mathbb{V}'_1$, $(v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^{\xi}[[\tau_1]]$, then $([v_1/x_1]e_1, [v'_1/x_2]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^{\xi}[[\tau_2]]$

(for all (v_1, v'_1)), as well as $v \in \mathcal{V}_{\Sigma_1}[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$ and $v' \in \mathcal{V}_{\Sigma_2}[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$.

The latter two proof goals are immediate from our assumptions.

From our assumptions, since $v \in \mathcal{V}_{\Sigma_1}[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$ and $v' \in \mathcal{V}_{\Sigma_2}[[\tau_1 \xrightarrow{\ell_k} \tau_2]]$, we have that

- $v = \lambda(x_1 : \tau_1.e_1)$ such that $\forall \Sigma'_1 \leq \Sigma_1$, if $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1}[[\tau_1]]$ such that $\forall v_1 \in \mathbb{V}_1$, $v_1 \in \mathcal{V}_{\Sigma'_1}[[\tau_1]]$, then $[v_1/x_1]e_1 \in \mathcal{E}_{\Sigma'_1}[[\tau_2]][\ell_k]$
- $v' = \lambda(x_2 : \tau_1.e_2)$ such that $\forall \Sigma'_2 \leq \Sigma_2$, if $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_2}[[\tau_1]]$ such that $\forall v'_1 \in \mathbb{V}'_1$, $v'_1 \in \mathcal{V}_{\Sigma'_2}[[\tau_1]]$, then $[v'_1/x_2]e_2 \in \mathcal{E}_{\Sigma'_2}[[\tau_2]][\ell_k]$

Suppose we have $\mu \equiv_{\xi} \mu' : \Sigma'_1 \uplus \Sigma'_2$. By definition, this gives us $\mu : \Sigma'_1$ and $\mu' : \Sigma'_2$. Unrolling the unary term interpretation, we have

- Since $[v_1/x_1]e_1 \in \mathcal{E}_{\Sigma'_1}[[\tau_2]][\ell_k]$,

$$\nu_{\Sigma'_1} \{ [v_1/x_1]e_1 \parallel \mu \} \Downarrow \nu_{\Sigma'_1} \{ \mathbb{V}_2 \parallel \mu_1 \}$$

such that $\mu_1 : \Sigma''_1$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma''_1}[[\tau_2]]$$

and $\forall K_1 \sim \ell_1 \in (\Sigma''_1 \setminus \Sigma'_1). \ell_k \sqsubseteq \ell_1$

- Since $[v'_1/x_2]e_2 \in \mathcal{E}_{\Sigma'_2}[\tau_2][\ell_k]$,

$$\nu\Sigma'_2\{[v'_1/x_2]e_2 \parallel \mu'\} \Downarrow \nu\Sigma''_2\{\mathbb{V}'_2 \parallel \mu_2\}$$

such that $\mu_2 : \Sigma''_2$ and

$$\forall v'_2 \in \mathbb{V}'_2. v'_2 \in \mathcal{V}_{\Sigma''_2}[\tau_2]$$

and $\forall K_2 \sim \ell_2 \in (\Sigma''_2 \setminus \Sigma'_2). \ell_k \sqsubseteq \ell_2$

To show that $([v_1/x_1]e_1, [v'_1/x_2]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_2]$, we must show that

- If $\mu \equiv_\xi \mu' : \Sigma'_1 \uplus \Sigma'_2$ then

$$\nu\Sigma_1\{[v_1/x_1]e_1 \parallel \mu\} \Downarrow \nu\Sigma''_1\{\mathbb{V}_2 \parallel \mu_1\}$$

$$\nu\Sigma_2\{[v'_1/x_2]e_2 \parallel \mu'\} \Downarrow \nu\Sigma''_2\{\mathbb{V}'_2 \parallel \mu_2\}$$

such that $\mu_1 \equiv_\xi \mu_2 : \Sigma''_1 \uplus \Sigma''_2$ and

$$\forall v_2 \in \mathbb{V}_2, \exists v'_2 \in \mathbb{V}'_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma''_1, \Sigma''_2}^\xi[\tau_2]$$

$$\forall v'_2 \in \mathbb{V}'_2, \exists v_2 \in \mathbb{V}_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma''_1, \Sigma''_2}^\xi[\tau_2]$$

Note that since $\ell \sqsubseteq \ell_k$ and $\ell \not\sqsubseteq \xi$, we have that $\ell_k \not\sqsubseteq \xi$ (Lemma 28). As such, since each of the effects satisfy $\ell_k \sqsubseteq \ell_1$ and $\ell_k \sqsubseteq \ell_2$, we also have that $\ell_1 \not\sqsubseteq \xi$ and $\ell_2 \not\sqsubseteq \xi$ (Lemma 28). That is, neither $[v_1/x_1]e_1$ nor $[v'_1/x_2]e_2$ produce observable effects. Since $\forall K_1 \sim \ell_1 \in (\Sigma''_1 \setminus \Sigma'_1). \text{kc} \sqsubseteq \ell_1, \forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma). \text{kc} \sqsubseteq \ell_2$, with $\ell_1 \not\sqsubseteq \xi$ and $\ell_2 \not\sqsubseteq \xi$, we have that $\mu_1 : \Sigma''_1$ and $\mu_2 : \Sigma''_2$ implies $\mu_1 \equiv_\xi \mu_2 : \Sigma''_1 \uplus \Sigma''_2$. This is because we already had that $\mu \equiv_\xi \mu' : \Sigma'_1 \uplus \Sigma'_2$, and we additionally have that $\Sigma''_1 \leq \Sigma'_1$ and $\Sigma''_2 \leq \Sigma'_2$, meaning any observable keys in the memory maintain their relatedness and any new keys are unobservable and thus can be arbitrary.

Since we have $\ell \triangleleft \tau_2$, by the **IH** on values in \mathbb{V}_2 and \mathbb{V}'_2 , we have that $\forall v_2 \in \mathbb{V}_2, \forall v'_2 \in \mathbb{V}'_2, (v_2, v'_2) \in \mathcal{E}_{\Sigma''_1, \Sigma''_2}^\xi[\tau_2]$. This gives us what we want to show for $([v_1/x_1]e_1, [v'_1/x_2]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_2]$.

So far, we have that $\forall v_1 \in \mathbb{V}_1$ and $\forall v'_1 \in \mathbb{V}'_1$ that $([v_1/x_1]e_1, [v'_1/x_2]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_2]$, where $v_1 \in \mathcal{V}_{\Sigma'_1}[\tau_1]$ and $v'_1 \in \mathcal{V}_{\Sigma'_1}[\tau_1]$. We would like to show that $\forall (v_1, v'_1) \in \mathbb{V}_1 \times \mathbb{V}'_1$ with $(v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_1]$, then $([v_1/x_1]e_1, [v'_1/x_2]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_2]$.

By Lemma 11, we have that if $(v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_1]$, then $v_1 \in \mathcal{V}_{\Sigma'_1}[\tau_1]$ and $v'_1 \in \mathcal{V}_{\Sigma'_2}[\tau_1]$.

Thus, given the above results, we immediately have that if $(v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_1]$ then $([v_1/x_1]e_1, [v'_1/x_2]e_2) \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi[\tau_2]$, as required.

- **Case:** $\frac{\ell \sqsubseteq \ell'}{\ell \triangleleft \text{key}_{\ell'}}$

Since $\ell \sqsubseteq \ell'$ from the premise and $\ell \not\sqsubseteq \xi$, we have that $\ell' \not\sqsubseteq \xi$. As such, by the definition of the binary value interpretation, we need to show that $v \in \mathcal{V}_{\Sigma_1}^\xi[\text{key}_{\ell'}]$ and $v' \in \mathcal{V}_{\Sigma_2}^\xi[\text{key}_{\ell'}]$, which is immediate from our assumptions.

□

Lemma 59 (Term Splitting Lemma). *If $\ell \triangleleft \tau$ and $\ell \not\preceq \xi$, then if $e \in \mathcal{E}_\Sigma[[\tau]][\text{kc}]$ and $e' \in \mathcal{E}_{\Sigma'}[[\tau]][\text{kc}]$ and $\text{kc} \not\preceq \xi$, then $(e, e') \in \mathcal{E}_{\Sigma, \Sigma'}^\xi[[\tau]]$.*

Proof. Suppose we have that $e \in \mathcal{E}_\Sigma[[\tau]][\text{kc}]$ and $e' \in \mathcal{E}_{\Sigma'}[[\tau]][\text{kc}]$ and $\text{kc} \not\preceq \xi$. Suppose we have $\mu \equiv_\xi \mu' : \Sigma \uplus \Sigma'$, which by definition gives us $\mu : \Sigma$ and $\mu' : \Sigma'$. By the definition of the unary term interpretation, this means that

- Since $e \in \mathcal{E}_\Sigma[[\tau]][\text{kc}]$,

$$\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$$

such that $\mu_1 : \Sigma_1$ and

$$\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}[[\tau]]$$

and $\forall K_1 \sim \ell_1 \in (\Sigma_1 \setminus \Sigma). \text{kc} \sqsubseteq \ell_1$

- Since $e' \in \mathcal{E}_{\Sigma'}[[\tau]][\text{kc}]$,

$$\nu\Sigma'\{e' \parallel \mu'\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}$$

such that $\mu_2 : \Sigma_2$ and

$$\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}[[\tau]]$$

and $\forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma'). \text{kc} \sqsubseteq \ell_2$

To show that $(e, e') \in \mathcal{E}_{\Sigma, \Sigma'}^\xi[[\tau]]$, we must show that

- If $\mu \equiv_\xi \mu' : \Sigma \uplus \Sigma'$ then

$$\nu\Sigma\{e \parallel \mu\} \Downarrow \nu\Sigma_1\{\mathbb{V}_1 \parallel \mu_1\}$$

$$\nu\Sigma'\{e' \parallel \mu'\} \Downarrow \nu\Sigma_2\{\mathbb{V}_2 \parallel \mu_2\}$$

such that $\mu_1 \equiv_\xi \mu_2 : \Sigma_1 \uplus \Sigma_2$ and

$$\forall v_1 \in \mathbb{V}_1, \exists v_2 \in \mathbb{V}_2. (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[[\tau]]$$

$$\forall v_2 \in \mathbb{V}_2, \exists v_1 \in \mathbb{V}_1. (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[[\tau]]$$

Note that since $\text{kc} \not\preceq \xi$, since each of the effects satisfy $\text{kc} \sqsubseteq \ell_1$ and $\text{kc} \sqsubseteq \ell_2$, we also have that $\ell_1 \not\preceq \xi$ and $\ell_2 \not\preceq \xi$ (Lemma 28). That is, neither e nor e' produce observable effects. Since $\forall K_1 \sim \ell_1 \in (\Sigma_1 \setminus \Sigma). \text{kc} \sqsubseteq \ell_1, \forall K_2 \sim \ell_2 \in (\Sigma_2 \setminus \Sigma'). \text{kc} \sqsubseteq \ell_2$, with $\ell_1 \not\preceq \xi$ and $\ell_2 \not\preceq \xi$, we have that $\mu_1 : \Sigma_1$ and $\mu_2 : \Sigma_2$ implies $\mu_1 \equiv_\xi \mu_2 : \Sigma_1 \uplus \Sigma_2$. This is because we already had that $\mu \equiv_\xi \mu' : \Sigma \uplus \Sigma'$, and we additionally have that $\Sigma_1 \leq \Sigma$ and $\Sigma_2 \leq \Sigma'$ (Lemma 24), meaning any observable keys in the memory maintain their relatedness and any new keys are unobservable and thus can be arbitrary.

From Lemma 12, we know that with $\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma_1}[[\tau]]$ and $\forall v_2 \in \mathbb{V}_2. v_2 \in \mathcal{V}_{\Sigma_2}[[\tau]]$, we get that $\forall v_1 \in \mathbb{V}_1. v_2 \in \mathbb{V}_2. (v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi[[\tau]]$, which is sufficient to show the double containment required by the binary term interpretation. □

Lemma 60 (Un-Subtype). *If $\tau' \leq \tau$, then if $v \in \mathcal{V}_\Sigma[[\tau']]$, then $v \in \mathcal{V}_\Sigma[[\tau]]$.*

Proof. Suppose we have $\tau' \leq \tau$ and $v \in \mathcal{V}_\Sigma[\tau']$. We proceed by rule induction on $\tau' \leq \tau$:

- **Case:**
$$\frac{\tau'_1 \leq \tau_1 \quad \tau'_2 \leq \tau_2 \quad \ell_1 \sqsubseteq \ell_2}{(\tau'_1 + \tau'_2)_{\ell_1} \leq (\tau_1 + \tau_2)_{\ell_2}}$$

In this case, we have that $v \in \mathcal{V}_\Sigma[(\tau'_1 + \tau'_2)_{\ell_1}]$. By the definition of the value interpretation, this means that $v \in \mathcal{V}_\Sigma[\tau'_1 + \tau'_2]$, which then means that either $v = 1 \cdot v_1$ for $v_1 \in \mathcal{V}_\Sigma[\tau'_1]$ or $v = 2 \cdot v_2$ for $v_2 \in \mathcal{V}_\Sigma[\tau'_2]$.

WLOG, suppose it is the case that $v = 1 \cdot v_1$. By the **IH**, since $\tau'_1 \leq \tau_1$ and $v_1 \in \mathcal{V}_\Sigma[\tau'_1]$, we have that $v_1 \in \mathcal{V}_\Sigma[\tau_1]$, which gives us that $1 \cdot v_1 \in \mathcal{V}_\Sigma[\tau_1 + \tau_2]$, which then implies that $v_1 \in \mathcal{V}_\Sigma[(\tau_1 + \tau_2)_{\ell_1}]$, all by definition of the value interpretation.

- **Case:**
$$\frac{\tau'_1 \leq \tau_1 \quad \tau'_2 \leq \tau_2}{\tau'_1 \times \tau'_2 \leq \tau_1 \times \tau_2}$$

In this case, we have that $v \in \mathcal{V}_\Sigma[\tau'_1 \times \tau'_2]$. By the definition of the value interpretation, this means that $v = \langle v_1, v_2 \rangle$ for $v_1 \in \mathcal{V}_\Sigma[\tau'_1]$ and $v_2 \in \mathcal{V}_\Sigma[\tau'_2]$.

By the **IH**, since $\tau'_1 \leq \tau_1$ and $\tau'_2 \leq \tau_2$, we have that $v_1 \in \mathcal{V}_\Sigma[\tau_1]$ and $v_2 \in \mathcal{V}_\Sigma[\tau_2]$, which gives us that $v \in \mathcal{V}_\Sigma[\tau_1 \times \tau_2]$.

- **Case:**
$$\frac{\tau_1 \leq \tau'_1 \quad \tau'_2 \leq \tau_2 \quad \ell_k \sqsubseteq \ell'_k}{\tau'_1 \xrightarrow{\ell'_k} \tau'_2 \leq \tau_1 \xrightarrow{\ell_k} \tau_2}$$

In this case, we have that $v \in \mathcal{V}_\Sigma[\tau'_1 \xrightarrow{\ell'_k} \tau'_2]$. By the definition of the value interpretation, this means that $v = \lambda(x.e)$ such that for all Σ' such that $\Sigma' \leq \Sigma$ and for all \mathbb{V}_1 such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_1]$ and $\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma'}[\tau'_1]$, we have that $[v_1/x]e \in \mathcal{E}_{\Sigma'}[\tau'_2][\ell'_k]$.

We would like to show that $v \in \mathcal{V}_\Sigma[\tau_1 \xrightarrow{\ell_k} \tau_2]$. We already have that $v = \lambda(x.e)$.

Suppose that we have some $\Sigma' \leq \Sigma$ and set $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'}[\tau_1]$ with $\forall v_1 \in \mathbb{V}_1. v_1 \in \mathcal{V}_{\Sigma'}[\tau_1]$. By the **IH**, since $\tau_1 \leq \tau'_1$, we have that $v_1 \in \mathcal{V}_{\Sigma'}[\tau'_1]$. From the previous reasoning, this means we can obtain that $[v_1/x]e \in \mathcal{E}_{\Sigma'}[\tau'_2][\ell'_k]$.

Unfolding the definition of the term interpretation, we have

- Since $[v_1/x]e \in \mathcal{E}_{\Sigma'}[\tau'_2][\ell'_k]$, if $\mu : \Sigma'$, then

$$\nu^{\Sigma'}\{[v_1/x]e \parallel \mu\} \Downarrow \nu^{\Sigma^*}\{\mathbb{V} \parallel \mu^*\}$$

such that $\mu^* : \Sigma^*$ and

$$\forall v'_2 \in \mathbb{V}. v'_2 \in \mathcal{V}_{\Sigma^*}[\tau'_2]$$

and $\forall K \sim \ell \in (\Sigma^* \setminus \Sigma'). \ell'_k \sqsubseteq \ell$.

By the **IH**, we have that each v'_2 is in $\mathcal{V}_{\Sigma^*}[\tau_2]$. Also, note that since $\ell_k \sqsubseteq \ell'_k$, for all keys in $\Sigma^* \setminus \Sigma'$, the levels being greater than or equal to ℓ'_k implies they are greater than or equal to ℓ_k .

With this, we have what we need to show for the term interpretation $[v_1/x]e \in \mathcal{E}_{\Sigma'}[\tau_2][\ell_k]$.

- **Case:**
$$\frac{\tau_1 \leq \tau_2 \quad \epsilon_1 \sqsubseteq \epsilon_2}{(\text{enc}_\ell \tau_1)_{\epsilon_1} \leq (\text{enc}_\ell \tau_2)_{\epsilon_2}}$$

In this case, we have that $v \in \mathcal{V}_\Sigma[(\text{enc}_\ell \tau_1)_{\epsilon_1}]$. By the definition of the value interpretation, this means that $v \in \mathcal{V}_\Sigma[\text{enc}_\ell \tau_1]$, which then means that $\exists v', v_k. v = \mathcal{D}(v_k, v')$ and $v' \in \mathcal{V}_\Sigma[\tau_1]$.

By the **IH**, we have that $v' \in \mathcal{V}_\Sigma \llbracket \tau_2 \rrbracket$, and with the existing v_k , we have what we want to show for $v \in \mathcal{V}_\Sigma \llbracket (\text{enc}_\ell \tau_2)_{e_2} \rrbracket$.

- **Omitted:** unit, key

□

Lemma 61 (Bin-Subtype). *If $\tau' \leq \tau$, then if $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau' \rrbracket$, then $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau \rrbracket$.*

Proof. Suppose we have $\tau' \leq \tau$ and $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau' \rrbracket$. We proceed by rule induction on $\tau' \leq \tau$:

- **Case:**
$$\frac{\tau'_1 \leq \tau_1 \quad \tau'_2 \leq \tau_2 \quad \ell_1 \sqsubseteq \ell_2}{(\tau'_1 + \tau'_2)_{\ell_1} \leq (\tau_1 + \tau_2)_{\ell_2}}$$

In this case, we have that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\tau'_1 + \tau'_2)_{\ell_1} \rrbracket$.

We proceed by casing on whether $\ell_1 \sqsubseteq \xi$:

- $\ell_1 \sqsubseteq \xi$:

By the definition of the value interpretation, we have that either

- $v = 1 \cdot v_1$ and $v' = 1 \cdot v'_1$ for $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau'_1 \rrbracket$, or
- $v = 2 \cdot v_2$ and $v' = 2 \cdot v'_2$ for $(v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau'_2 \rrbracket$

WLOG, suppose it is the case that $v = 1 \cdot v_1$ and $v' = 1 \cdot v'_1$. By the **IH**, since $\tau'_1 \leq \tau_1$ and $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau'_1 \rrbracket$, we have that $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 \rrbracket$.

We proceed by casing on whether $\ell_2 \sqsubseteq \xi$:

- $\ell_2 \sqsubseteq \xi$:

In this case, we must show that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$, which we have immediately.

- $\ell_2 \not\sqsubseteq \xi$:

In this case, we must show that $v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$ and $v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_1 + \tau_2 \rrbracket$. By the definition of the unary interpretation, this means either $v = 1 \cdot v_1$ with $v_1 \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_1 \rrbracket$ or $v = 2 \cdot v_2$ with $v_2 \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_2 \rrbracket$ (and similarly for v'). We already have that $v = 1 \cdot v_1$ and $v' = 1 \cdot v'_1$, and we have that $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 \rrbracket$. By the Lemma 11, we also have that $v_1 \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_1 \rrbracket$ and $v'_1 \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_1 \rrbracket$, as required.

- $\ell_1 \not\sqsubseteq \xi$:

By the definition of the value interpretation, we have that $v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau'_1 + \tau'_2 \rrbracket$ and $v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau'_1 + \tau'_2 \rrbracket$.

Note that since $\ell_1 \not\sqsubseteq \xi$ and $\ell_1 \sqsubseteq \ell_2$, it must be the case that $\ell_2 \not\sqsubseteq \xi$ (Lemma 28).

As such, it is sufficient to show that $v \in \mathcal{V}_{\Sigma_1} \llbracket \tau_1 + \tau_2 \rrbracket$ and $v' \in \mathcal{V}_{\Sigma_2} \llbracket \tau_1 + \tau_2 \rrbracket$. This follows from Lemma 30.

- **Case:**
$$\frac{\tau'_1 \leq \tau_1 \quad \tau'_2 \leq \tau_2}{\tau'_1 \times \tau'_2 \leq \tau_1 \times \tau_2}$$

In this case, we have that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau'_1 \times \tau'_2 \rrbracket$. By the definition of the value interpretation, this means that $v = \langle v_1, v_2 \rangle$ and $v' = \langle v'_1, v'_2 \rangle$ for $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau'_1 \rrbracket$ and $(v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau'_2 \rrbracket$.

By the **IH**, since $\tau'_1 \leq \tau_1$ and $\tau'_2 \leq \tau_2$, we have that $(v_1, v'_1) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 \rrbracket$ and $(v_2, v'_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_2 \rrbracket$, which gives us that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 \times \tau_2 \rrbracket$.

• **Case:**
$$\frac{\tau_1 \leq \tau'_1 \quad \tau'_2 \leq \tau_2 \quad \ell_k \sqsubseteq \ell'_k}{\tau'_1 \xrightarrow{\ell'_k} \tau'_2 \leq \tau_1 \xrightarrow{\ell_k} \tau_2}$$

In this case, we have that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau'_1 \xrightarrow{\ell'_k} \tau'_2 \rrbracket$. By the definition of the value interpretation, this means that $v =_\alpha \lambda(x.e)$ and $v' =_\alpha \lambda(x.e')$ such that for all Σ'_1, Σ'_2 such that $\Sigma'_1 \leq \Sigma_1$ and $\Sigma'_2 \leq \Sigma_2$ such that for all $\forall \mathbb{V}_1, \mathbb{V}'_1$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1} \llbracket \tau_1 \rrbracket$, $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_2} \llbracket \tau_1 \rrbracket$, and $\forall (v_1, v'_1) \in \mathbb{V}_1 \times \mathbb{V}'_1$, $(v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau'_1 \rrbracket$, we have that $([v_1/x]e, [v'_1/x]e') \in \mathcal{E}_{\Sigma'}^\xi \llbracket \tau'_2 \rrbracket$.

We would like to show that $(v, v') \in \mathcal{V}_{\Sigma}^\xi \llbracket \tau_1 \xrightarrow{\ell_k} \tau_2 \rrbracket$. We already have that $v = \lambda(x.e)$ and $v' = \lambda(x.e')$.

Suppose that we have some $\Sigma'_1 \leq \Sigma_1$ and $\Sigma'_2 \leq \Sigma_2$ and $\mathbb{V}_1, \mathbb{V}'_1$ such that $\mathbb{V}_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_1} \llbracket \tau_1 \rrbracket$, $\mathbb{V}'_1 \in \mathcal{L}\mathcal{V}_{\Sigma'_2} \llbracket \tau_1 \rrbracket$, and $\forall (v_1, v'_1) \in \mathbb{V}_1 \times \mathbb{V}'_1$, $(v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau_1 \rrbracket$. By the **IH**, since $\tau_1 \leq \tau'_1$, we have that $(v_1, v'_1) \in \mathcal{V}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau'_1 \rrbracket$. From the previous reasoning, this means we can obtain that $([v_1/x]e, [v'_1/x]e') \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau'_2 \rrbracket$.

Suppose we have $\mu \equiv_\xi \mu' : \Sigma'_1 \uplus \Sigma'_2$. Unfolding the definition of the term interpretation, we have

- Since $([v_1/x]e, [v'_1/x]e') \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau'_2 \rrbracket$,

$$\nu_{\Sigma'_1} \{ [v_1/x]e \parallel \mu \} \Downarrow \nu_{\Sigma^*} \{ \mathbb{V}_2 \parallel \mu^* \}$$

$$\nu_{\Sigma'_2} \{ [v'_1/x]e' \parallel \mu' \} \Downarrow \nu_{\Sigma^{**}} \{ \mathbb{V}'_2 \parallel \mu^{**} \}$$

such that $\mu^* \equiv_\xi \mu^{**} : \Sigma^*, \Sigma^{**}$ and

$$\forall v_2 \in \mathbb{V}_2. \exists v'_2 \in \mathbb{V}'_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma^*, \Sigma^{**}}^\xi \llbracket \tau'_2 \rrbracket$$

$$\forall v'_2 \in \mathbb{V}'_2. \exists v_2 \in \mathbb{V}_2. (v_2, v'_2) \in \mathcal{V}_{\Sigma^*, \Sigma^{**}}^\xi \llbracket \tau'_2 \rrbracket$$

By the **IH**, we have that each double contained pair (v_2, v'_2) is in $\mathcal{V}_{\Sigma^*, \Sigma^{**}}^\xi \llbracket \tau_2 \rrbracket$.

With this, we have what we need to show for the term interpretation $([v_1/x]e, [v'_1/x]e') \in \mathcal{E}_{\Sigma'_1, \Sigma'_2}^\xi \llbracket \tau_2 \rrbracket$.

• **Case:**
$$\frac{\tau_1 \leq \tau_2 \quad \epsilon_1 \sqsubseteq \epsilon_2}{(\text{enc}_\ell \tau_1)_{\epsilon_1} \leq (\text{enc}_\ell \tau_2)_{\epsilon_2}}$$

In this case, we have that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\text{enc}_\ell \tau_1)_{\epsilon_1} \rrbracket$.

We proceed by casing on whether $\epsilon_1 \sqsubseteq \xi$:

- $\epsilon_1 \sqsubseteq \xi$:

This means that we have $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \text{enc}_\ell \tau_1 \rrbracket$.

By the definition of the binary value interpretation, this means we have $\exists v_i, v_{ki} \cdot v_1 = \mathcal{D}(v_{k1}, v)$ and $v_2 = \mathcal{D}(v_{k2}, v')$ for $i \in \{1, 2\}$.

We proceed by casing on whether $\ell \sqsubseteq \xi$:

– $\ell \sqsubseteq \xi$:

In this case, we have that $v_{k1} = v_{k2}$ and $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_1 \rrbracket$. By the **IH**, we have that $(v_1, v_2) \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket \tau_2 \rrbracket$.

For $\epsilon_2 \sqsubseteq \xi$, with all of the above results, we have that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\text{enc}_{\tau_2} \ell)_{\epsilon_2} \rrbracket$.

For $\epsilon_2 \not\sqsubseteq \xi$, by Lemma 11, we have that $v_1 \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_1 \rrbracket$ and $v_2 \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_1 \rrbracket$, which then allows us to show $v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket (\text{enc}_{\tau_2} \ell)_{\epsilon_2} \rrbracket$ and $v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket (\text{enc}_{\tau_2} \ell)_{\epsilon_2} \rrbracket$.

– $\ell \not\sqsubseteq \xi$:

In this case, we have that $v_1 \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_1 \rrbracket$, $v_2 \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_1 \rrbracket$, and $v \doteq v'$. By the **IH**, we have that $v_1 \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \tau_2 \rrbracket$ and $v_2 \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \tau_2 \rrbracket$.

For $\epsilon_2 \sqsubseteq \xi$, with all of the above results, we have that $(v, v') \in \mathcal{V}_{\Sigma_1, \Sigma_2}^\xi \llbracket (\text{enc}_{\tau_2} \ell)_{\epsilon_2} \rrbracket$.

For $\epsilon_2 \not\sqsubseteq \xi$, with the IH result we immediately have that $v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket (\text{enc}_{\tau_2} \ell)_{\epsilon_2} \rrbracket$ and $v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket (\text{enc}_{\tau_2} \ell)_{\epsilon_2} \rrbracket$.

▪ $\epsilon_1 \not\sqsubseteq \xi$:

This means that $v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \text{enc}_\ell \tau_1 \rrbracket$ and $v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \text{enc}_\ell \tau_1 \rrbracket$.

Note that since $\epsilon_1 \not\sqsubseteq \xi$ and $\epsilon_1 \sqsubseteq \epsilon_2$, it must be the case that $\epsilon_2 \not\sqsubseteq \xi$ (Lemma 28).

As such, it is sufficient to show that $v \in \mathcal{V}_{\Sigma_1}^\xi \llbracket \text{enc}_\ell \tau_2 \rrbracket$ and $v' \in \mathcal{V}_{\Sigma_2}^\xi \llbracket \text{enc}_\ell \tau_2 \rrbracket$. This follows from Lemma 30.

• **Omitted:** unit, key

□

Bibliography

- [1] Amal Ahmed, Derek Dreyer, and Andreas Rossberg. State-dependent representation independence. In *Proceedings of the 36th Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '09, pages 340–353, New York, NY, USA, 2009. Association for Computing Machinery. ISBN 9781605583792. doi: 10.1145/1480881.1480925. URL <https://doi.org/10.1145/1480881.1480925>. 1.2, 5.1
- [2] Aslan Askarov, Daniel Hedin, and Andrei Sabelfeld. Cryptographically-masked flows. *Theor. Comput. Sci.*, 402(2-3):82–101, 2008. doi: 10.1016/J.TCS.2008.04.028. URL <https://doi.org/10.1016/j.tcs.2008.04.028>. 1.1, 1.2, 2, 2.2, 2.3, 2.3, 1, 4.1, 4.3
- [3] Lars Birkedal, Bernhard Reus, Jan Schwinghammer, Kristian Støvring, Jacob Thamsborg, and Hongseok Yang. Step-indexed kripke models over recursive worlds. *SIGPLAN Not.*, 46(1):119–132, January 2011. ISSN 0362-1340. doi: 10.1145/1925844.1926401. URL <https://doi.org/10.1145/1925844.1926401>. 1.2, 5.1
- [4] Dorothy E. Denning. A lattice model of secure information flow. *Commun. ACM*, 19(5): 236–243, May 1976. ISSN 0001-0782. doi: 10.1145/360051.360056. URL <https://doi.org/10.1145/360051.360056>. 2.1
- [5] Jean-Yves Girard. *Interprétation fonctionnelle et élimination des coupures de l'arithmétique d'ordre supérieur*. PhD thesis, Université Paris VII, 1972. 1.1
- [6] Joseph A. Goguen and José Meseguer. Security policies and security models. In *1982 IEEE Symposium on Security and Privacy*, pages 11–11, 1982. doi: 10.1109/SP.1982.10014. 1.1
- [7] Simon Oddershede Gregersen, Johan Bay, Amin Timany, and Lars Birkedal. Mechanized logical relations for termination-insensitive noninterference. *Proc. ACM Program. Lang.*, 5(POPL):1–29, 2021. doi: 10.1145/3434291. URL <https://doi.org/10.1145/3434291>. 1.1, 1.2, 3.1, 4.4.1
- [8] Nevin Heintze and Jon G. Riecke. The slam calculus: programming with secrecy and integrity. In *Proceedings of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '98, page 365–377, New York, NY, USA, 1998. Association for Computing Machinery. ISBN 0897919793. doi: 10.1145/268946.268976. URL <https://doi.org/10.1145/268946.268976>. 1.2
- [9] Paul Blain Levy. *Call-By-Push-Value: A Subsuming Paradigm*, pages 27–47. Springer Netherlands, Dordrecht, 2003. ISBN 978-94-007-0954-6. doi: 10.1007/978-94-007-0954-6.2. URL <https://doi.org/10.1007/>

- [10] Daryl McCullough. Noninterference and the composability of security properties. In *Proceedings. 1988 IEEE Symposium on Security and Privacy*, pages 177–186, 1988. doi: 10.1109/SECPRI.1988.8110. 1.1, 4.1
- [11] John C. Mitchell and Eugenio Moggi. Kripke-style models for typed lambda calculus. *Annals of Pure and Applied Logic*, 51(1):99–124, 1991. ISSN 0168-0072. doi: [https://doi.org/10.1016/0168-0072\(91\)90067-V](https://doi.org/10.1016/0168-0072(91)90067-V). URL <https://www.sciencedirect.com/science/article/pii/016800729190067V>. 1.2, 5.1
- [12] Andrew M. Pitts and Ian Stark. Operational reasoning for functions with local state. *Higher Order Operational Techniques in Semantics (HOOTS)*, pages 227–273, 1998. 1.1
- [13] Gordon D. Plotkin. Lambda-definability and logical relations. Technical report, University of Edinburgh, 1973. 1.1
- [14] François Pottier and Vincent Simonet. Information flow inference for ML. *ACM Trans. Program. Lang. Syst.*, 25(1):117–158, 2003. doi: 10.1145/596980.596983. URL <https://doi.org/10.1145/596980.596983>. 1.2, 3.1, 3.2
- [15] Vineet Rajani and Deepak Garg. On the expressiveness and semantics of information flow types. *Journal of Computer Security*, 28(1):129–156, 2020. doi: 10.3233/JCS-191382. URL <https://doi.org/10.3233/JCS-191382>. 1.2, 3.1
- [16] Andrei Sabelfeld and Andrew C. Myers. Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21(1):5–19, 2003. doi: 10.1109/JSAC.2002.806121. 1.1
- [17] Andrei Sabelfeld and David Sands. Dimensions and principles of declassification. In *18th IEEE Computer Security Foundations Workshop (CSFW'05)*, pages 255–269, 2005. doi: 10.1109/CSFW.2005.15. 1.1, 1.1
- [18] Geoffrey Smith and Dennis Volpano. Secure information flow in a multi-threaded imperative language. In *Proceedings of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '98*, page 355–364, New York, NY, USA, 1998. Association for Computing Machinery. ISBN 0897919793. doi: 10.1145/268946.268975. URL <https://doi.org/10.1145/268946.268975>. 1.1
- [19] Richard Statman. Logical relations and the typed λ -calculus. *Information and Control*, 65(2/3):85–97, 1985. doi: 10.1016/S0019-9958(85)80001-2. URL [https://doi.org/10.1016/S0019-9958\(85\)80001-2](https://doi.org/10.1016/S0019-9958(85)80001-2). 1.1
- [20] Eijiro Sumii and Benjamin C. Pierce. Logical relations for encryption. *Journal of Computer Security*, 11(4):521–554, 2003. doi: 10.3233/JCS-2003-11403. URL <https://journals.sagepub.com/doi/abs/10.3233/JCS-2003-11403>. 1.1, 1.2
- [21] William W. Tait. Intensional interpretations of functionals of finite type I. *The Journal of Symbolic Logic*, 32(2):198–212, 1967. ISSN 00224812. URL <http://www.jstor.org/stable/2271658>. 1.1
- [22] Dennis Volpano, Cynthia Irvine, and Geoffrey Smith. A sound type system for secure flow analysis. *J. Comput. Secur.*, 4(2–3):167–187, January 1996. ISSN 0926-227X. 1.1

- [23] Steve Zdancewic. *Programming Languages for Information Security*. PhD thesis, Cornell University, USA, 2002. 1.2
- [24] Yu Zhang. Cryptographic logical relations. *Theoretical Computer Science*, 394(1):39–63, 2008. ISSN 0304-3975. doi: <https://doi.org/10.1016/j.tcs.2007.09.033>. URL <https://www.sciencedirect.com/science/article/pii/S0304397507006809>. 1.2