AALBORG UNIVERSITY
Institute for Computer Science

Title:

Bisimilarity in the Spi-Calculus

Project period:

1/2-2001 - 8/6-2001

Project group E1-119b:

Ulrik Frendrup

Jesper Nyholm Jensen

Supervisor:

Hans Hüttel

Impression: 6

Number of pages: 64

Synopsis:

The Spi-calculus is a process calculus intended for the description and verification of security protocols. Abadi and Gordon have described how common notions of correctness can be described by means of behavioural equivalence for the Spi-calculus. They suggest using testing equivalence as the notion of behavioural equivalence. However, proving testing equivalence is hard, wherefore some alternative notions of equivalence have been proposed.
Abadi and Gordon introduced the notion of framed bisimilarity and Boreale et al. introduced the notion of environment sensitive bisimilarity. Both equivalences are already known to be sound approximations of may-testing equivalence.
In this report we show that framed bisimilarity and a strong late version of environment sensitive bisimilarity are in fact one and the same relation. We have also formulated an early version of framed bisimilarity, called frameless framed bisimilarity, and shown that this is the same as a strong early environment sensitive bisimilarity.
Finally, we propose some modal logics for the Spi-calculus and show that strong early and strong late environment sensitive bisimilarity can be characterized by these logics.

Danish Summary

Denne rapport er dokumentation for projektgruppe E1-119b's speciale på Dat6-semesteret foråret 2001 på instituttet for datalogi, Aalborg universitet.

Projektets tema er semantik. Projektet omhandler forskellige bisimilariteter for Spi-kalkylen. Vi har bevist, at der er interessante sammenhænge mellem disse bisimilariteter, og endvidere har vi foreslået nogle modallogikker for Spi-kalkylen.

Spi-kalkylen er en proceskalkyle udviklet af Abadi og Gordon[3] med henblik på beskrivelse og verifikation af sikkerhedsprotokoller. Abadi og Gordon har beskrevet hvordan sikkerhedsegenskaber for sikkerhedsprotokoller kan udtrykkes ved hjælp af testingækvivalens. Desværre er testingækvivalens svært at bevise, hvorfor der er foreslået to bisimuleringsækvivalenser for Spi-kalkylen, som er lettere at bevise.

Den første af de foreslåede bisimuleringsækvivalenser kaldes framed bisimilaritet og blev introduceret af Abadi og Gordon i [2]. En framed bisimulering relaterer processer i forhold til et frame-theory par. Et frame-theory par indeholder information om hvilke navne processernes omgivelser kender og hvilke beskeder sendt af processerne processernes omgivelser ikke kan skelne mellem. Den sidste af de foreslåede bisimuleringsækvivalenser kaldes environment sensitive bisimilaritet og blev introduceret af Boreale et al. i [6]. En environment sensitive bisimulering relaterer konfigurationer bestående af en proces og dens omgivelser. Det er tidligere bevist, at både framed bisimilaritet og environment sensitive bisimilaritet er sunde tilnærmelser af testingækvivalens.

Vi har defineret en stærk sen udgave af environment sensitive bisimulering og vist, at stærk sen environment sensitive bisimilaritet kan bruges til at karakterisere framed bisimilaritet. Der gælder, at to processer er framed bisimilære i forhold til et frame-theory par hvis og kun hvis disse processer indgår i to stærk sen environment sensitive bisimilære konfigurationer hvis omgivelser kan konverteres til det pågældende frame-theory par. Beviset for dette anvender blandt andet en alternativ karakterisering af framed bisimilaritet kaldet fenced bisimilaritet. Desuden har vi defineret frameless framed bisimulering, som er en tidlig udgave af framed bisimulering. Vi har bevist, at en stærk tidlig environment sensitive bisimilaritet kan karakteriseres ved hjælp af frameless framed bisimilaritet. Endelig har vi defineret nogle modallogikker for konfigurationer og vist, at stærk tidlig og stærk sen environment sensitive bisimilaritet kan karakteriseres ved hjælp af disse.

Preface

This report is the Master Thesis of project group E1-119b on the Dat6 semester at the Institute for Computer Science, Aalborg University.

The theme of the project is semantics. The project deals with different notions of bisimilarity for the Spi-calculus. Interesting connections between these bisimilarities have been proven, and some modal logics for the Spi-calculus have been proposed.

Source material will be referenced by a source number in square brackets, [*source number*], and the title and author of the source will be listed in the bibliography. Definitions, theorems, lemmas, corollaries, and examples, respectively, are numbered consecutively throughout the report. Figures and tables, respectively, are numbered consecutively throughout each chapter. For example, the first figure of chapter 3 will be referenced as figure 3.1. A list of symbols used throughout the report can be seen on page vii.

Aalborg June 7, 2001.

Ulrik Frendrup

Jesper Nyholm Jensen

Glossary

Below are listed the notations used for sets, functions, predicates, and relations throughout this report. They will be presented in order of appearance.

Sets			
Set	**Ranged over by**	**Description**	**Section**
$\mathcal{N}$	a, b, c, d, k, m, n	Names.	2.1
$\mathcal{V}$	u, v	Variables.	2.1
$\mathcal{L}$	K, L	Expressions.	2.1
$\mathcal{G}$	G	Guards.	2.1
$\mathcal{A}g$	A	Agents.	2.1
$\mathcal{M}$	M, N	Messages.	2.1
$\mathcal{P}r$	P, Q, R	Processes.	2.1
$\mathcal{A}ct$	α	Process actions.	2.2
$\mathcal{F}r$	fr	Frames.	3.1
$\mathcal{T}h$	th	Theories.	3.1
Σ	σ	Environments.	4.1
$\mathcal{Z}$	x, y, z	Environment variables.	4.1
Υ	ζ	Environment messages.	4.1
Γ	C	Configurations.	4.2
$\mathcal{A}ct_e$	δ	Environment actions.	4.2
Ω	η	Formula messages.	7.1
Φ	ϕ	Logic consisting of formulae without free variables.	7.1
Φ_0	ϕ	Base logic.	7.2
$\mathcal{F}, \mathcal{EM}$	ϕ	Extensions of the base logic. Used to characterize a strong early environment sensitive bisimilarity.	7.2
$\mathcal{LM}$	ϕ	Logic used to characterize strong late environment sensitive bisimilarity.	7.3.2

Functions			
Function	**Type**	**Description**	**Section**
e	$\mathcal{L} \to \mathcal{M} \cup \{\partial\}$	Function for evaluating expressions to messages. ∂ is a special symbol used to express that an expression cannot be evaluated to a message.	2.2
e'	$\mathcal{G} \to \{tt, ff\}$	Function for evaluating guards.	2.2
π_1, π_2	$\mathcal{T}h \to \mathcal{P}(\mathcal{M})$	Projection functions for theories.	3.2
ξ	$\mathcal{F}r \times \mathcal{T}h \times \mathcal{M} \times \mathcal{M} \to \mathcal{F}r \times \mathcal{T}h \cup \{\bot\}$	Function for computing the smallest extension, with respect to a pair of messages, of a frame-theory pair. $\bot$ is an invalid frame-theory pair returned when there does not exist such an extension.	3.3
$\mathcal{A}$	$\mathcal{P}(\mathcal{M}) \to \mathcal{P}(\mathcal{M})$	The analysis of a set of messages.	4.1
$\mathcal{S}$	$\mathcal{P}(\mathcal{M}) \to \mathcal{P}(\mathcal{M})$	The synthesis of a set of messages.	4.1
$\mathcal{I}$	$\mathcal{P}(\mathcal{M}) \to \mathcal{P}(\mathcal{M})$	The irreducibles of a set of messages.	4.1
$\mathcal{K}$	$\mathcal{P}(\mathcal{M}) \to \mathcal{P}(\mathcal{M})$	The knowledge of a set of messages.	4.1
core	$\mathcal{P}(\mathcal{M}) \times \mathcal{M} \to \mathcal{M}$	The core of a message with respect to a set of messages.	4.1
$\mathcal{F}_e$	$\Sigma \times \Sigma \to \mathcal{F}r \times \mathcal{T}h$	Function for constructing a frame-theory pair from two equivalent environments.	5.2
$\mathcal{F}_{ESB}$	$\mathcal{P}(\Gamma \times \Gamma) \to \mathcal{P}(\mathcal{F}r \times \mathcal{T}h \times \mathcal{P}r \times \mathcal{P}r)$	Function for constructing a framed bisimulation from a strong late environment sensitive bisimulation.	5.2
$\mathcal{O}_{fr}$	$\mathcal{T}h \to \mathcal{P}(\mathcal{N} \times \mathcal{N})$	Function for extracting the set of pairs of names from a theory.	6.1
$\mathcal{O}_{th}$	$\mathcal{T}h \to \mathcal{T}h$	Function for extracting the subset of a theory that does not contain pairs of names.	6.1
$\mathcal{C}$	$\mathcal{P}(\mathcal{N}) \to \mathcal{P}(\mathcal{N} \times \mathcal{N})$	Copy-pairing function for a set of names.	6.1
Ξ	$\mathcal{T}h \times \mathcal{M} \times \mathcal{M} \to \mathcal{T}h \cup \{\top\}$	Function for computing the smallest extension, with respect to a pair of messages, of a theory. $\top$ is an invalid theory returned when there does not exist such an extension.	6.2

continued on next page.

continued from previous page.

Function	Type	Description	Section
$\mathcal{F}'_e$	$\Sigma \times \Sigma \to \mathcal{T}h$	Function for constructing a theory from two equivalent environments.	6.3
$\mathcal{F}_{EESB}$	$\mathcal{P}(\Gamma \times \Gamma) \to \mathcal{P}(\mathcal{T}h \times \mathcal{P}r \times \mathcal{P}r)$	Function for constructing a frameless framed bisimulation from a strong early environment sensitive bisimulation.	6.3
T	$\Sigma \times \Upsilon \to \Upsilon$	Function for substituting names of an environment message to environment variables.	7.1
Δ	$\Gamma \to \mathcal{P}(\Phi)$	Function for finding the set of formulae from Δ that a certain configuration satisfies.	7.2
Δ^S	$\Gamma \to \mathcal{P}(\mathcal{LM})$	Function for finding the set of formulae from Δ that a certain configuration S-satisfies.	7.3.2

Predicates

Predicate	Description	Section
$\leftrightarrow$	The frame-theory pair indistinguishability predicate.	3.1
ok	The ok frame-theory predicate.	3.1
$\leftrightsquigarrow$	The theory indistinguishability predicate.	6.1
$\surd$	The ok theory predicate.	6.1

Relations

Relation	Description	Section
$\equiv_\alpha$	α-Convertibility relation.	2.1
$\xrightarrow{\alpha}$	Transition relation.	2.2
$\simeq$	Testing equivalence.	2.3
$\leq$	The frame-theory pair extension preorder relation.	3.1
$\sim_f$	Framed bisimilarity.	3.2
$\sim_\#$	Fenced bisimilarity.	3.3
$\sim_e$	Environment equivalence.	4.1
$\xrightarrow[\delta]{\alpha}$	Strong environment sensitive transition relation.	4.2
$\overset{\alpha}{\Longrightarrow}_\delta$	Weak environment sensitive transition relation.	4.2
$\approx_{EESB}$	Weak early environment sensitive bisimilarity.	4.3
$\sim_{EESB}$	Strong early environment sensitive bisimilarity.	4.3
$\sim'_e$	Environment equivalence.	4.4
$\sim''_e$	Environment equivalence.	5.1
$\sim_{ESB}$	Strong late environment sensitive bisimilarity.	5.1

continued on next page.

continued from previous page.		
Relation	**Description**	**Section**
$\sqsubseteq$	The theory extension preorder relation.	6.1
$\sim_{ff}$	Frameless framed bisimilarity.	6.1
$\sim_{f\#}$	Frameless fenced bisimilarity.	6.2
$\sim''_{EESB}$	Strong early environment sensitive bisimilarity based on the environment equivalence $\sim''_e$.	7.0
$\equiv$	Syntactic identity of formulae.	7.1
$\models$	Satisfaction relation between configurations and formulae.	7.1
$=_{\mathcal{F}}$	Logical process equivalence induced by the logic $\mathcal{F}$.	7.2
$=_{\mathcal{EM}}$	Logical process equivalence induced by the logic $\mathcal{EM}$.	7.2
$\sim^S_{ESB}$	S-Environment sensitive bisimilarity.	7.3.1
$\models_S$	S-Satisfaction relation between configurations and formulae.	7.3.2
$=_{\mathcal{LM}^S}$	Logical process equivalence induced by the logic $\mathcal{LM}$ and the set S.	7.3.2
$=_{\mathcal{LM}}$	Logical process equivalence induced by the logic $\mathcal{LM}$.	7.3.2

Contents

1 Introduction

In recent years cryptography has widely been used in distributed systems to obtain secrecy, authentication, integrity, and to prevent frauds from being carried out by dishonest people. However, the use of cryptography in a distributed system does not necessarily give the system these properties. There exist many cases of people having found flaws in cryptographic protocols years after these were proposed and integrated in systems[15]. Due to this, some researchers have been focusing on using formal methods for analyzing cryptographic protocols. A popular approach is to model protocols as concurrent processes in a process calculus like the π-calculus.

1.1 The π-Calculus

Although the π-calculus appears suited for describing security protocols at an abstract level it suffers from the fact that it does not include any constructs for encryption and decrypting needed when describing actual implementations of security protocols. Consider an example where a process P_1 wants to send some secret datum d to another process P_2. In the π-calculus this can be achieved by creating a new channel c which is used for the transmission of d as illustrated in the following π-process.

$$PROTOCOL \stackrel{def}{=} (\nu\ c)(\bar{c}d.P_1 \mid c(z).P_2)$$

The transmission of d on c is secure since c is not known by anyone but P_1 and P_2. In an implementation of $PROTOCOL$ the processes P_1 and P_2 could be placed on different machines. In this case the communication between the processes is not necessarily secure if it uses a public channel and the transmission of d on c should be implemented in a way that guarantees the secrecy of d. The definition of $PROTOCOL$ in the π-calculus does not say anything about how this is done.

1.2 The Spi-Calculus

The Spi-calculus was first presented by Abadi and Gordon in [3] and was designed for describing and analyzing security protocols. The Spi-calculus is an extension of the π-calculus

with cryptographic primitives. With these it is possible to represent the use of cryptography in security protocols in a way that is more suited for describing actual implementations. In [3], Abadi and Gordon describe how common notions of correctness of security protocols can be described by means of behavioural equivalence for the Spi-calculus. For instance, consider a protocol $S(M)$ transmitting the message M. S has the property of secrecy if its observable behaviour does not depend on M, i.e. if $S(M_1) \sim S(M_2)$ for any messages M_1 and M_2. Abadi and Gordon suggest using the notion of may-testing equivalence due to De Nicola and Hennessy as the notion of behavioural equivalence for the Spi-calculus. Two processes are testing equivalent if they allow the same end observations in all observation contexts. As observers in the Spi-calculus setting are potentially malicious, two processes are thus equivalent if they respond identically to identical attacks. However, while the notion of testing equivalence is perfect from a philosophical point of view it is less ideal for actual reasoning about protocols as its definition involves universal quantification over all attackers. This has been dealt with in two different ways.

1.3 Bisimilarities in the Spi-Calculus

In [2], Abadi and Gordon introduce the notion of framed bisimilarity based on the concept of a frame-theory pair. A frame-theory pair is a pair (fr, th), where fr is the set of names known by the observer and th is a finite set of identities on messages that the observer assumes. If $(M, N) \in th$ the observer cannot distinguish between messages M and N. Equivalence judgements of framed bisimilarity are relative to a frame-theory pair, i.e. $(fr, th) \vdash P \sim_f Q$ if P and Q are equivalent under the assumptions in (fr, th). Abadi and Gordon have shown that $\sim_f$ is a sound approximation of may-testing equivalence in the sense that it implies may-testing equivalence under natural conditions on the frame-theory pair involved. In [6], Boreale et al. let the knowledge of the observer become part of the semantics of processes. Their notion of environment sensitive bisimilarity compares configurations of the form $\sigma \rhd P$, where σ records the messages and names that are known to the environment. Equivalence judgments are thus of the form $\sigma_1 \rhd P \approx_{EESB} \sigma_2 \rhd Q$. Boreale et al. have shown that $\approx_{EESB}$, too, is a sound approximation of may-testing equivalence.It has been proven that there exist environment sensitive bisimilar configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ for which there does not exist a frame-theory pair such that P and Q are framed bisimilar with respect to this pair.

1.4 New Results

In this report, we present a new strong late version of the environment sensitive bisimilarity given by Boreale at al. and prove that this can be used as an alternative characterization of framed bisimilarity. The characterization states that two configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ are strong late environment sensitive bisimilar if and only if P and Q are framed bisimilar with respect to $\mathcal{F}_e(\sigma_P, \sigma_Q)$, where $\mathcal{F}_e$ is a function that given two equivalent environments returns a frame-theory pair.

Furthermore, we present a new early version of framed bisimilarity called frameless framed bisimilarity. This bisimilarity can be used to characterize a strong version of the early environment sensitive bisimilarity given by Boreale at al. This is easily proven using an adaptation of the proof technique used to prove that the strong late version of the environment sensitive bisimilarity is the same as framed bisimilarity.

Finally, we propose some modal logics for the Spi-calculus. We prove that these can be used to characterize the strong early version and our new strong late version of the environment sensitive bisimilarity given by Boreale at al. The definition of our new strong late version of environment sensitive bisimulation makes it difficult to give a logical characterization of strong late environment sensitive bisimilarity directly. Therefore, we introduce a new notion of environment sensitive bisimulation called S-environment sensitive bisimulation, show that there is a useful connection between S-environment sensitive bisimilarity and strong late environment sensitive bisimilarity, and give a logical characterization of S-environment sensitive bisimilarity.

1.5 Outline of the Report

This report contains eight chapters and is organized as follows. Chapter 2 contains the syntax and semantics of the variant of the Spi-calculus we will be working with. Furthermore, we present the notion of testing equivalence defined by Abadi and Gordon in [3]. In chapter 3 we present the notion of framed bisimulation introduced by Abadi and Gordon in [2]. We also present an alternative characterization of framed bisimilarity, called fenced bisimilarity, given by Elkjær et al. in [7]. In chapter 4 the notion of environment sensitive bisimulation, defined by Boreale et al. in [6], is given. In chapter 5 we present a new strong late version of the environment sensitive bisimulation given by Boreale at al. and prove that strong late environment sensitive bisimilarity is in fact an alternative characterization of framed bisimilarity. In chapter 6 we present an early version of framed bisimulation called frameless framed bisimulation. Moreover, we present results stating that frameless framed bisimilarity is an alternative characterization of a strong version of the environment sensitive bisimilarity defined by Boreale et al. In chapter 7 we propose some modal logics for the Spi-calculus and prove that we can use these to give logical characterizations of environment sensitive bisimilarities. Finally, chapter 8 concludes on our work.

2 The Spi-Calculus

This chapter contains preliminaries on the variant of the Spi-calculus we will be working with. The variant is inspired by [6] and [10]. We will first describe the syntax and semantics and then give a definition of testing equivalence for Spi-processes.

2.1 Syntax

We begin by giving the syntax for the variant of the Spi-calculus we will be working with. The syntactic categories are: an infinite set of ***names***, $\mathcal{N}$, an infinite set of ***variables***, $\mathcal{V}$, a set of ***expressions*** $\mathcal{L}$, a set of ***guards***, $\mathcal{G}$, and a set of ***agents***, $\mathcal{A}g$. We let a, b, c, d, k, m, and n range over $\mathcal{N}$, u and v over $\mathcal{V}$, K and L over $\mathcal{L}$, G over $\mathcal{G}$, and A over $\mathcal{A}g$. The set of expressions consists of the names, the variables, and elements that can be constructed from these using the ***encryption***, ***decryption***, ***pair***, ***left projection***, and ***right projection*** constructors. The set of guards can be constructed using the ***true***, ***conjunction***, ***comparison***, and ***is a name*** constructors. The set of agents in the Spi-calculus can be constructed with the constructors for ***inaction***, ***input prefix***, ***output prefix***, ***guarding***, ***nondeterministic choice***, ***parallel composition***, ***restriction***, and ***replication***. The grammars for $\mathcal{L}$, $\mathcal{G}$, and $\mathcal{A}g$ are presented below.

$$\begin{aligned} K, L ::= &\ a \mid u \mid \{L\}^E_L \mid \{L\}^D_L \mid (L, L) \mid \pi_l(L) \mid \pi_r(L) \\ G ::= &\ tt \mid G \wedge G \mid L = L \mid L : \mathcal{N} \\ A ::= &\ \mathbf{0} \mid L(u).A \mid \overline{L}L.A \mid GA \mid A + A \mid A|A \mid (\nu\ a)A \mid\ !A \end{aligned}$$

This variant of the Spi-calculus differs from the Spi-calculus originally presented by Abadi and Gordon in [3] by the fact that numbers are not explicitly expressible and by the fact that decryption and projection appear in expressions instead of in agents.

For a tuple $\tilde{k} \stackrel{def}{=} (k_1, \ldots, k_n) \subseteq \mathcal{N}$ we use the shorthand notations $\{L\}^E_{\tilde{k}}$ and $\{L\}^D_{\tilde{k}}$ for the expressions $\{\cdots\{L\}^E_{k_1}\cdots\}^E_{k_n}$ and $\{\cdots\{L\}^D_{k_n}\cdots\}^D_{k_1}$, respectively. Furthermore, we may use the longhand notations $\{L\}^E_{\emptyset}$ and $\{L\}^D_{\emptyset}$ for the expression L.

We call the subset of expressions of $\mathcal{L}$ that only consist of names, encryption, and pairs

the set of ***messages***, $\mathcal{M}$, and let M and N range over it. So, $\mathcal{M}$ is the set of messages that can be generated from the following grammar.

$$M, N ::= \quad a \mid \{N\}_a^E \mid (N, N)$$

There are two binding structures in our variant of the Spi-calculus. In the agent $(\nu\ a)A$, the name a is bound in A and in the agent $L(u).A$, the variable u is bound in A. The sets of ***free names***, $\mathrm{fn}(A)$, ***bound names***, $\mathrm{bn}(A)$, ***names***, $\mathrm{n}(A)$, ***free variables***, $\mathrm{fv}(A)$, and ***bound variables***, $\mathrm{bv}(A)$, of an agent A are defined as expected. We will write $A\{M/u\}$ for the agent obtained by replacing every free occurrence of u in A by M, renaming bound names as necessary. We identify agents up to renaming of bound names and variables. If the agents A_1 and A_2 can be identified up to renaming of bound names and variables then A_1 and A_2 are α***-convertible***, written $A_1 \equiv_\alpha A_2$. We will call an agent that does not contain any free variables a process and let $\mathcal{P}r$ denote the set of all processes, i.e. $\mathcal{P}r = \{A \in \mathcal{A}g \mid \mathrm{fv}(A) = \emptyset\}$. The set of processes is ranged over by P, Q, and R.

The following example shows how the Spi-calculus can be used to model a cryptographic protocol.

Example 1. In this example we will model a simplified version of the 'Wide Mouthed Frog Protocol'[15]. In this protocol the principals A and B share the keys k_{AS} and k_{BS}, respectively, with a server S. Before A sends some secret message M to B, it first creates a new key k_{AB} and sends it to the server encrypted with the key k_{AS}. The server then decrypts the received message and sends k_{AB} to B encrypted with the key k_{BS}. Now, A can send its secret message M to B encrypted with the key k_{AB}. The protocol can be expressed in the Spi-calculus as follows.

$$\begin{aligned}
A(M) &\stackrel{def}{=} (\nu\ k_{AB})\overline{c_{AS}}\{k_{AB}\}^E_{k_{AS}}.\overline{c_{AB}}\{M\}^E_{k_{AB}}.\mathbf{0} \\
B &\stackrel{def}{=} c_{SB}(u).c_{AB}(v).F(\{v\}^D_{\{u\}^D_{k_{BS}}}) \\
S &\stackrel{def}{=} c_{AS}(u).\overline{c_{SB}}\{\{u\}^D_{k_{AS}}\}^E_{k_{BS}}.\mathbf{0} \\
Sys(N) &\stackrel{def}{=} (\nu\ k_{AS})(\nu\ k_{BS})(A(N) \mid B \mid S)
\end{aligned}$$

where $F(M)$ is an agent representing the behavior of B when it receives the message M.

■

2.2 Semantics

Before we present the semantics of the Spi-calculus we need to define some evaluation functions. We will need a function $e : \mathcal{L} \to \mathcal{M} \cup \{\partial\}$ to evaluate expressions to messages, ∂ is a special symbol used to express that an expression cannot be evaluated to a message. We also need a function $e' : \mathcal{G} \to \{tt, ff\}$ to evaluate guards.

Definition 1 (The Evaluation Function e)
The function $e : \mathcal{L} \to \mathcal{M} \cup \{\partial\}$ is defined as

$$
\begin{aligned}
e(a) &\stackrel{def}{=} a \\
e(u) &\stackrel{def}{=} \partial \\
e(\{L\}^E_K) &\stackrel{def}{=} \begin{cases} \{N\}^E_b & \text{if } e(K) = b \in \mathcal{N} \wedge e(L) = N \neq \partial \\ \partial & \text{otherwise} \end{cases} \\
e(\{L\}^D_K) &\stackrel{def}{=} \begin{cases} N & \text{if } e(K) = b \in \mathcal{N} \wedge e(L) = \{N\}^E_b \\ \partial & \text{otherwise} \end{cases} \\
e((L_1, L_2)) &\stackrel{def}{=} \begin{cases} (M, N) & \text{if } e(L_1) = M \neq \partial \wedge e(L_2) = N \neq \partial \\ \partial & \text{otherwise} \end{cases} \\
e(\pi_l(L)) &\stackrel{def}{=} \begin{cases} M & \text{if } L = (L_1, L_2) \wedge e(L_1) = M \wedge e(L_2) \neq \partial \\ \partial & \text{otherwise} \end{cases} \\
e(\pi_r(L)) &\stackrel{def}{=} \begin{cases} M & \text{if } L = (L_1, L_2) \wedge e(L_2) = M \wedge e(L_1) \neq \partial \\ \partial & \text{otherwise} \end{cases}
\end{aligned}
$$

■

Definition 2 (The Evaluation Function e')
The function $e' : \mathcal{G} \to \{tt, ff\}$ is defined as

$$
\begin{aligned}
e'(tt) &\stackrel{def}{=} tt \\
e'(G_1 \wedge G_2) &\stackrel{def}{=} e'(G_1) \wedge e'(G_2) \\
e'(L_1 = L_2) &\stackrel{def}{=} \begin{cases} tt & \text{if } e(L_1) = e(L_2) \neq \partial \\ ff & \text{otherwise} \end{cases} \\
e'(L : \mathcal{N}) &\stackrel{def}{=} \begin{cases} tt & \text{if } e(L) \in \mathcal{N} \\ ff & \text{otherwise} \end{cases}
\end{aligned}
$$

■

The (late) operational semantics for the variant of the Spi-calculus is given by the labelled transition system $(\mathcal{A}g, \mathcal{A}ct, \longrightarrow)$, where $\longrightarrow$ is the smallest relation closed under the rules in table 2.1. The symmetric rules for Sum, Par, and Com have been omitted. $\mathcal{A}ct$, ranged over by α, is the set of actions given by the following grammar.

$$\alpha ::= \tau \mid a(u) \mid (\nu\ \tilde{c})\bar{a}N$$

Transitions have the form $A \stackrel{\alpha}{\longrightarrow} A'$.

[Alpha]	$\dfrac{A' \xrightarrow{\alpha} A''}{A \xrightarrow{\alpha} A''}$	$A \equiv_\alpha A'$
[Inp]	$\dfrac{}{L(u).A \xrightarrow{a(u)} A}$	$e(L) = a$
[Outp]	$\dfrac{}{\overline{L}_1 L_2.A \xrightarrow{\bar{a}N} A}$	$e(L_1) = a$ and $e(L_2) = N \neq \partial$
[Grd]	$\dfrac{A \xrightarrow{\alpha} A'}{GA \xrightarrow{\alpha} A'}$	$e'(G) = tt$
[Sum]	$\dfrac{A_1 \xrightarrow{\alpha} A_1'}{A_1 + A_2 \xrightarrow{\alpha} A_1'}$	
[Par]	$\dfrac{A_1 \xrightarrow{\alpha} A_1'}{A_1 \mid A_2 \xrightarrow{\alpha} A_1' \mid A_2}$	$\mathrm{bn}(\alpha) \cap \mathrm{fn}(A_2) = \emptyset$
[Com]	$\dfrac{A_1 \xrightarrow{(\nu\ \tilde{c})\bar{a}N} A_1' \quad A_2 \xrightarrow{a(u)} A_2'}{A_1 \mid A_2 \xrightarrow{\tau} (\nu\ \tilde{c})(A_1' \mid A_2'\{N/u\})}$	$\tilde{c} \cap \mathrm{fn}(A_2) = \emptyset$
[Res]	$\dfrac{A \xrightarrow{\alpha} A'}{(\nu\ b)A \xrightarrow{\alpha} (\nu\ b)A'}$	$b \notin \mathrm{n}(\alpha)$
[Open]	$\dfrac{A \xrightarrow{(\nu\ \tilde{c})\bar{a}N} A'}{(\nu\ b)A \xrightarrow{(\nu\ \{b\}\cup\tilde{c})\bar{a}N} A'}$	$b \in (\mathrm{n}(N) \setminus \tilde{c})$ and $b \neq a$
[Rep]	$\dfrac{A \mid !A \xrightarrow{\alpha} A'}{!A \xrightarrow{\alpha} A'}$	

Table 2.1: Late operational semantics for the Spi-calculus.

2.3 Testing Equivalence

In the paper [3], Abadi and Gordon suggest using the notion of may-testing equivalence[9] due to De Nicola and Hennessy as the notion of behavioural equivalence for the Spi-calculus.

In this section we present this equivalence.

First we need to define some notations. A barb is a name, a, or a co-name $\bar{a}$. For a name a and a process P we write $P \downarrow a$ if $P \xrightarrow{a(u)} P'$ for some u and P' and $P \downarrow \bar{a}$ if $P \xrightarrow{(\nu\ \tilde{c})\bar{a}N} P'$ for some $\tilde{c}$, N, and P'.

Definition 3 (Testing Equivalence)
Two processes P and Q are testing equivalent, written $P \simeq Q$, if for every process R and barb β it holds that

(i) if $P|R \xrightarrow{\tau}{}^* P'$ and $P' \downarrow \beta$ for some P' then there exists Q' such that $Q|R \xrightarrow{\tau}{}^* Q'$ and $Q' \downarrow \beta$, and

(ii) the converse, with the role of P and Q exchanged.

■

If two processes are testing equivalent we can interpret this as though they are revealing the same information to the "environment", i.e. observers, attackers etc. As an example of a pair of testing equivalent processes consider the following two processes $P \stackrel{def}{=} (\nu\ k)\bar{a}\{m\}^E_k.\mathbf{0}$ and $Q \stackrel{def}{=} (\nu\ k)\bar{a}\{m'\}^E_k.\mathbf{0}$. The processes reveal the messages $\{m\}^E_k$ and $\{m'\}^E_k$, respectively, but none of these can ever be decrypted since the processes never reveal the key k.

In [3] Abadi and Gordon describe how common notions of correctness can be described by means of testing equivalence. For instance, consider a protocol $S(M)$ transmitting the message M. S has the property of secrecy if its observable behaviour does not depend on M, i.e. if $S(M_1) \simeq S(M_2)$ for any messages M_1 and M_2. The following example illustrates how testing equivalence can be used to check for authenticity and/or integrity.

Example 2. In this example we will show how to check for authenticity and/or integrity in the protocol presented in example 1. This can be done by using testing equivalence to compare the actual protocol with a specification. The specification is obtained by replacing B with $B_{Spec}(M)$ which behaves as B when it receives the message M. The specification is defined as follows.

$$\begin{aligned} A(M) &\stackrel{def}{=} (\nu\ k_{AB})\overline{c_{AS}}\{k_{AB}\}^E_{k_{AS}}.\overline{c_{AB}}\{M\}^E_{k_{AB}}.\mathbf{0} \\ B_{Spec}(M) &\stackrel{def}{=} c_{SB}(u).c_{AB}(v).F(M) \\ S &\stackrel{def}{=} c_{AS}(u).\overline{c_{SB}}\{\{u\}^D_{k_{AS}}\}^E_{k_{BS}}.\mathbf{0} \\ Sys_{Spec}(N) &\stackrel{def}{=} (\nu\ k_{AS})(\nu\ k_{BS})(A(N) \mid B_{Spec}(N) \mid S) \end{aligned}$$

Sys has the property of authenticity (integrity) if $Sys(M) \simeq Sys_{Spec}(M)$ for all messages M. ■

While the notion of testing equivalence is perfect from a philosophical point of view it is less ideal for actual reasoning about protocols as its definition involves universal quantification over all processes/attackers. To get rid of this universal quantification Abadi and Gordon introduced the notion of framed bisimilarity in [2] and showed that this is sound with respect to testing equivalence. Boreale et. al proposed another notion of bisimilarity called environment sensitive bisimilarity in [6] and showed that it, too, is sound with respect to testing equivalence. These two notions of bisimilarity are presented in the following two chapters.

3 Framed Bisimulation

In this chapter we present framed bisimulation as defined in [2] by Abadi and Gordon and fenced bisimulation as defined in [7] by Elkjær et al. First we present some preliminaries needed for the definition of framed and fenced bisimulation.

3.1 Frames and Theories

The definition of framed bisimulation is based on the notions of ***frame*** and ***theory***. A framed bisimulation relates two processes P and Q in the context of a frame and a theory. A frame is a finite set of names and a theory is a finite set of pairs of messages. Intuitively, a frame contains the names from P and Q that are available to the environment, and a theory contains pairs of messages coming from P and Q that cannot be distinguished by an observer. We will use fr to range over the set of frames, $\mathcal{F}r$, and th to range over the set of theories, $\mathcal{T}h$. Two messages M and N are indistinguishable with respect to the frame-theory pair (fr, th) if $(fr, th) \vdash M \leftrightarrow N$ can be derived using the rules in table 3.1. Some of the rules in the semantics of the $(fr, th) \vdash M \leftrightarrow N$ predicate presented in [2] have been omitted in our presentation since our grammar for messages does not allow a message to be a number. The results from [2] and [7] presented in this chapter were proven for a message grammar containing numbers. However, it can easily be shown that they also hold for our message grammar.

[Eq frame]	$\dfrac{n \in fr}{(fr, th) \vdash n \leftrightarrow n}$
[Eq theory]	$\dfrac{(M, N) \in th}{(fr, th) \vdash M \leftrightarrow N}$
[Eq pair]	$\dfrac{(fr, th) \vdash M \leftrightarrow N \quad (fr, th) \vdash M' \leftrightarrow N'}{(fr, th) \vdash (M, M') \leftrightarrow (N, N')}$
[Eq encrypt]	$\dfrac{(fr, th) \vdash M \leftrightarrow N \quad (fr, th) \vdash M' \leftrightarrow N'}{(fr, th) \vdash \{M\}^E_{M'} \leftrightarrow \{N\}^E_{N'}}$

Table 3.1: The indistinguishability predicate.

In a framed bisimulation we only consider frame-theory pairs that exhibit certain properties.

Definition 4 (Ok Frame-Theory Pair)
The pair (fr, th) is ok, written $(fr, th) \vdash ok$, if

(i) for all $(M, N) \in th$:

- $M \in \mathcal{M}$ and there are messages M_1 and M_2 such that $M = \{M_1\}^E_{M_2}$ and there is no N' such that $(fr, th) \vdash M_2 \leftrightarrow N'$.
- $N \in \mathcal{M}$ and there are messages N_1 and N_2 such that $N = \{N_1\}^E_{N_2}$ and there is no M' such that $(fr, th) \vdash M' \leftrightarrow N_2$.

(ii) for all $(M, N) \in th$ and $(M', N') \in th$, $M = M'$ if and only if $N = N'$.

■

The definition of framed bisimulation requires that a frame-theory pair can be extended.

Definition 5 (Extension of a Frame-Theory Pair)
(fr', th') is an extension of (fr, th), written $(fr, th) \leq (fr', th')$, if for all M and N, $(fr, th) \vdash M \leftrightarrow N$ implies $(fr', th') \vdash M \leftrightarrow N$. ■

The following theorem, proven in [2], makes it easier to show whether or not one ok frame-theory pair is an extension of another.

Theorem 1
Let $(fr', th') \vdash ok$, then $(fr, th) \leq (fr', th')$ if and only if $fr \subseteq fr'$ and $(fr', th') \vdash M \leftrightarrow N$ for each pair $(M, N) \in th$. ■

3.2 Framed Bisimulation

A ***framed process pair*** is a quadruple (fr, th, P, Q). If R is a set of framed process pairs and $(fr, th, P, Q) \in R$ this is written $(fr, th) \vdash P\ R\ Q$. A ***framed relation*** is a set of framed process pairs such that $(fr, th) \vdash P\ R\ Q$ implies $(fr, th) \vdash ok$. A framed relation R is ***symmetric*** if $(fr, th) \vdash P\ R\ Q$ implies $(fr, \{(N, M) \mid (M, N) \in th\}) \vdash Q\ R\ P$. For a theory th we let $\pi_1(th) \stackrel{def}{=} \{M \mid \exists N.(M, N) \in th\}$ and $\pi_2(th) \stackrel{def}{=} \{N \mid \exists M.(M, N) \in th\}$. Now, we are ready to present the notion of ***framed bisimulation***.

Definition 6 (Framed Bisimulation)
A symmetric framed relation R is a framed bisimulation if whenever $(fr, th) \vdash P\ R\ Q$ it holds that

(i) if $P \xrightarrow{\tau} P'$ then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(fr, th) \vdash P'\ R\ Q'$,

(ii) if $P \xrightarrow{a(u)} P'$ and $a \in fr$ then there exists Q' such that $Q \xrightarrow{a(u)} Q'$ and for all sets $\tilde{n}$, where $\tilde{n} \cap (\mathrm{fn}(P, Q) \cup fr \cup \mathrm{n}(th)) = \emptyset$, and all $M, N \in \mathcal{M}$, where $(fr \cup \tilde{n}, th) \vdash M \leftrightarrow N$, it holds that $(fr \cup \tilde{n}, th) \vdash P'\{M/u\}\ R\ Q'\{N/u\}$, and

(iii) if $P \xrightarrow{(\nu\ \tilde{m})\bar{a}M} P'$, $a \in fr$ and $\tilde{m} \cap (\mathrm{fn}(P) \cup fr \cup \mathrm{n}(\pi_1(th))) = \emptyset$ then there exist $\tilde{n}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{n})\bar{a}N} Q'$, $\tilde{n} \cap (\mathrm{fn}(Q) \cup fr \cup \mathrm{n}(\pi_2(th))) = \emptyset$, and there exists (fr', th') such that $(fr, th) \leq (fr', th')$, $(fr', th') \vdash M \leftrightarrow N$, and $(fr', th') \vdash P'\ R\ Q'$.

■

From the definition of framed bisimulation we define the notion of ***framed bisimilarity***.

Definition 7 (Framed Bisimilarity)
P and Q are framed bisimilar with respect to the frame-theory pair (fr, th), written $(fr, th) \vdash P \sim_f Q$, if there exists a framed bisimulation R such that $(fr, th) \vdash P\ R\ Q$. ■

In [2], Abadi and Gordon have shown that $\sim_f$ is a sound approximation of testing equivalence in the sense that it implies testing equivalence under natural conditions on the frame-theory pair involved.

Theorem 2 (Soundness of Framed Bisimilarity with respect to Testing Equivalence)
Let $P, Q \in \mathcal{P}r$ and $n \in \mathcal{N}$ such that $n \notin \mathrm{fn}(P, Q)$. If $(\mathrm{fn}(P, Q) \cup \{n\}, \emptyset) \vdash P \sim_f Q$ then $P \simeq Q$. ■

3.3 Fenced Bisimulation

To avoid the existential quantification over frame-theory pairs in case *(iii)* of definition 6 Elkjær et al. presented an alternative characterization of framed bisimilarity called fenced bisimilarity. Fenced bisimulation makes use of the function ξ shown in figure 3.1.

```
1  ξ((fr, th), M, N)
2    IF ((fr, th) ⊢ M ↔ N) THEN RETURN (fr, th)
3    CASE (M, N) OF
4    [M = N = n] :
5         (fr_ξ, th_ξ) := (fr ∪ {n}, th)
6         λ := ∅
7         FOR EACH ({M_1}^E_{M_2}, {N_1}^E_{N_2}) ∈ th_ξ DO
8           IF ∃L.((fr_ξ, th_ξ) ⊢ M_2 ↔ L ∨ (fr_ξ, th_ξ) ⊢ L ↔ N_2) THEN
9              th_ξ := th_ξ \ {({M_1}^E_{M_2}, {N_1}^E_{N_2})}
10             λ := λ ∪ {({M_1}^E_{M_2}, {N_1}^E_{N_2})}
11          FOR EACH ({M_1}^E_{M_2}, {N_1}^E_{N_2}) ∈ λ DO
12             (fr_ξ, th_ξ) := ξ(ξ((fr_ξ, th_ξ), M_2, N_2), M_1, N_1)
13   [M = {M_1}^E_{M_2}, N = {N_1}^E_{N_2}] :
14        IF ((fr, th) ⊢ M_2 ↔ N_2) THEN (fr_ξ, th_ξ) := ξ((fr, th), M_1, N_1)
15        ELSE
16          IF ∃(O, O') ∈ th.(O = M ⇎ O' = N) THEN RETURN(⊥)
17          (fr_ξ, th_ξ) := (fr, th ∪ {(M, N)})
18          λ := ∅
19          FOR EACH ({O_1}^E_{O_2}, {O'_1}^E_{O'_2}) ∈ th_ξ DO
20            IF ∃L.((fr_ξ, th_ξ) ⊢ O_2 ↔ L ∨ (fr_ξ, th_ξ) ⊢ L ↔ O'_2) THEN
21               th_ξ := th_ξ \ {({O_1}^E_{O_2}, {O'_1}^E_{O'_2})}
22               λ := λ ∪ {({O_1}^E_{O_2}, {O'_1}^E_{O'_2})}
23          FOR EACH ({O_1}^E_{O_2}, {O'_1}^E_{O'_2}) ∈ λ DO
24             (fr_ξ, th_ξ) := ξ(ξ((fr_ξ, th_ξ), O_2, O'_2), O_1, O'_1)
25   [M = (M_1, M_2), N = (N_1, N_2)] :
26        (fr_ξ, th_ξ) := ξ(ξ((fr, th), M_2, N_2), M_1, N_1)
27   [otherwise] :
28         RETURN (⊥)
29   RETURN (fr_ξ, th_ξ)
```

Figure 3.1: Algorithm for computing $\xi((fr, th), M, N)$.

The case for numbers in the ξ-function presented in [7] has been omitted in our presentation since our grammar for messages does not allow a message to be a number. $\xi((fr, th), M, N)$

evaluates to the smallest extension (fr', th') of (fr, th) such that $(fr', th') \vdash ok$ and $(fr', th') \vdash M \leftrightarrow N$[7]. If this is not possible $\xi((fr, th), M, N)$ evaluates to the invalid frame-theory pair $\perp$. The notion of ***fenced bisimulation*** is defined as follows.

Definition 8 (Fenced Bisimulation)
A symmetric framed relation, R, is a fenced bisimulation if whenever $(fr, th) \vdash P\ R\ Q$ it holds that

(i) if $P \xrightarrow{\tau} P'$ then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $(fr, th) \vdash P'\ R\ Q'$,

(ii) if $P \xrightarrow{a(u)} P'$ and $a \in fr$ then there exists Q' such that $Q \xrightarrow{a(u)} Q'$ and for all sets $\tilde{n}$, where $\tilde{n} \cap (\mathrm{fn}(P, Q) \cup fr \cup \mathrm{n}(th)) = \emptyset$, and all $M, N \in \mathcal{M}$, where $(fr \cup \tilde{n}, th) \vdash M \leftrightarrow N$, it holds that $(fr \cup \tilde{n}, th) \vdash P'\{M/u\}\ R\ Q'\{N/u\}$, and

(iii) if $P \xrightarrow{(\nu\ \tilde{m})\bar{a}M} P'$, $a \in fr$ and $\tilde{m} \cap (\mathrm{fn}(P) \cup fr \cup \mathrm{n}(\pi_1(th))) = \emptyset$ then there exist $\tilde{n}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{n})\bar{a}N} Q'$, $\tilde{n} \cap (\mathrm{fn}(Q) \cup fr \cup \mathrm{n}(\pi_2(th))) = \emptyset$, and $\xi((fr, th), M, N) \vdash P'\ R\ Q'$.

■

From the definition of fenced bisimulation we define the notion of ***fenced bisimilarity***.

Definition 9 (Fenced Bisimilarity)
P and Q are fenced bisimilar with respect to the frame-theory pair (fr, th), written $(fr, th) \vdash P \sim_{\#} Q$, if there exists a fenced bisimulation R such that $(fr, th) \vdash P\ R\ Q$. ■

The following theorem, proven by Elkjær et al. in [7], states that two processes are framed bisimilar with respect to a frame-theory pair if and only if they are fenced bisimilar with respect to the same frame-theory pair.

Theorem 3 (Coincidence of $\sim_f$ and $\sim_{\#}$)
$(fr, th) \vdash P \sim_f Q$ if and only if $(fr, th) \vdash P \sim_{\#} Q$. ■

In the following chapter we proceed by presenting the notion of environment sensitive bisimilarity, where Boreale et al. let the knowledge of the observer become part of the semantics of processes.

4 Environment Sensitive Bisimulation

In this chapter we present the notion of environment sensitive bisimulation first introduced by Boreale et al. in [6]. As framed bisimulation environment sensitive bisimulation does not relate processes directly, instead it relates configurations of the form $\sigma \rhd P$, where σ is an environment used to record the messages sent to and received from the process P. In this chapter we will consider an expression and message grammar without pairs and projection. We will continue to refer to the set of expressions and the set of messages as $\mathcal{L}$ and $\mathcal{M}$, respectively.

4.1 Environments

The set of environments Σ consists of functions/substitutions of the type $\mathcal{Z} \to \mathcal{M}$, where $\mathcal{Z}$ is a set of environment variables for which it holds that $\mathcal{Z} \cap \mathcal{V} = \emptyset$. We let σ range over Σ and x, y, and z over $\mathcal{Z}$. We write $\{M_1/x_1, M_2/x_2, \ldots, M_n/x_n\}$ for the environment that simultaneously maps every occurrence of x_i to M_i for all $i \in \{1, 2, \ldots, n\}$. Furthermore, we write $\sigma[x \mapsto M]$ for the environment that maps x to M and all other environment variables to the same as the environment σ. The messages that an environment σ can send to a process are of the form $e(\zeta\sigma)$, where ζ is an ***environment message***. The set of environment messages, Υ, is given by the following grammar.

$$\zeta ::= \ a \mid x \mid \{\zeta\}^E_\zeta \mid \{\zeta\}^D_\zeta$$

The set of environment variables in an environment message ζ is denoted $\mathrm{fz}(\zeta)$. To describe the information that can be deduced from an environment we define some functions first presented in [5], [6], and [14].

The analysis of a set of messages W is the set of messages that can be deduced from W by decryption.

Definition 10 (Analysis of a Set of Messages)
The analysis of a set $W \subseteq \mathcal{M}$, written $\mathcal{A}(W)$, is the smallest set satisfying

(i) $W \subseteq \mathcal{A}(W)$

(ii) if $k \in \mathcal{A}(W)$ and $\{M\}_k^E \in \mathcal{A}(W)$ then $M \in \mathcal{A}(W)$

■

The synthesis of a set of messages W is the set of messages that can be generated from the analysis of W.

Definition 11 (Synthesis of a Set of Messages)
The synthesis of a set $W \subseteq \mathcal{M}$, written $\mathcal{S}(W)$, is the smallest set satisfying

(i) $\mathcal{A}(W) \subseteq \mathcal{S}(W)$

(ii) if $k \in \mathcal{S}(W) \cap \mathcal{N}$ and $M \in \mathcal{S}(W)$ then $\{M\}_k^E \in \mathcal{S}(W)$

■

The irreducibles of a set of messages W is the subset of the analysis of W that cannot be decrypted further.

Definition 12 (Irreducibles of a Set of Messages)
The irreducibles of a set $W \subseteq \mathcal{M}$, written $\mathcal{I}(W)$, is defined by

$$\mathcal{I}(W) \stackrel{def}{=} \{M \in \mathcal{A}(W) \mid M \in \mathcal{N} \vee (M = \{N\}_k^E \wedge k \notin \mathcal{A}(W))\}$$

■

The knowledge of a set of messages W is the set of names of the analysis of W.

Definition 13 (Knowledge of a Set of Messages)
The knowledge of a set $W \subseteq \mathcal{M}$, written $\mathcal{K}(W)$, is defined by $\mathcal{K}(W) \stackrel{def}{=} \mathcal{A}(W) \cap \mathcal{N}$. ■

For an environment σ we will use the shorthand notations $\mathcal{A}(\sigma)$, $\mathcal{S}(\sigma)$, $\mathcal{I}(\sigma)$, and $\mathcal{K}(\sigma)$ for $\mathcal{A}(\text{range}(\sigma))$, $\mathcal{S}(\text{range}(\sigma))$, $\mathcal{I}(\text{range}(\sigma))$, and $\mathcal{K}(\text{range}(\sigma))$, respectively.

Given a set of messages W, we denote by $\text{core}(W, M)$ what is left of the message M when it is decrypted as much as possible with respect to the knowledge of W.

Definition 14 (Core)
Let $W \subseteq \mathcal{M}$. The core of the message $M \in \mathcal{M}$ with respect to W, written $\mathrm{core}(W, M)$, is defined by

$$\mathrm{core}(W, M) \stackrel{def}{=} \begin{cases} \mathrm{core}(W, M') & \text{if } M = \{M'\}_k^E \text{ and } k \in \mathcal{K}(W) \\ M & \text{otherwise} \end{cases}$$

■

It can be seen that $\bigcup_{M \in W} \mathrm{core}(W, M) = \mathcal{I}(W)$. For an environment σ and a message M we will use the shorthand notation $\mathrm{core}(\sigma, M)$ for $\mathrm{core}(\mathrm{range}(\sigma), M)$.

We say that two environments are equivalent if they satisfy the same formulae.

Definition 15 (Equivalence of Environments, $\sim_e$)
Let Φ denote the set of formulae that can be generated from the following grammar.

$$\phi ::= \ tt \mid \phi \wedge \phi \mid \zeta = \zeta \mid \zeta : \mathcal{N}$$

Two environments σ_1 and σ_2 are equivalent, written $\sigma_1 \sim_e \sigma_2$, if $\mathrm{dom}(\sigma_1) = \mathrm{dom}(\sigma_2)$ and for each formula $\phi \in \Phi$ with $\mathrm{fn}(\phi) = \emptyset$ and $\mathrm{fz}(\phi) \subseteq \mathrm{dom}(\sigma_1)$ it holds that $e'(\phi\sigma_1) = tt$ if and only if $e'(\phi\sigma_2) = tt$. ■

4.2 Environment Sensitive Semantics

In the environment sensitive semantics environments and processes are paired in configurations.

Definition 16 (Configurations)
The set of configurations, Γ, is defined as

$$\Gamma \stackrel{def}{=} \{\sigma \rhd P \mid \sigma \in \Sigma \wedge P \in \mathcal{P}r\}$$

■

Configurations are ranged over by C.

The environment sensitive semantics for configurations is given by the labelled transition system $(\Gamma, \mathcal{A}ct_e, \longrightarrow)$, where $\longrightarrow$ is the smallest relation closed under the rules in table 4.1. Transitions have the form $\sigma \rhd P \xrightarrow[\delta]{\alpha} \sigma' \rhd P'$ and represent interactions between the process P and the environment σ. α is the process action and δ is the complementary environment action. The set of environment actions, $\mathcal{A}ct_e$, consists of the actions that can be generated using the following grammar.

$$\delta ::= \ - \mid a(z) \mid (\nu\ \tilde{c})\bar{a}\zeta$$

[E-Tau]	$\dfrac{P \xrightarrow[-]{\tau} P'}{\sigma \rhd P \xrightarrow[-]{\tau} \sigma \rhd P'}$	
[E-Inp]	$\dfrac{P \xrightarrow{a(u)} P'}{\sigma \rhd P \xrightarrow[(\nu\ \tilde{c})\bar{a}\zeta]{a(u)} \sigma[\tilde{z} \mapsto \tilde{c}] \rhd P'\{N/u\}}$	$e(\zeta\sigma) = N \neq \partial$, $\tilde{z} \cap \mathrm{dom}(\sigma) = \emptyset$, $a \in \mathcal{A}(\sigma)$, $\tilde{c} = \mathrm{n}(\zeta)$, and $\tilde{c} \cap \mathrm{fn}(P, \sigma) = \emptyset$
[E-Out]	$\dfrac{P \xrightarrow{(\nu\ \tilde{c})\bar{a}N} P'}{\sigma \rhd P \xrightarrow[a(z)]{(\nu\ \tilde{c})\bar{a}N} \sigma[z \mapsto N] \rhd P'}$	$a \in \mathcal{A}(\sigma), z \notin \mathrm{dom}(\sigma)$, and $\tilde{c} \cap \mathrm{fn}(\sigma) = \emptyset$

Table 4.1: Environment sensitive semantics.

For a configuration C we use $C \xRightarrow[\hat{\delta}]{\hat{\alpha}} C'$ as a shorthand notation for $C \xrightarrow[-]{\tau}{}^* \xrightarrow[\delta]{\alpha} \xrightarrow[-]{\tau}{}^* C'$ if $\alpha \neq \tau$ and $C \xrightarrow[-]{\tau}{}^* C'$ otherwise.

4.3 Environment Sensitive Bisimulation

We are now ready to define the notion of ***weak early environment sensitive bisimulation*** introduced by Boreale et al. in [6].

Definition 17 (Weak Early Environment Sensitive Bisimulation)
A symmetric relation $R \subseteq \Gamma \times \Gamma$ is a weak early environment sensitive bisimulation if $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$ implies $\sigma_P \sim_e \sigma_Q$ and whenever $\sigma_P \rhd P \xrightarrow[\delta]{\alpha} \sigma'_P \rhd P'$ there exist α', σ'_Q, and Q' such that $\sigma_Q \rhd Q \xRightarrow[\hat{\delta}]{\hat{\alpha'}} \sigma'_Q \rhd Q'$ and $(\sigma'_P \rhd P', \sigma'_Q \rhd Q') \in R$. ■

From the notion of weak early environment sensitive bisimulation we define the notion of ***weak early environment sensitive bisimilarity***.

Definition 18 (Weak Early Environment Sensitive Bisimilarity)
The configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ are weak early environment sensitive bisimilar, written $\sigma_P \rhd P \approx_{EESB} \sigma_Q \rhd Q$, if there exists a weak early environment sensitive bisimulation R such that $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. ■

In [6], Boreale et al. have shown that weak early environment sensitive bisimilarity is a sound approximation of testing equivalence in the sense that it implies testing equivalence under natural conditions on the environments involved.

Theorem 4 (Soundness of $\approx_{EESB}$ with respect to $\simeq$)
Let $P, Q \in \mathcal{P}r$. If $\mathrm{fn}(P,Q) = \mathrm{range}(\sigma)$ and $\sigma \rhd P \approx_{EESB} \sigma \rhd Q$ then $P \simeq Q$. ■

The following example illustrates that there exist configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ such that $\sigma_P \rhd P \approx_{EESB} \sigma_Q \rhd Q$ for which there does not exist a frame-theory pair (fr, th) such that $(fr, th) \vdash P \sim_f Q$.

Example 3. Consider the processes P and Q defined by

$$P \stackrel{def}{=} (\nu\ n)(\nu\ k)\bar{a}\{n\}^E_k.a(u).((u = b)\bar{a}n.\mathbf{0} \mid (u = c)\bar{a}n.\mathbf{0})$$
$$Q \stackrel{def}{=} (\nu\ m)(\nu\ n)(\nu\ k)\bar{a}\{\{n\}^E_m\}^E_k.a(u).((u = b)\bar{a}n.\mathbf{0} \mid (u = c)\bar{a}m.\mathbf{0})$$

It can be proven that $\{a/x_1, b/x_2, c/x_3\} \rhd P \approx_{EESB} \{a/x_1, b/x_2, c/x_3\} \rhd Q$. However, there does not exist a frame-theory pair (fr, th) such that $(fr, th) \vdash P \sim_f Q$ since there cannot exist a frame-theory pair (fr', th') such that $(fr', th') \vdash n \leftrightarrow m$. ■

The problem described in the example above also arises for ***strong early environment sensitive bisimilarity*** defined as follows.

Definition 19 (Strong Early Environment Sensitive Bisimulation)
A symmetric relation $R \subseteq \Gamma \times \Gamma$ is a strong early environment sensitive bisimulation if $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$ implies $\sigma_P \sim_e \sigma_Q$ and whenever $\sigma_P \rhd P \xrightarrow[\delta]{\alpha} \sigma'_P \rhd P'$ there exist α', σ'_Q, and Q' such that $\sigma_Q \rhd Q \xrightarrow[\delta]{\alpha'} \sigma'_Q \rhd Q'$ and $(\sigma'_P \rhd P', \sigma'_Q \rhd Q') \in R$. ■

From the notion of strong early environment sensitive bisimulation we define the notion of ***strong early environment sensitive bisimilarity***.

Definition 20 (Strong Early Environment Sensitive Bisimilarity)
The configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ are strong early environment sensitive bisimilar, written $\sigma_P \rhd P \sim_{EESB} \sigma_Q \rhd Q$, if there exists a strong early environment sensitive bisimulation R such that $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. ■

4.4 Equality of Equivalences of Environments

The logical characterization used in the definition of equivalence of environments makes it difficult to check whether or not two environments are equivalent since it contains a quantification over all formulae. Therefore, Boreale et al. gave an alternative characterization of equivalence of environments. In this section we present this alternative characterization.

For a tuple $\tilde{M} \stackrel{def}{=} M_{i \in I}$ and a tuple $\tilde{J} \stackrel{def}{=} (j_1, \ldots, j_n) \subseteq I$ we let $\tilde{M}[\tilde{J}]$ denote the tuple $(M_{j_1}, \ldots, M_{j_n})$.

Definition 21 (Equivalence of Environments, $\sim'_e$)
Let σ and σ' be environments and assume $\mathrm{dom}(\sigma) = \mathrm{dom}(\sigma') = \{x_i \mid i \in I\}$ for some set of indices I. For each $i \in I$ let $N_i \stackrel{def}{=} \mathrm{core}(\sigma, \sigma(x_i))$ and $N'_i \stackrel{def}{=} \mathrm{core}(\sigma', \sigma'(x_i))$. σ and σ' are equivalent, written $\sigma \sim'_e \sigma'$, if for each $i \in I$ the following holds,

(i) for some tuple $\tilde{J}_i \subseteq I$ it holds that $\sigma(x_i) = \{N_i\}^E_{\tilde{N}[\tilde{J}_i]}$ and $\sigma'(x_i) = \{N'_i\}^E_{\tilde{N}'[\tilde{J}_i]}$,

(ii) for each $j \in I$, $N_i = N_j$ if and only if $N'_i = N'_j$, and

(iii) $N_i \in \mathcal{N}$ if and only if $N'_i \in \mathcal{N}$.

■

The following theorem, proven by Boreale et al. in [6], states that the two notions of equivalence of environments coincide.

Theorem 5 (Coincidence of $\sim_e$ and $\sim'_e$)
$\sigma_1 \sim_e \sigma_2$ if and only if $\sigma_1 \sim'_e \sigma_2$. ■

4.5 Properties of Environments

In this section we present two lemmas proven by Boreale et al. in [6]. We will need these lemmas in the following chapters.

Lemma 1
Let $\sigma \stackrel{def}{=} \{M_i/x_i\}_{i \in I}$.

(*i*) If $M \in \mathcal{A}(\sigma)$ then there exists $\zeta \in \Upsilon$ such that $\mathrm{n}(\zeta) = \emptyset$, $\mathrm{fz}(\zeta) \subseteq \mathrm{dom}(\sigma)$, and $e(\zeta\sigma) = M$.

(*ii*) If $a \in \mathcal{A}(\sigma)$ then $a = \mathrm{core}(\sigma, \sigma(x_i))$, for some $i \in I$.

■

Lemma 2
Let $\sigma_1 \stackrel{def}{=} \{M_i/x_i\}_{i \in I}$ and $\sigma_2 \stackrel{def}{=} \{M'_i/x_i\}_{i \in I}$ be two environments such that $\sigma_1 \sim_e \sigma_2$. Let $\tilde{N} \stackrel{def}{=} \mathrm{core}(\sigma_1, \sigma_1(x_i))_{i \in I}$ and $\tilde{N}' \stackrel{def}{=} \mathrm{core}(\sigma_2, \sigma_2(x_i))_{i \in I}$. For each $\zeta \in \Upsilon$ such that $\mathrm{n}(\zeta) = \emptyset$ and $\mathrm{fz}(\zeta) \subseteq \mathrm{dom}(\sigma_1)$, either

(*i*) $e(\zeta\sigma_1) = e(\zeta\sigma_2) = \partial$, or

(*ii*) there exist $i \in I$ and a tuple $\tilde{J} \subseteq I$ such that $e(\zeta\sigma_1) = \{N_i\}^E_{\tilde{N}[\tilde{J}]}$ and $e(\zeta\sigma_2) = \{N'_i\}^E_{\tilde{N}'[\tilde{J}]}$. ■

In the following chapter we will proceed by showing that a late version of strong early environment sensitive bisimilarity based on a new notion of equivalence of environments is the same as framed bisimilarity.

5 Two Notions of Framed Bisimilarity

As mentioned in the previous chapter there exist configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ such that $\sigma_P \rhd P \sim_{EESB} \sigma_Q \rhd Q$ for which there does not exist a frame-theory pair (fr, th) such that $(fr, th) \vdash P \sim_f Q$. This is due to the fact that for two equivalent environments σ_1 and σ_2 we can have $\text{core}(\sigma_1, \sigma_1(x)) = a$ and $\text{core}(\sigma_2, \sigma_2(x)) = b$ for two different names a and b. In this chapter we present a new strong late version of the environment sensitive bisimulation given by Boreale at al. For this definition we will use a notion of equivalence of environments that does not allow a and b to be different. Furthermore, we will prove that the strong late version of environment sensitive bisimilarity can be used as an alternative characterization of framed bisimilarity. In the first four sections we will consider an expression and message grammar without pairs and projection. We will continue to refer to the set of expressions and the set of messages as $\mathcal{L}$ and $\mathcal{M}$, respectively. In section 5.5 we will extend the results of the first four sections to an expression and message grammar with pairs and projection.

5.1 Strong Late Environment Sensitive Bisimulation

The strong late version of environment sensitive bisimulation we present is based on a new notion of equivalence of environments.

Definition 22 (Equivalence of Environments, $\sim''_e$)
Let σ and σ' be environments and assume $\text{dom}(\sigma) = \text{dom}(\sigma') = \{x_i \mid i \in I\}$ for some set of indices I. For each $i \in I$ let $N_i \stackrel{def}{=} \text{core}(\sigma, \sigma(x_i))$ and $N'_i \stackrel{def}{=} \text{core}(\sigma', \sigma'(x_i))$. σ and σ' are equivalent, written $\sigma \sim''_e \sigma'$, if for each $i \in I$ the following holds,

(i) for some $\tilde{k}_i$ it holds that $\sigma(x_i) = \{N_i\}^E_{\tilde{k}_i}$ and $\sigma'(x_i) = \{N'_i\}^E_{\tilde{k}_i}$,

(ii) for each $j \in I$, $N_i = N_j$ if and only if $N'_i = N'_j$, and

(iii) for each $N \in \mathcal{N}$, $N_i = N$ if and only if $N'_i = N$.

■

The following theorem states soundness of $\sim''_e$ with respect to $\sim_e$ and $\sim'_e$. This implies that lemmas 1 and 2 also hold for $\sim''_e$.

Theorem 6 (Soundness of $\sim''_e$ with respect to $\sim_e$ and $\sim'_e$)
$\sigma_1 \sim''_e \sigma_2$ implies $\sigma_1 \sim_e \sigma_2$ and $\sigma_1 \sim'_e \sigma_2$.

Proof: It is easily seen from definitions 21 and 22 that $\sigma_1 \sim''_e \sigma_2$ implies $\sigma_1 \sim'_e \sigma_2$. By theorem 5 we also have that $\sigma_1 \sim''_e \sigma_2$ implies $\sigma_1 \sim_e \sigma_2$. ■

To see that $\sim''_e$ is not complete with respect to $\sim_e$ and $\sim'_e$ consider the two environments $\sigma_1 \stackrel{def}{=} \{\{a\}^E_{k_1}/x_1, k_1/x_2\}$ and $\sigma_2 \stackrel{def}{=} \{\{b\}^E_{k_2}/x_1, k_2/x_2\}$. We have $\sigma_1 \sim'_e \sigma_2$ but not $\sigma_1 \sim''_e \sigma_2$.

Now, we define the notion of ***strong late environment sensitive bisimulation***.

Definition 23 (Strong Late Environment Sensitive Bisimulation)
A symmetric relation $R \subseteq \Gamma \times \Gamma$ is a strong late environment sensitive bisimulation if $(\sigma_1 \rhd P, \sigma_2 \rhd Q) \in R$ implies $\sigma_1 \sim''_e \sigma_2$ and if $P \stackrel{\alpha}{\longrightarrow} P'$ then

(i) if $\alpha = \tau$ then there exists Q' such that $Q \stackrel{\alpha}{\longrightarrow} Q'$ and $(\sigma_1 \rhd P', \sigma_2 \rhd Q') \in R$.

(ii) if $\alpha = a(u)$ and $a \in \mathcal{A}(\sigma_1)$ then there exists Q' such that $Q \stackrel{a(u)}{\longrightarrow} Q'$ and for all $\zeta \in \Upsilon$, where $e(\zeta\sigma_1) \neq \partial$ and $\mathrm{n}(\zeta) \cap \mathrm{fn}(P, Q, \sigma_1, \sigma_2) = \emptyset$, $(\sigma_1[\tilde{z} \mapsto \tilde{c}] \rhd P'\{e(\zeta\sigma_1)/u\}, \sigma_2[\tilde{z} \mapsto \tilde{c}] \rhd Q'\{e(\zeta\sigma_2)/u\}) \in R$, where $\tilde{z} \cap \mathrm{dom}(\sigma_1) = \emptyset$ and $\tilde{c} = \mathrm{n}(\zeta)$.

(iii) if $\alpha = (\nu\ \tilde{c})\bar{a}M$, $a \in \mathcal{A}(\sigma_1)$, and $\tilde{c} \cap \mathrm{fn}(P, \sigma_1) = \emptyset$ then there exist $\tilde{d}$, N, and Q' such that $Q \stackrel{(\nu\ \tilde{d})\bar{a}N}{\longrightarrow} Q'$, where $\tilde{d} \cap \mathrm{fn}(Q, \sigma_2) = \emptyset$, and $(\sigma_1[z \mapsto M] \rhd P', \sigma_2[z \mapsto N] \rhd Q') \in R$, where $z \notin \mathrm{dom}(\sigma_1)$.

■

From the definition of strong late environment sensitive bisimulation we define the notion of ***strong late environment sensitive bisimilarity***.

Definition 24 (Strong Late Environment Sensitive Bisimilarity)
The configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ are strong late environment sensitive bisimilar, written $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$, if there exists a strong late environment sensitive bisimulation R such that $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. ■

5.2 The Functions $\mathcal{F}_e$ and $\mathcal{F}_{ESB}$

Since strong late environment sensitive bisimilarity relates pairs of configurations and framed bisimilarity relates pairs of processes with respect to frame-theory pairs we need a way to convert a pair of environments to a frame-theory pair to be able to use strong late environment sensitive bisimilarity to characterize framed bisimilarity. Therefore, we define a function $\mathcal{F}_e$ that takes two equivalent environments as input and returns a frame-theory pair.

Definition 25 (The Function $\mathcal{F}_e$)
Let σ_1 and σ_2 be two environments such that $\sigma_1 \sim_e'' \sigma_2$ and $\mathrm{dom}(\sigma_1) = \mathrm{dom}(\sigma_2) = \{x_i \mid i \in I\}$, and let $N_i \stackrel{def}{=} \mathrm{core}(\sigma_1, \sigma_1(x_i))$ and $N_i' \stackrel{def}{=} \mathrm{core}(\sigma_2, \sigma_2(x_i))$. Also, let $\mathit{fr} \stackrel{def}{=} \{N_i \mid i \in I \wedge N_i \in \mathcal{N}\}$ and $\mathit{th} \stackrel{def}{=} \{(N_i, N_i') \mid i \in I \wedge N_i \notin \mathcal{N}\}$. The function $\mathcal{F}_e$ is defined as $\mathcal{F}_e(\sigma_1, \sigma_2) \stackrel{def}{=} (\mathit{fr}, \mathit{th})$. ■

From the definition of $\mathcal{F}_e$ we define the function $\mathcal{F}_{ESB}$ that takes a strong late environment sensitive bisimulation as input and returns a set of framed process pairs which will later turn out to be a framed bisimulation.

Definition 26 (The Function $\mathcal{F}_{ESB}$)
Let R be a strong late environment sensitive bisimulation. Then $\mathcal{F}_{ESB}(R) \stackrel{def}{=} \{(\mathit{fr}, \mathit{th}, P, Q) \mid \exists \sigma_1, \sigma_2.((\sigma_1 \rhd P, \sigma_2 \rhd Q) \in R \wedge \mathcal{F}_e(\sigma_1, \sigma_2) = (\mathit{fr}, \mathit{th}))\}$. ■

The following theorem states that a frame-theory pair returned from $\mathcal{F}_e$ is ok. This implies that a relation returned by $\mathcal{F}_{ESB}$ is a framed relation.

Theorem 7
Let $\sigma_1 \sim_e'' \sigma_2$ and $(\mathit{fr}, \mathit{th}) \stackrel{def}{=} \mathcal{F}_e(\sigma_1, \sigma_2)$, then $(\mathit{fr}, \mathit{th}) \vdash \mathit{ok}$.

Proof:

(i) Assume $(M, N) \in \mathit{th}$. By definition of $\mathcal{F}_e$ we have $M = \{M_1\}^E_{M_2}$. Since $M_2 \in \mathcal{N}$ and $M_2 \neq \mathrm{core}(\sigma_1, \sigma_1(x))$ for all $x \in \mathrm{dom}(\sigma_1)$ we have $M_2 \notin \mathit{fr}$ and there does not exist N' such that $(\mathit{fr}, \mathit{th}) \vdash M_2 \leftrightarrow N'$. Similarly for N.

(ii) Assume $(M, N) \in \mathit{th}$, $(M', N') \in \mathit{th}$, and $M = M'$. Since $M = \mathrm{core}(\sigma_1, \sigma_1(x))$ and $M' = \mathrm{core}(\sigma_1, \sigma_1(y))$ for some $x, y \in \mathrm{dom}(\sigma_1)$ we have by *(ii)* of definition 22 that $N = \mathrm{core}(\sigma_2, \sigma_2(x)) = \mathrm{core}(\sigma_2, \sigma_2(y)) = N'$. Similarly it can be shown that $M = M'$ if $(M, N) \in \mathit{th}$, $(M', N') \in \mathit{th}$, and $N = N'$.

■

In the following two sections we show that if $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ then $\mathcal{F}_e(\sigma_P, \sigma_Q) \vdash P \sim_f Q$ and if $(\mathit{fr}, \mathit{th}) \vdash P \sim_f Q$, $\sigma_P \sim_e'' \sigma_Q$, and $\mathcal{F}_e(\sigma_P, \sigma_Q) = (\mathit{fr}, \mathit{th})$ then $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$.

5.3 Soundness

To prove soundness of strong late environment sensitive bisimilarity with respect to framed bisimilarity we make use of the following four lemmas.

Lemma 3
Let $\sigma_1 \sim''_e \sigma_2$ and $(fr, th) \stackrel{def}{=} \mathcal{F}_e(\sigma_1, \sigma_2)$. For all sets of names $\tilde{c}$ and all $M, N \in \mathcal{M}$, where $\tilde{c} \cap \mathrm{n}(\sigma_1, \sigma_2) = \emptyset$ and $(fr \cup \tilde{c}, th) \vdash M \leftrightarrow N$, there exists $\zeta \in \Upsilon$ such that $M = e(\zeta\sigma_1)$, $N = e(\zeta\sigma_2)$, and $\mathrm{n}(\zeta) = \tilde{c}$.

Proof: We will prove that there exists $\zeta \in \Upsilon$ such that $M = e(\zeta\sigma_1)$, $N = e(\zeta\sigma_2)$, and $\mathrm{n}(\zeta) \subseteq \tilde{c}$. This will prove the lemma since $e(\zeta\sigma) = e(\{\{\zeta\}^E_{\tilde{c}}\}^D_{\tilde{c}}\sigma)$. The proof is by induction on the depth of the inference of $(fr \cup \tilde{c}, th) \vdash M \leftrightarrow N$.

Basis: depth $= 0$.

Case $M = N = n \in \tilde{c}$.
In this case we let $\zeta \stackrel{def}{=} n$.

Case $M = N = n \in fr$ or $(M, N) \in th$.
By lemmas 1 and 2 there exists $\zeta \in \Upsilon$ such that $M = e(\zeta\sigma_1)$, $N = e(\zeta\sigma_2)$, and $\mathrm{n}(\zeta) = \emptyset$.

Step: depth > 0.

Case $M = \{M_1\}^E_{M_2}$, $N = \{N_1\}^E_{N_2}$, and $(M, N) \notin th$.
Since $(M, N) \notin th$, $(fr \cup \tilde{c}, th) \vdash M \leftrightarrow N$ must have been deduced by the Eq encrypt rule. That is $(fr \cup \tilde{c}, th) \vdash M_1 \leftrightarrow N_1$ and $(fr \cup \tilde{c}, th) \vdash M_2 \leftrightarrow N_2$. By induction there exist $\zeta_1, \zeta_2 \in \Upsilon$ such that $M_1 = e(\zeta_1\sigma_1)$, $N_1 = e(\zeta_1\sigma_2)$, $\mathrm{n}(\zeta_1) \subseteq \tilde{c}$, $M_2 = e(\zeta_2\sigma_1)$, $N_2 = e(\zeta_2\sigma_2)$, and $\mathrm{n}(\zeta_2) \subseteq \tilde{c}$. So, by letting $\zeta \stackrel{def}{=} \{\zeta_1\}^E_{\zeta_2}$ we get $M = e(\zeta\sigma_1)$, $N = e(\zeta\sigma_2)$, and $\mathrm{n}(\zeta) \subseteq \tilde{c}$.

■

Lemma 4
Let $\sigma_1 \sim''_e \sigma_2$. For all sets of names $\tilde{c}$ and for all sets of variables $\tilde{z}$, where $\tilde{c} \cap \mathrm{fn}(\sigma_1, \sigma_2) = \emptyset$ and $\tilde{z} \cap \mathrm{dom}(\sigma_1) = \emptyset$, it holds that $\sigma_1[\tilde{z} \mapsto \tilde{c}] \sim''_e \sigma_2[\tilde{z} \mapsto \tilde{c}]$.

Proof: This is trivial since $\tilde{c}$ cannot be used to decrypt any messages in range(σ_1) and range(σ_2). ■

Lemma 5
Let $\sigma_1 \sim''_e \sigma_2$ and $(fr, th) \stackrel{def}{=} \mathcal{F}_e(\sigma_1, \sigma_2)$. Then $(fr \cup \tilde{c}, th) = \mathcal{F}_e(\sigma_1[\tilde{z} \mapsto \tilde{c}], \sigma_2[\tilde{z} \mapsto \tilde{c}])$, where $\tilde{z} \cap \mathrm{dom}(\sigma_1) = \emptyset$ and $\tilde{c} \cap \mathrm{fn}(\sigma_1, \sigma_2) = \emptyset$.

Proof: This is trivial since $\mathrm{core}(\sigma_1[\tilde{z} \mapsto \tilde{c}], \sigma_1[\tilde{z} \mapsto \tilde{c}](x)) = \mathrm{core}(\sigma_1, \sigma_1(x))$ and $\mathrm{core}(\sigma_2[\tilde{z} \mapsto \tilde{c}], \sigma_2[\tilde{z} \mapsto \tilde{c}](x)) = \mathrm{core}(\sigma_2, \sigma_2(x))$ for all $x \notin \tilde{z}$. ■

Lemma 6
Let $\sigma_1 \sim''_e \sigma_2$ and $(fr, th) \stackrel{def}{=} \mathcal{F}_e(\sigma_1, \sigma_2)$. If $\sigma_1[z \mapsto M] \sim''_e \sigma_2[z \mapsto N]$, where $z \notin \mathrm{dom}(\sigma_1)$, then

(*i*) $(fr, th) \leq (fr', th')$, and

(*ii*) $(fr', th') \vdash M \leftrightarrow N$,

where $(fr', th') \stackrel{def}{=} \mathcal{F}_e(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N])$.

Proof: Let $\sigma'_1 \stackrel{def}{=} \sigma_1[z \mapsto M]$ and $\sigma'_2 \stackrel{def}{=} \sigma_2[z \mapsto N]$.

(*i*) By theorem 7 we get $(fr', th') \vdash ok$. It is easily seen that $fr \subseteq fr'$, so by theorem 1 it is enough to show that $(fr', th') \vdash M' \leftrightarrow N'$ for each $(M', N') \in th$ to prove that $(fr, th) \leq (fr', th')$. Assume $(M', N') \in th$. Since $M' = \mathrm{core}(\sigma_1, \sigma_1(x))$ and $N' = \mathrm{core}(\sigma_2, \sigma_2(x))$ for some $x \in \mathrm{dom}(\sigma_1)$, there exists $\tilde{k} \subseteq fr$ such that $\sigma_1(x) = \{M'\}^E_{\tilde{k}}$ and $\sigma_2(x) = \{N'\}^E_{\tilde{k}}$. Let $M'' = \mathrm{core}(\sigma'_1, \sigma'_1(x))$ and $N'' = \mathrm{core}(\sigma'_2, \sigma'_2(x))$, then there exists $\tilde{k}' \subseteq fr'$ such that $\sigma_1(x) = \sigma'_1(x) = \{M''\}^E_{\tilde{k}'}$ and $\sigma_2(x) = \sigma'_2(x) = \{N''\}^E_{\tilde{k}'}$. $\tilde{k}'$ can be split into two sets $\tilde{k}'_1$ and $\tilde{k}'_2$ such that $M' = \{M''\}^E_{\tilde{k}'_1}$, $N' = \{N''\}^E_{\tilde{k}'_1}$, and $\tilde{k} = \tilde{k}'_2$. We must have either $(M'', N'') \in th'$ or $M'' = N'' \in fr'$. From table 3.1 we easily deduce $(fr', th') \vdash M' \leftrightarrow N'$.

(*ii*) Let $\tilde{M} = \mathrm{core}(\sigma'_1, \sigma'_1(x))_{x \in \mathrm{dom}(\sigma'_1)}$ and $\tilde{N} = \mathrm{core}(\sigma'_2, \sigma'_2(x))_{x \in \mathrm{dom}(\sigma'_2)}$. Since $M \in \mathcal{A}(\sigma'_1)$ we have, by lemma 1, that there exists $\zeta \in \Upsilon$ such that $M = e(\zeta\sigma'_1)$, and by lemma 2 we get $M = \{M_x\}^E_{\tilde{k}}$ and $N = \{N_x\}^E_{\tilde{k}}$. Since $\tilde{k} \subseteq fr'$ and either $(M_x, N_x) \in th'$ or $M_x = N_x \in fr'$ we deduce $(fr', th') \vdash M \leftrightarrow N$ from table 3.1.

■

Now, we are ready to prove that a framed relation returned from $\mathcal{F}_{ESB}$ is a framed bisimulation.

Theorem 8 (Soundness)
Let R be a strong late environment sensitive bisimulation. Then $\mathcal{F}_{ESB}(R)$ is a framed bisimulation.

Proof: Assume $(fr, th) \vdash P \ \mathcal{F}_{ESB}(R)\ Q$. Then there must exist σ_P and σ_Q such that $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$ and $\mathcal{F}_e(\sigma_P, \sigma_Q) = (fr, th)$.

$P \stackrel{\tau}{\longrightarrow} P'$.
Since R is a strong late environment sensitive bisimulation there exists Q' such that $Q \stackrel{\tau}{\longrightarrow} Q'$ and $(\sigma_P \rhd P', \sigma_Q \rhd Q') \in R$. This implies $(fr, th) \vdash P' \ \mathcal{F}_{ESB}(R)\ Q'$.

$P \xrightarrow{a(u)} P'$ and $a \in fr$.

We have that $a \in \mathcal{A}(\sigma_P)$, and since R is a strong late environment sensitive bisimulation there exists Q' such that $Q \xrightarrow{a(u)} Q'$ and for all $\zeta \in \Upsilon$, where $e(\zeta\sigma_P) \neq \partial$ and $\mathrm{n}(\zeta) \cap \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) = \emptyset$, it holds that $(\sigma_P[\tilde{z} \mapsto \tilde{c}] \rhd P'\{e(\zeta\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \tilde{c}] \rhd Q'\{e(\zeta\sigma_Q)/u\}) \in R$, where $\tilde{z} \cap \mathrm{dom}(\sigma_P) = \emptyset$ and $\tilde{c} = \mathrm{n}(\zeta)$.
Let $\tilde{n}$ be a set of names such that $\tilde{n} \cap (\mathrm{fn}(P, Q) \cup fr \cup \mathrm{n}(th)) = \emptyset$ and let $M, N \in \mathcal{M}$ such that $(fr \cup \tilde{n}, th) \vdash M \leftrightarrow N$. By lemma 3 there exists $\zeta' \in \Upsilon$ such that $M = e(\zeta'\sigma_P)$, $N = e(\zeta'\sigma_Q)$, and $\tilde{n} = \mathrm{n}(\zeta')$. Since $\tilde{n} \cap \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) = \emptyset$ it follows by lemma 5 that $(fr \cup \tilde{n}, th) \vdash P'\{M/u\}\ \mathcal{F}_{ESB}(R)\ Q'\{N/u\}$.

$P \xrightarrow{(\nu\ \tilde{m})\bar{a}M} P'$, $a \in fr$, and $\tilde{m} \cap (\mathrm{fn}(P) \cup fr \cup \mathrm{n}(\pi_1(th))) = \emptyset$.
In this case we have $a \in \mathcal{A}(\sigma_P)$ and $\tilde{m} \cap \mathrm{fn}(P, \sigma_P) = \emptyset$. So by the fact that R is a strong late environment sensitive bisimulation there exist $\tilde{n}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{n})\bar{a}N} Q'$, $\tilde{n} \cap \mathrm{fn}(Q, \sigma_Q) = \emptyset$, and $(\sigma_P[z \mapsto M] \rhd P', \sigma_Q[z \mapsto N] \rhd Q') \in R$, where $z \notin \mathrm{dom}(\sigma_P)$. By lemma 6 $(fr, th) \leq \mathcal{F}_e(\sigma_P[z \mapsto M], \sigma_Q[z \mapsto N])$ and $\mathcal{F}_e(\sigma_P[z \mapsto M], \sigma_Q[z \mapsto N]) \vdash M \leftrightarrow N$. This proves the theorem since $\mathcal{F}_e(\sigma_P[z \mapsto M], \sigma_Q[z \mapsto N]) \vdash P'\ \mathcal{F}_{ESB}(R)\ Q'$ and $\tilde{n} \cap (\mathrm{fn}(Q) \cup fr \cup \mathrm{n}(\pi_2(th))) = \emptyset$.

■

5.4 Completeness

To prove completeness of strong late environment sensitive bisimilarity with respect to framed bisimilarity we need the following three lemmas.

Lemma 7
Let $\sigma_1 \sim''_e \sigma_2$ and $(fr, th) \stackrel{def}{=} \mathcal{F}_e(\sigma_1, \sigma_2)$. Also, let $\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap \mathrm{n}(\sigma_1, \sigma_2) = \emptyset$ and $e(\zeta\sigma_1) \neq \partial$, $M \stackrel{def}{=} e(\zeta\sigma_1)$, and $N \stackrel{def}{=} e(\zeta\sigma_2)$. Then $(fr \cup \mathrm{n}(\zeta), th) \vdash M \leftrightarrow N$.

Proof: The proof is by induction on the structure of ζ.

Basis:

Case $\zeta = a$.
This case is trivial since $(fr \cup \{a\}, th) \vdash a \leftrightarrow a$.

Case $\zeta = x$.
Since $\sigma_1 \sim''_e \sigma_2$ there exists $\tilde{k}$ such that $\sigma_1(x) = \{\mathrm{core}(\sigma_1, \sigma_1(x))\}^E_{\tilde{k}}$ and $\sigma_2(x) = \{\mathrm{core}(\sigma_2, \sigma_2(x))\}^E_{\tilde{k}}$. We have $(\mathrm{core}(\sigma_1, \sigma_1(x)), \mathrm{core}(\sigma_2, \sigma_2(x))) \in th$ or $\mathrm{core}(\sigma_1, \sigma_1(x)) = \mathrm{core}(\sigma_2, \sigma_2(x)) \in fr$ and $\tilde{k} \subseteq fr$. From table 3.1 we deduce $(fr, th) \vdash M \leftrightarrow N$.

Step:

Case $\zeta = \{\zeta_1\}^E_{\zeta_2}$.
By induction we get $(fr \cup \mathrm{n}(\zeta_1), th) \vdash e(\zeta_1\sigma_1) \leftrightarrow e(\zeta_1\sigma_2)$ and $(fr \cup \mathrm{n}(\zeta_2), th) \vdash e(\zeta_2\sigma_1) \leftrightarrow e(\zeta_2\sigma_2)$. This implies $(fr \cup \mathrm{n}(\zeta), th) \vdash M \leftrightarrow N$.

Case $\zeta = \{\zeta_1\}^D_{\zeta_2}$.
By induction we get $(fr \cup \mathrm{n}(\zeta_1), th) \vdash e(\zeta_1\sigma_1) \leftrightarrow e(\zeta_1\sigma_2)$ and $(fr \cup \mathrm{n}(\zeta_2), th) \vdash e(\zeta_2\sigma_1) \leftrightarrow e(\zeta_2\sigma_2)$. This implies $(fr \cup \mathrm{n}(\zeta), th) \vdash e(\zeta_1\sigma_1) \leftrightarrow e(\zeta_1\sigma_2)$ and $(fr \cup \mathrm{n}(\zeta), th) \vdash e(\zeta_2\sigma_1) \leftrightarrow e(\zeta_2\sigma_2)$. Since $e(\{\zeta_1\}^D_{\zeta_2}\sigma_1) = M$ and $e(\{\zeta_1\}^D_{\zeta_2}\sigma_2) = N$, $(fr \cup \mathrm{n}(\zeta), th) \vdash e(\zeta_1\sigma_1) \leftrightarrow e(\zeta_1\sigma_2)$ can only have been deduced if $(fr \cup \mathrm{n}(\zeta), th) \vdash e(\zeta_2\sigma_1) \leftrightarrow e(\zeta_2\sigma_2)$ and $(fr \cup \mathrm{n}(\zeta), th) \vdash M \leftrightarrow N$.

■

Lemma 8
Let $(fr, th) \vdash ok$, $\xi((fr, th), M, N) \neq \bot$, and $(fr', th') \stackrel{def}{=} \xi((fr, th), M, N)$, then

$$\begin{aligned} fr' &= \mathcal{K}(fr \cup \pi_1(th) \cup \{M\}) = \mathcal{K}(fr \cup \pi_2(th) \cup \{N\}) \\ \pi_1(th') &= \mathcal{I}(fr \cup \pi_1(th) \cup \{M\}) \setminus \mathcal{N} \\ \pi_2(th') &= \mathcal{I}(fr \cup \pi_2(th) \cup \{N\}) \setminus \mathcal{N} \end{aligned}$$

Proof: In the proof we make use of the fact that $(fr, th) \vdash ok$ implies

$$\begin{aligned} fr &= \mathcal{K}(fr \cup \pi_1(th)) = \mathcal{K}(fr \cup \pi_2(th)) \\ \pi_1(th) &= \mathcal{I}(fr \cup \pi_1(th)) \setminus \mathcal{N} \\ \pi_2(th) &= \mathcal{I}(fr \cup \pi_2(th)) \setminus \mathcal{N} \end{aligned}$$

The proof will be by induction on the number n_ξ of calls of the ξ-function.

Basis: $n_\xi = 1$.

Case $(fr, th) \vdash M \leftrightarrow N$.
We have $fr' = fr = \mathcal{K}(fr \cup \pi_1(th))$. Since $M \in \mathcal{S}(fr \cup \pi_1(th))$ it follows that $fr' = \mathcal{K}(fr \cup \pi_1(th) \cup \{M\})$. For similar reasons we also have $fr' = \mathcal{K}(fr \cup \pi_2(th) \cup \{N\})$, $\pi_1(th') = \mathcal{I}(fr \cup \pi_1(th) \cup \{M\}) \setminus \mathcal{N}$, and $\pi_2(th') = \mathcal{I}(fr \cup \pi_2(th) \cup \{N\}) \setminus \mathcal{N}$.

Case $M = N = n$ and there does not exist $(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2}) \in th$ such that $M_2 = N_2 = n$.
$fr' = fr \cup \{n\} = \mathcal{K}(fr \cup \pi_1(th)) \cup \{n\}$. Since there does not exist $(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2}) \in th$ such that $M_2 = N_2 = n$ we have $fr' = \mathcal{K}(fr \cup \pi_1(th) \cup \{n\})$. Similarly we have $fr' = \mathcal{K}(fr \cup \pi_2(th) \cup \{n\})$. Since $\pi_1(th') = \pi_1(th) = \mathcal{I}(fr \cup \pi_1(th)) \setminus \mathcal{N}$ and there does not exist $(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2}) \in th$ such that $M_2 = N_2 = n$ we have $\pi_1(th') = \mathcal{I}(fr \cup \pi_1(th) \cup \{n\}) \setminus \mathcal{N}$. Similarly for $\pi_2(th')$.

Case $M = \{M_1\}^E_{M_2}$, $N = \{N_1\}^E_{N_2}$, and $M_2, N_2 \notin fr$.

We have $fr' = fr = \mathcal{K}(fr \cup \pi_1(th)) = \mathcal{K}(fr \cup \pi_2(th))$. Since $M_2, N_2 \notin fr$ it follows that $fr' = \mathcal{K}(fr \cup \pi_1(th) \cup \{M\}) = \mathcal{K}(fr \cup \pi_2(th) \cup \{N\})$. Also, $\pi_1(th') = \pi_1(th) \cup \{M\} = \mathcal{I}(fr \cup \pi_1(th)) \setminus \mathcal{N} \cup \{M\}$. Since $M_2 \notin fr$ it follows that $\pi_1(th') = \mathcal{I}(fr \cup \pi_1(th) \cup \{M\}) \setminus \mathcal{N}$. Similarly for $\pi_2(th')$.

Step: $n_\xi > 1$.

Case $M = \{M_1\}^E_{M_2}$, $N = \{N_1\}^E_{N_2}$, and $(fr, th) \vdash M_2 \leftrightarrow N_2$ ($M_2 = N_2 \in fr$).

We have $(fr', th') = \xi((fr, th), M_1, N_1)$ (line 14 of the ξ-function in figure 3.1). By induction we get $fr' = \mathcal{K}(fr \cup \pi_1(th) \cup \{M_1\}) = \mathcal{K}(fr \cup \pi_2(th) \cup \{N_1\})$, $\pi_1(th') = \mathcal{I}(fr \cup \pi_1(th) \cup \{M_1\}) \setminus \mathcal{N}$, and $\pi_2(th') = \mathcal{I}(fr \cup \pi_2(th) \cup \{N_1\}) \setminus \mathcal{N}$. Since $M_2, N_2 \in fr$ it follows that $fr' = \mathcal{K}(fr \cup \pi_1(th) \cup \{M\}) = \mathcal{K}(fr \cup \pi_2(th) \cup \{N\})$, $\pi_1(th') = \mathcal{I}(fr \cup \pi_1(th) \cup \{M\}) \setminus \mathcal{N}$, and $\pi_2(th') = \mathcal{I}(fr \cup \pi_2(th) \cup \{N\}) \setminus \mathcal{N}$.

Case $M = N = n \notin fr$ and there exists $(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2}) \in th$ such that $M_2 = N_2 = n$.

Let $\lambda \stackrel{def}{=} \{(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2}) \in th \mid M_2, N_2 \in \{n\}\}$ (lines 6-10 of the ξ-function in figure 3.1). Furthermore, let $fr_\xi \stackrel{def}{=} fr \cup \{n\}$, $th_\xi \stackrel{def}{=} th \setminus \lambda$. Let (fr^i_ξ, th^i_ξ) be the frame-theory pair obtained from the ith application of the ξ-function in the for-loop in lines 11-12 of the ξ-function in figure 3.1. Since $(fr^0_\xi, th^0_\xi) \vdash ok$ ($fr^0_\xi = fr_\xi$ and $th^0_\xi = th_\xi$) it follows, by the fact that the frame-theory pair returned by the ξ-function is ok, that $(fr^i_\xi, th^i_\xi) \vdash ok$ for all i. Now, let M^i_λ and N^i_λ be the messages M_1 and N_1, respectively, of the ith run of line 12 of the ξ-function in figure 3.1. Let (fr^F_ξ, th^F_ξ) be the frame-theory pair obtained from the final application of the

ξ-function in the for-loop. Then, by induction, we have

$$\begin{aligned}
\mathcal{I}(fr' \cup \pi_1(th')) &= \mathcal{I}(fr_\xi^F \cup \pi_1(th_\xi^F)) \\
&= \mathcal{I}(\mathcal{K}(fr_\xi^{F-1} \cup \pi_1(th_\xi^{F-1}) \cup \{M_\lambda^F\}) \cup \\
&\qquad \mathcal{I}(fr_\xi^{F-1} \cup \pi_1(th_\xi^{F-1}) \cup \{M_\lambda^F\}) \setminus \mathcal{N}) \\
&= \mathcal{I}(\mathcal{I}(fr_\xi^{F-1} \cup \pi_1(th_\xi^{F-1}) \cup \{M_\lambda^F\})) \\
&= \mathcal{I}(fr_\xi^{F-1} \cup \pi_1(th_\xi^{F-1}) \cup \{M_\lambda^F\}) \\
&= \mathcal{I}(\mathcal{K}(fr_\xi^{F-2} \cup \pi_1(th_\xi^{F-2}) \cup \{M_\lambda^{F-1}\}) \cup \\
&\qquad \mathcal{I}(fr_\xi^{F-2} \cup \pi_1(th_\xi^{F-2}) \cup \{M_\lambda^{F-1}\}) \setminus \mathcal{N} \cup \{M_\lambda^F\}) \\
&= \mathcal{I}(\mathcal{I}(fr_\xi^{F-2} \cup \pi_1(th_\xi^{F-2}) \cup \{M_\lambda^{F-1}\}) \cup \{M_\lambda^F\}) \\
&= \mathcal{I}(fr_\xi^{F-2} \cup \pi_1(th_\xi^{F-2}) \cup \{M_\lambda^{F-1}\} \cup \{M_\lambda^F\}) \\
&\qquad \vdots \qquad\qquad \vdots \\
&= \mathcal{I}(fr_\xi^0 \cup \pi_1(th_\xi^0) \cup \{M_\lambda^1\} \cup \cdots \cup \{M_\lambda^F\}) \\
&= \mathcal{I}(fr \cup \{n\} \cup \pi_1(th_\xi^0) \cup \{M_\lambda^1\} \cup \cdots \cup \{M_\lambda^F\}) \\
&= \mathcal{I}(fr \cup \{n\} \cup \pi_1(th_\xi^0) \cup \{\{M_\lambda^1\}_n^E\} \cup \cdots \cup \{\{M_\lambda^F\}_n^E\}) \\
&= \mathcal{I}(fr \cup \{n\} \cup \pi_1(th_\xi^0) \cup \pi_1(\lambda)) \\
&= \mathcal{I}(fr \cup \{M\} \cup \pi_1(th))
\end{aligned}$$

Similarly for $\mathcal{I}(fr' \cup \pi_2(th'))$. It now follows that $fr' = \mathcal{K}(fr \cup \{M\} \cup \pi_1(th)) = \mathcal{K}(fr \cup \{N\} \cup \pi_2(th))$, $\pi_1(th') = \mathcal{I}(fr \cup \{M\} \cup \pi_1(th)) \setminus \mathcal{N}$, and $\pi_2(th') = \mathcal{I}(fr \cup \{N\} \cup \pi_2(th)) \setminus \mathcal{N}$.

This concludes the proof. ■

Lemma 9
Let $\sigma_1 \sim_e'' \sigma_2$, $(fr, th) \stackrel{def}{=} \mathcal{F}_e(\sigma_1, \sigma_2)$, $\xi(fr, th, M, N) \neq \perp$, and $(fr', th') \stackrel{def}{=} \xi(fr, th, M, N)$ for some $M, N \in \mathcal{M}$. Then $\sigma_1[z \mapsto M] \sim_e'' \sigma_2[z \mapsto N]$ and $\mathcal{F}_e(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N]) = (fr', th')$, where $z \notin \mathrm{dom}(\sigma_1)$.

Proof: Let

$$\sigma_1'(x) \stackrel{def}{=} \begin{cases} \mathrm{core}(\sigma_1, \sigma_1(x)) & x \neq z \\ M & x = z \end{cases}$$

and

$$\sigma_2'(x) \stackrel{def}{=} \begin{cases} \mathrm{core}(\sigma_2, \sigma_2(x)) & x \neq z \\ N & x = z \end{cases}$$

Then $\mathrm{range}(\sigma_1') = fr \cup \pi_1(th) \cup \{M\}$ and $\mathrm{range}(\sigma_2') = fr \cup \pi_2(th) \cup \{N\}$. Furthermore, $\mathrm{core}(\sigma_1[z \mapsto M], \sigma_1[z \mapsto M](x)) = \mathrm{core}(\sigma_1', \sigma_1'(x))$ and $\mathrm{core}(\sigma_2[z \mapsto N], \sigma_2[z \mapsto N](x)) = \mathrm{core}(\sigma_2', \sigma_2'(x))$. By lemma 8 and the way the algorithm for computing ξ works (the frame is never reduced, and each pair from the theory and (M, N) keeps being a

pair and both messages in a pair are decrypted with the same key from the frame) we get $(\mathrm{core}(\sigma_1', \sigma_1'(x)), \mathrm{core}(\sigma_2', \sigma_2'(x))) \in th'$ or $\mathrm{core}(\sigma_1', \sigma_1'(x)) = \mathrm{core}(\sigma_2', \sigma_2'(x)) \in fr'$ and $\sigma_1'(x) = \{\mathrm{core}(\sigma_1', \sigma_1'(x))\}_{\tilde{k}}^E$ and $\sigma_2'(x) = \{\mathrm{core}(\sigma_2', \sigma_2'(x))\}_{\tilde{k}}^E$ for some $\tilde{k} \subseteq fr'$. Since $\sigma_1(x) = \{\sigma_1'(x)\}_{\tilde{k}'}^E$ and $\sigma_2(x) = \{\sigma_2'(x)\}_{\tilde{k}'}^E$ for some $\tilde{k}' \subseteq fr \subseteq fr'$ it follows from the fact that $(fr', th') \vdash o\tilde{k}$ that $\sigma_1[z \mapsto M] \sim_e'' \sigma_2[z \mapsto N]$ and clearly $\mathcal{F}_e(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N]) = (fr', th')$. ■

Finally, we are ready to prove completeness. By theorem 3 it is enough to show that strong late environment sensitive bisimilarity is complete with respect to fenced bisimilarity.

Theorem 9 (Completeness)
Let S be a fenced bisimulation. Then $R \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \sigma_P \sim_e'' \sigma_Q \wedge \exists (fr, th).((fr, th) \vdash P\ S\ Q \wedge \mathcal{F}_e(\sigma_P, \sigma_Q) = (fr, th))\}$ is a strong late environment sensitive bisimulation.

Proof: Assume $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. Then there exists (fr, th) such that $(fr, th) \vdash P\ S\ Q$ and $\mathcal{F}_e(\sigma_P, \sigma_Q) = (fr, th)$.

$P \stackrel{\tau}{\longrightarrow} P'$.
Since S is a fenced bisimulation there exists Q' such that $Q \stackrel{\tau}{\longrightarrow} Q'$ and $(fr, th) \vdash P'\ S\ Q'$. This implies that $(\sigma_P \rhd P', \sigma_Q \rhd Q') \in R$.

$P \stackrel{a(u)}{\longrightarrow} P'$ and $a \in \mathcal{A}(\sigma_P)$.
We have that $a \in fr$, and since S is a fenced bisimulation there exists Q' such that $Q \stackrel{a(u)}{\longrightarrow} Q'$ and, for all sets $\tilde{n}$, where $\tilde{n} \cap (\mathrm{fn}(P, Q) \cup fr \cup \mathrm{n}(th)) = \emptyset$, and for all $M, N \in \mathcal{M}$, if $(fr \cup \tilde{n}, th) \vdash M \leftrightarrow N$ then $(fr \cup \tilde{n}, th) \vdash P'\{M/u\}\ S\ Q'\{N/u\}$.
Assume $\zeta \in \Upsilon$, where $\mathrm{e}(\zeta\sigma_P) \neq \partial$ and $\mathrm{n}(\zeta) \cap \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) = \emptyset$. By lemma 4 we have $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \sim_e'' \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)]$, where $\tilde{z} \cap \mathrm{dom}(\sigma_P) = \emptyset$. By lemma 5 we get $\mathcal{F}_e(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)], \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)]) = (fr \cup \mathrm{n}(\zeta), th)$. Since $(fr \cup \mathrm{n}(\zeta), th) \vdash e(\zeta\sigma_P) \leftrightarrow e(\zeta\sigma_Q)$ follows from lemma 7 we deduce $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}) \in R$.

$P \stackrel{(\nu\ \tilde{m})\bar{a}M}{\longrightarrow} P'$, $a \in \mathcal{A}(\sigma_P)$, and $\tilde{m} \cap \mathrm{fn}(P, \sigma_P) = \emptyset$.
In this case we have $a \in fr$ and $\tilde{m} \cap (\mathrm{fn}(P) \cup \mathrm{n}(\pi_1(th)) \cup fr) = \emptyset$. Since S is a fenced bisimulation there exist $\tilde{n}$, N, and Q' such that $Q \stackrel{(\nu\ \tilde{n})\bar{a}N}{\longrightarrow} Q'$, where $\tilde{n} \cap (\mathrm{fn}(Q) \cup \mathrm{n}(\pi_2(th)) \cup fr) = \emptyset$, and $\xi((fr, th), M, N) \vdash P'\ S\ Q'$.
It is easily seen that $\tilde{n} \cap \mathrm{fn}(Q, \sigma_2) = \emptyset$. By lemma 9 we have $\sigma_P[z \mapsto M] \sim_e'' \sigma[z \mapsto N]$ and $\mathcal{F}_e(\sigma_P[z \mapsto M], \sigma_Q[z \mapsto N]) = \xi((fr, th), M, N)$. Then it follows that $(\sigma_P[z \mapsto M] \rhd P', \sigma_Q[z \mapsto N] \rhd Q') \in R$.

■

We have shown soundness and completeness of strong late environment sensitive bisimilarity with respect to framed bisimilarity.

Corollary 1 (Soundness and Completeness)
$\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ if and only if $\mathcal{F}_e(\sigma_P, \sigma_Q) \vdash P \sim_f Q$. ■

Note that if $(fr, th) \vdash P \sim_f Q$ then there always exist σ_P and σ_Q such that $\sigma_P \sim''_e \sigma_Q$ and $\mathcal{F}_e(\sigma_P, \sigma_Q) = (fr, th)$.

5.5 Introducing Pairs

In this section we describe how the results from the previous sections of this chapter can be proven when we allow expressions to contain pairs and projection and messages to contain pairs. First we need to extend the environment messages, Υ, to include pairs and projection.

$$\zeta ::= a \mid x \mid \{\zeta\}^E_\zeta \mid \{\zeta\}^D_\zeta \mid (\zeta, \zeta) \mid \pi_l(\zeta) \mid \pi_r(\zeta)$$

The analysis and synthesis of a set of messages are naturally extended to deal with pairs as follows (the irreducibles and the knowledge of a set of messages need not be changed).

Definition 27 (Analysis of a Set of Messages)
The analysis of a set $W \subseteq \mathcal{M}$, written $\mathcal{A}(W)$, is the smallest set satisfying

(i) $W \subseteq \mathcal{A}(W)$

(ii) if $k \in \mathcal{A}(W)$ and $\{M\}^E_k \in \mathcal{A}(W)$ then $M \in \mathcal{A}(W)$

(iii) if $(M_1, M_2) \in \mathcal{A}(W)$ then $M_1 \in \mathcal{A}(W)$ and $M_2 \in \mathcal{A}(W)$

■

Definition 28 (Synthesis of a Set of Messages)
The synthesis of a set $W \subseteq \mathcal{M}$, written $\mathcal{S}(W)$, is the smallest set satisfying

(i) $\mathcal{A}(W) \subseteq \mathcal{S}(W)$

(ii) if $k \in \mathcal{S}(W) \cap \mathcal{N}$ and $M \in \mathcal{S}(W)$ then $\{M\}^E_k \in \mathcal{S}(W)$

(iii) if $M_1 \in \mathcal{A}(W)$ and $M_2 \in \mathcal{A}(W)$ then $(M_1, M_2) \in \mathcal{A}(W)$

■

A message $M \in \mathcal{M}$ can have several cores, which are found at different positions inside M. A position p is a string in $\{l, r\}^*$.

Definition 29 (Core)
The core of $M \in \mathcal{M}$ with respect to the set of messages $W \subseteq \mathcal{M}$ and the position p is

defined as follows, $\ominus$ is a special symbol used to express that a valid core does not exist at the position p.

$$\text{core}(W,p,M) \stackrel{def}{=} \begin{cases} a & \text{if } M = a \text{ and } p = \epsilon \\ \{N\}_k^E & \text{if } M = \{N\}_k^E,\ p = \epsilon, \text{ and } k \notin \mathcal{K}(W) \\ \text{core}(W,p,N) & \text{if } M = \{N\}_k^E \text{ and } k \in \mathcal{K}(W) \\ \text{core}(W,p',M_1) & \text{if } M = (M_1,M_2) \text{ and } p = lp' \\ \text{core}(W,p',M_2) & \text{if } M = (M_1,M_2) \text{ and } p = rp' \\ \ominus & \text{otherwise} \end{cases}$$

■

We will now give a definition of equivalence of environments where messages can contain pairs.

Definition 30 (Equivalence of Environments, $\sim_e''$)
Let σ and σ' be environments and assume $\text{dom}(\sigma) = \text{dom}(\sigma') = \{x_i \mid i \in I\}$ for some set of indices I. For each $i \in I$ and $p \in \{l,r\}^*$ let $N_{(i,p)} \stackrel{def}{=} \text{core}(\sigma, p, \sigma(x_i))$ and $N'_{(i,p)} \stackrel{def}{=} \text{core}(\sigma', p, \sigma'(x_i))$. Let the predicate $(\sigma,\sigma') \vdash M \sim M'$ be defined as follows. $(\sigma,\sigma') \vdash M \sim M'$ if there exists $\tilde{k}$ such that $M = \{M_0\}_{\tilde{k}}^E$ and $M' = \{M'_0\}_{\tilde{k}}^E$ for some M_0 and M'_0 such that either $M_0 = N_{(i,p)}$ and $M'_0 = N'_{(i,p)}$ for some i and p or $M_0 = (M_1,M_2)$, $M'_0 = (M'_1,M'_2)$, $(\sigma,\sigma') \vdash M_1 \sim M'_1$ and $(\sigma,\sigma') \vdash M_2 \sim M'_2$. σ and σ' are equivalent, written $\sigma \sim_e'' \sigma'$, if for each $i \in I$ the following holds

(i) $(\sigma,\sigma') \vdash \sigma(x_i) \sim \sigma'(x_i)$,

(ii) for each $p,q \in \{l,r\}^*$ and $j \in I$, $N_{(i,p)} = N_{(j,q)}$ if and only if $N'_{(i,p)} = N'_{(j,q)}$, and

(iii) for each $p \in \{l,r\}^*$ and $N \in \mathcal{N}$, $N_{(i,p)} = N$ if and only if $N'_{(i,p)} = N$.

■

With the new definition of core we need a new definition of the function $\mathcal{F}_e$.

Definition 31 (The Function $\mathcal{F}_e$)
Let σ_1 and σ_2 be environments such that $\sigma_1 \sim_e'' \sigma_2$ and $\text{dom}(\sigma_1) = \text{dom}(\sigma_2) = \{x_i \mid i \in I\}$. Let $fr \stackrel{def}{=} \{\text{core}(\sigma_1,p,\sigma_1(x_i)) \mid i \in I \wedge p \in \{l,r\}^* \wedge \text{core}(\sigma_1,p,\sigma_1(x_i)) \in \mathcal{N}\}$ and $th \stackrel{def}{=} \{(\text{core}(\sigma_1,p,\sigma_1(x_i)), \text{core}(\sigma_2,p,\sigma_2(x_i))) \mid i \in I \wedge p \in \{l,r\}^* \wedge \text{core}(\sigma_1,p,\sigma_1(x_i)) \notin \mathcal{N} \wedge \text{core}(\sigma_1,p,\sigma_1(x_i)) \neq \ominus\}$. Then $\mathcal{F}_e(\sigma_1,\sigma_2) \stackrel{def}{=} (fr,th)$. ■

To prove theorems 8 and 9, when we allow messages to contain pairs, we only need to prove that lemmas 1 to 9 and theorem 7 hold when pairs are allowed. Boreale et al. have shown that this is the case for lemmas 1 and 2 for an equivalence on environments that contains $\sim_e''$. Theorem 7 and lemmas 4 and 5 are easily proven when pairs are allowed. Lemmas 3 and 8 are easily proven by adding a case for pairs in the induction step of the proofs and

lemma 7 is easily proven by adding cases for pairs and projection in the induction step of the proof. The proofs of lemmas 6 and 9 need to be changed when pairs are allowed. We will only change the proof of lemma 6 here as the proof of lemma 9 is changed in a similar way.

Lemma 10 (Lemma 6 with Pairs)
Let $\sigma_1 \sim''_e \sigma_2$ and $(fr, th) \stackrel{def}{=} \mathcal{F}_e(\sigma_1, \sigma_2)$. If $\sigma_1[z \mapsto M] \sim''_e \sigma_2[z \mapsto N]$, where $z \notin \mathrm{dom}(\sigma_1)$, then

(i) $(fr, th) \leq (fr', th')$, and

(ii) $(fr', th') \vdash M \leftrightarrow N$,

where $(fr', th') \stackrel{def}{=} \mathcal{F}_e(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N])$.

Proof:

(i) By theorem 7 we get $(fr', th') \vdash ok$. It is easily seen that $fr \subseteq fr'$, so by theorem 1 it is enough to show that $(fr', th') \vdash M' \leftrightarrow N'$ for each $(M', N') \in th$ to prove that $(fr, th) \leq (fr', th')$. Assume $(M', N') \in th$. There exists $p \in \{l, r\}^*$ and $x \in \mathrm{dom}(\sigma_1)$ such that $M' = \mathrm{core}(\sigma_1, p, \sigma_1(x))$ and $N' = \mathrm{core}(\sigma_2, p, \sigma_2(x))$. Since $\sigma_1[z \mapsto M] \sim''_e \sigma_2[z \mapsto N]$ we have $(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N]) \vdash \sigma_1[z \mapsto M](x) \sim \sigma_2[z \mapsto N](x)$. Let $(M_i, M'_i)_{i \in I}$ be the messages M_0 and M'_0 (see definition 30) used to prove $(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N]) \vdash \sigma_1[z \mapsto M](x) \sim \sigma_2[z \mapsto N](x)$. It is easily seen that $(fr', th') \vdash M_i \leftrightarrow M'_i$ for each $i \in I$. There must exist $i \in I$ and $\tilde{k} \subseteq fr'$ such $M' = \{M_i\}^E_{\tilde{k}}$ and $N' = \{M'_i\}^E_{\tilde{k}}$. This implies $(fr', th') \vdash M' \leftrightarrow N'$

(ii) This is easily seen from definition 30.

■

In the following chapter we will show that a new version of framed bisimilarity, called frameless framed bisimilarity, is sound and complete with respect to strong early environment sensitive bisimilarity.

6 Two Notions of Strong Early Environment Sensitive Bisimilarity

In this chapter we will show that a new slightly different version of framed bisimilarity, called frameless framed bisimilarity, is sound and complete with respect to strong early environment sensitive bisimilarity. The proof is very similar to the proof of soundness and completeness of strong late environment sensitive bisimilarity with respect to framed bisimilarity. We will not go through the details of the proof here but merely state the lemmas needed.

6.1 Frameless Framed Bisimilarity

In this section we present an early version of framed bisimulation called frameless framed bisimulation. The definition of frameless framed bisimulation is based on the notion of a theory. A frameless framed bisimulation relates two processes P and Q in the context of a theory. As in chapter 3 a theory is a finite set of pairs of messages. Intuitively, a theory contains pairs of messages coming from P and Q that cannot be distinguished by an observer. Two messages M and N are indistinguishable with respect to the theory th if $th \vdash M \leftrightsquigarrow N$ can be derived using the rules in table 6.1.

[Eq theory]	$\dfrac{(M,N) \in th}{th \vdash M \leftrightsquigarrow N}$
[Eq pair]	$\dfrac{th \vdash M \leftrightsquigarrow N \quad th \vdash M' \leftrightsquigarrow N'}{th \vdash (M,M') \leftrightsquigarrow (N,N')}$
[Eq encrypt]	$\dfrac{th \vdash M \leftrightsquigarrow N \quad th \vdash M' \leftrightsquigarrow N'}{th \vdash \{M\}^E_{M'} \leftrightsquigarrow \{N\}^E_{N'}}$

Table 6.1: The indistinguishability predicate.

In a frameless framed bisimulation we only consider theories that exhibit certain properties.

Definition 32 (Ok Theory)
The theory th is ok, written $th \vdash \surd$, if

(i) for all $(M,N) \in th$, $M, N \in \mathcal{N}$ or $M = \{M_1\}^E_{M_2}$ and $N = \{N_1\}^E_{N_2}$ for some messages M_1, M_2, N_1, and N_2.

(ii) for all $(M,N) \in th$

- if $M = \{M_1\}^E_{M_2}$ then there is no N' such that $th \vdash M_2 \leftrightsquigarrow N'$.
- if $N = \{N_1\}^E_{N_2}$ then there is no M' such that $th \vdash M' \leftrightsquigarrow N_2$.

(iii) for all $(M,N) \in th$ and $(M',N') \in th$, $M = M'$ if and only if $N = N'$.

■

The definition of frameless framed bisimulation requires that a theory can be extended.

Definition 33 (Extension of a Theory)
th' is an extension of th, written $th \sqsubseteq th'$, if for all M and N, $th \vdash M \leftrightsquigarrow N$ implies $th' \vdash M \leftrightsquigarrow N$. ■

We will need two functions to split a theory into two sets, one containing the pairs of names and one containing the other pairs.

Definition 34 (The Functions $\mathcal{O}_{fr}$ and $\mathcal{O}_{th}$)
Let th be a theory. Then $\mathcal{O}_{fr}(th) \stackrel{def}{=} \{(M,N) \in th \mid M \in \mathcal{N} \wedge N \in \mathcal{N}\}$ and $\mathcal{O}_{th}(th) \stackrel{def}{=} \{(M,N) \in th \mid M \notin \mathcal{N} \vee N \notin \mathcal{N}\}$. ■

The following theorem makes it easier to show whether or not one ok theory is an extension of another.

Theorem 10
Let $th' \vdash \surd$, then $th \sqsubseteq th'$ if and only if $\mathcal{O}_{fr}(th) \subseteq \mathcal{O}_{fr}(th')$ and $th' \vdash M \leftrightsquigarrow N$ for each pair $(M, N) \in \mathcal{O}_{th}(th)$. ■

A ***frameless framed process pair*** is a triple (th, P, Q). If R is a set of frameless framed process pairs and $(th, P, Q) \in R$ this is written $th \vdash P\ R\ Q$. A ***frameless framed relation*** is a set of frameless framed process pairs such that $th \vdash P\ R\ Q$ implies $th \vdash \surd$. A frameless framed relation R is ***symmetric*** if $th \vdash P\ R\ Q$ implies $\{(N, M) \mid (M, N) \in th\} \vdash Q\ R\ P$. For a set of names V we define $\mathcal{C}(V) \stackrel{def}{=} \{(a, a) \mid a \in V\}$. Now, we are ready to present the notion of ***frameless framed bisimulation***.

Definition 35 (Frameless Framed Bisimulation)
A symmetric frameless framed relation R is a frameless framed bisimulation if whenever $th \vdash P\ R\ Q$ it holds that

(i) if $P \xrightarrow{\tau} P'$ then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $th \vdash P'\ R\ Q'$,

(ii) if $P \xrightarrow{a(u)} P'$ and $a \in \pi_1(th)$ then $a \in \pi_2(th)$ and for all $\tilde{n}$ with $\tilde{n} \cap (\mathrm{fn}(P) \cup \mathrm{n}(\pi_1(th))) = \emptyset$ and all $M \in \mathcal{S}(\tilde{n} \cup \pi_1(th))$, there exist N and Q' such that $Q \xrightarrow{a(u)} Q'$, $\tilde{n} \cap (\mathrm{fn}(Q) \cup \mathrm{n}(\pi_2(th))) = \emptyset$, and $th \cup \mathcal{C}(\tilde{n}) \vdash M \leftrightsquigarrow N$, and it holds that $th \cup \mathcal{C}(\tilde{n}) \vdash P'\{M/u\}\ R\ Q'\{N/u\}$, and

(iii) if $P \xrightarrow{(\nu\ \tilde{m})\bar{a}M} P'$, $a \in \pi_1(th)$, and $\tilde{m} \cap (\mathrm{fn}(P) \cup \mathrm{n}(\pi_1(th))) = \emptyset$ then $a \in \pi_2(th)$ and there exist $\tilde{n}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{n})\bar{a}N} Q'$, $\tilde{n} \cap (\mathrm{fn}(Q) \cup \mathrm{n}(\pi_2(th))) = \emptyset$, and there exists th' such that $th \sqsubseteq th'$, $th' \vdash M \leftrightsquigarrow N$, and $th' \vdash P'\ R\ Q'$.

■

From the definition of frameless framed bisimulation we define the notion of ***frameless framed bisimilarity***.

Definition 36 (Frameless Framed Bisimilarity)
P and Q are frameless framed bisimilar with respect to the theory th, written $th \vdash P \sim_{ff} Q$, if there exists a frameless framed bisimulation R such that $th \vdash P\ R\ Q$. ■

6.2 Frameless Fenced Bisimilarity

To be able to use the proof technique used to prove soundness and completeness of strong late environment sensitive bisimilarity with respect to framed bisimilarity to prove soundness and completeness of frameless framed bisimilarity with respect to strong early environment sensitive bisimilarity we introduce a frameless version of fenced bisimulation. This frameless fenced bisimulation makes use of the Ξ-function presented in figure 6.1. $\Xi(th, M, N)$ evaluates to the smallest extension th' of th such that $th' \vdash \surd$ and $th' \vdash M \leftrightsquigarrow N$ (lemma 12 on page 42). If this is not possible $\Xi(th, M, N)$ evaluates to the invalid theory $\top$.

1 $\Xi(th, M, N)$
2 IF $(th \vdash M \leftrightsquigarrow N)$ THEN RETURN th
3 CASE (M, N) OF
4 $[M = m, N = n]$:
5 IF $\exists (O, O') \in th.(O = M \iff O' = N)$ THEN RETURN$(\top)$
6 $th_\Xi := th \cup \{(m, n)\}$
7 $\lambda := \emptyset$
8 FOR EACH $(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2}) \in th_\Xi$ DO
9 IF $\exists L.(th_\Xi \vdash M_2 \leftrightsquigarrow L \ \vee \ th_\Xi \vdash L \leftrightsquigarrow N_2)$ THEN
10 $th_\Xi := th_\Xi \setminus \{(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2})\}$
11 $\lambda := \lambda \cup \{(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2})\}$
12 FOR EACH $(\{M_1\}^E_{M_2}, \{N_1\}^E_{N_2}) \in \lambda$ DO
13 $th_\Xi := \Xi(\Xi(th_\Xi, M_2, N_2), M_1, N_1)$
14 $[M = \{M_1\}^E_{M_2}, N = \{N_1\}^E_{N_2}]$:
15 IF $(th \vdash M_2 \leftrightsquigarrow N_2)$ THEN $th_\Xi := \Xi(th, M_1, N_1)$
16 ELSE
17 IF $\exists (O, O') \in th.(O = M \iff O' = N)$ THEN RETURN$(\top)$
18 $th_\Xi := th \cup \{(M, N)\}$
19 $\lambda := \emptyset$
20 FOR EACH $(\{O_1\}^E_{O_2}, \{O'_1\}^E_{O'_2}) \in th_\Xi$ DO
21 IF $\exists L.(th_\Xi \vdash O_2 \leftrightsquigarrow L \ \vee \ th_\Xi \vdash L \leftrightsquigarrow O'_2)$ THEN
22 $th_\Xi := th_\Xi \setminus \{(\{O_1\}^E_{O_2}, \{O'_1\}^E_{O'_2})\}$
23 $\lambda := \lambda \cup \{(\{O_1\}^E_{O_2}, \{O'_1\}^E_{O'_2})\}$
24 FOR EACH $(\{O_1\}^E_{O_2}, \{O'_1\}^E_{O'_2}) \in \lambda$ DO
25 $th_\Xi := \Xi(\Xi(th_\Xi, O_2, O'_2), O_1, O'_1)$
26 $[M = (M_1, M_2), N = (N_1, N_2)]$:
27 $th_\Xi := \Xi(\Xi(th, M_2, N_2), M_1, N_1)$
28 $[otherwise]$:
29 RETURN $(\top)$
30 RETURN th_Ξ

Figure 6.1: Algorithm for computing $\Xi(th, M, N)$.

The notion of ***frameless fenced bisimulation*** is defined as follows.

Definition 37 (Frameless Fenced Bisimulation)
A symmetric frameless framed relation R is a frameless fenced bisimulation if whenever $th \vdash P\ R\ Q$ it holds that

(i) if $P \xrightarrow{\tau} P'$ then there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $th \vdash P'\ R\ Q'$,

(ii) if $P \xrightarrow{a(u)} P'$ and $a \in \pi_1(th)$ then $a \in \pi_2(th)$ and for all $\tilde{n}$ with $\tilde{n} \cap (\mathrm{fn}(P) \cup \mathrm{n}(\pi_1(th))) = \emptyset$ and all $M \in \mathcal{S}(\tilde{n} \cup \pi_1(th))$, there exist N and Q' such that $Q \xrightarrow{a(u)} Q'$, $\tilde{n} \cap (\mathrm{fn}(Q) \cup \mathrm{n}(\pi_2(th))) = \emptyset$, and $th \cup \mathcal{C}(\tilde{n}) \vdash M \leftrightsquigarrow N$, and it holds that $th \cup \mathcal{C}(\tilde{n}) \vdash P'\{M/u\}\ R\ Q'\{N/u\}$, and

(iii) if $P \xrightarrow{(\nu\ \tilde{m})\bar{a}M} P'$, $a \in \pi_1(th)$, and $\tilde{m} \cap (\mathrm{fn}(P) \cup \mathrm{n}(\pi_1(th))) = \emptyset$ then $a \in \pi_2(th)$ and there exist $\tilde{n}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{n})\bar{a}N} Q'$, $\tilde{n} \cap (\mathrm{fn}(Q) \cup \mathrm{n}(\pi_2(th))) = \emptyset$, and $\Xi(th, M, N) \vdash P'\ R\ Q'$.

■

From the definition of frameless fenced bisimulation we define the notion of ***frameless fenced bisimilarity***.

Definition 38 (Frameless Fenced Bisimilarity)
P and Q are frameless fenced bisimilar with respect to the theory th, written $th \vdash P \sim_{f\#} Q$, if there exists a frameless fenced bisimulation R such that $th \vdash P\ R\ Q$. ■

It can be proven that frameless framed bisimilarity coincides with frameless fenced bisimilarity. The proof of this is very similar to the proof of soundness and completeness of fenced bisimilarity with respect to framed bisimilarity given in [7]. We will not go through the details of the proof here but merely state the lemmas needed in the proof and the theorems themselves. To show soundness of frameless fenced bisimilarity with respect to frameless framed bisimilarity we need the following lemma.

Lemma 11
Let $th \vdash \surd$. If $\Xi(th, M, N) \neq \top$ then $th \sqsubseteq \Xi(th, M, N)$, $\Xi(th, M, N) \vdash \surd$, and $\Xi(th, M, N) \vdash M \leftrightsquigarrow N$. ■

Soundness of frameless fenced bisimilarity with respect to frameless framed bisimilarity is stated in the following theorem.

Theorem 11 (Soundness of Frameless Fenced Bisimilarity)
If $th \vdash P \sim_{f\#} Q$ then $th \vdash P \sim_{ff} Q$. ■

Two lemmas are needed to prove completeness of frameless fenced bisimilarity with respect to frameless framed bisimilarity. The first lemma states that the Ξ-function yields the smallest valid extension of a given theory with respect to a pair of messages.

Lemma 12
If $th \vdash \surd$ and there exists th' such that $th \sqsubseteq th'$, $th' \vdash \surd$, and $th' \vdash M \leftrightsquigarrow N$ then $\Xi(th, M, N) \neq \top$, $\Xi(th, M, N) \vdash \surd$, and $\Xi(th, M, N) \sqsubseteq th'$. ■

The second lemma states that when two processes are frameless framed bisimilar under an extension of a given theory they are also frameless fenced bisimilar under the smallest extension of this theory.

Lemma 13
If $th \vdash \surd$ and there exists th' such that $th \sqsubseteq th'$, $th' \vdash M \leftrightsquigarrow N$, and $th' \vdash P \sim_{ff} Q$ then $\Xi(th, M, N) \vdash P \sim_{f\#} Q$. ■

The completeness result is stated in the following theorem.

Theorem 12 (Completeness of Frameless Framed Bisimilarity)
If $th \vdash P \sim_{ff} Q$ then $th \vdash P \sim_{f\#} Q$. ■

Soundness and completeness of frameless fenced bisimilarity with respect to frameless framed bisimilarity is stated in the following corollary.

Corollary 2 (Coincidence of $\sim_{ff}$ and $\sim_{f\#}$)
$th \vdash P \sim_{ff} Q$ if and only if $th \vdash P \sim_{f\#} Q$. ■

6.3 Soundness and Completeness

In this section we will show that frameless framed bisimilarity is sound and complete with respect to strong early environment sensitive bisimilarity for an expression and message grammar without pairs and projection. We first define a function $\mathcal{F}'_e$ that takes two equivalent environments as input and returns a theory. Then it can be shown that if $th \vdash P \sim_{f\#} Q$, $\sigma_P \sim'_e \sigma_Q$, and $\mathcal{F}'_e(\sigma_P, \sigma_Q) = th$ then $\sigma_P \rhd P \sim_{EESB} \sigma_Q \rhd Q$, and if $\sigma_P \rhd P \sim_{EESB} \sigma_Q \rhd Q$ then $\mathcal{F}'_e(\sigma_P, \sigma_Q) \vdash P \sim_{f\#} Q$.

Definition 39 (The Function $\mathcal{F}'_e$)
Let σ_1 and σ_2 be two environments such that $\sigma_1 \sim'_e \sigma_2$ and $\mathrm{dom}(\sigma_1) = \mathrm{dom}(\sigma_2) = \{x_i \mid i \in I\}$. The function $\mathcal{F}'_e$ is defined as $\mathcal{F}'_e(\sigma_1, \sigma_2) \stackrel{def}{=} \{(\mathrm{core}(\sigma_1, \sigma_1(x_i)), \mathrm{core}(\sigma_2, \sigma_2(x_i))) \mid i \in I\}$.
■

From the definition of $\mathcal{F}'_e$ we define a function $\mathcal{F}_{EESB}$ that takes a strong early environment sensitive bisimulation as input and returns a set of frameless framed process pairs which will later turn out to be a frameless framed bisimulation.

Definition 40 (The Function $\mathcal{F}_{EESB}$)
Let R be a strong early environment sensitive bisimulation. Then $\mathcal{F}_{EESB}(R) \stackrel{def}{=} \{(th, P, Q) \mid \exists \sigma_1, \sigma_2.((\sigma_1 \rhd P, \sigma_2 \rhd Q) \in R \wedge \mathcal{F}'_e(\sigma_1, \sigma_2) = th)\}$. ■

The following theorem states that a theory returned from $\mathcal{F}'_e$ is ok. This implies that a relation returned by $\mathcal{F}_{EESB}$ is a frameless framed relation.

Theorem 13
Let $\sigma_1 \sim'_e \sigma_2$ and $th \stackrel{def}{=} \mathcal{F}'_e(\sigma_1, \sigma_2)$, then $th \vdash \surd$. ■

6.3.1 Soundness

To prove soundness of frameless framed bisimilarity with respect to strong early environment sensitive bisimilarity we make use of the following four lemmas.

Lemma 14
Let $\sigma_1 \sim'_e \sigma_2$ and $th \stackrel{def}{=} \mathcal{F}'_e(\sigma_1, \sigma_2)$. Also, let $\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap \mathrm{n}(\sigma_1, \sigma_2) = \emptyset$ and $e(\zeta\sigma_1) \neq \partial$, $M \stackrel{def}{=} e(\zeta\sigma_1)$, and $N \stackrel{def}{=} e(\zeta\sigma_2)$. Then $th \cup \mathcal{C}(\mathrm{n}(\zeta)) \vdash M \leftrightsquigarrow N$. ■

Lemma 15
Let $\sigma_1 \sim'_e \sigma_2$ and $th \stackrel{def}{=} \mathcal{F}'_e(\sigma_1, \sigma_2)$. Then $th \cup \mathcal{C}(\tilde{c}) = \mathcal{F}'_e(\sigma_1[\tilde{z} \mapsto \tilde{c}], \sigma_2[\tilde{z} \mapsto \tilde{c}])$, where $\tilde{z} \cap \mathrm{dom}(\sigma_1) = \emptyset$ and $\tilde{c} \cap \mathrm{fn}(\sigma_1, \sigma_2) = \emptyset$. ■

Lemma 16
Let $th \vdash \surd$, $\Xi(th, M, N) \neq \top$, and $th' \stackrel{def}{=} \Xi(th, M, N)$ then

$$\begin{aligned}
\pi_1(\mathcal{O}_{fr}(th')) &= \mathcal{K}(\pi_1(\mathcal{O}_{fr}(th)) \cup \pi_1(\mathcal{O}_{th}(th)) \cup \{M\}) \\
\pi_2(\mathcal{O}_{fr}(th')) &= \mathcal{K}(\pi_2(\mathcal{O}_{fr}(th)) \cup \pi_2(\mathcal{O}_{th}(th)) \cup \{N\}) \\
\pi_1(\mathcal{O}_{th}(th')) &= \mathcal{I}(\pi_1(\mathcal{O}_{fr}(th)) \cup \pi_1(\mathcal{O}_{th}(th)) \cup \{M\}) \setminus \mathcal{N} \\
\pi_2(\mathcal{O}_{th}(th')) &= \mathcal{I}(\pi_2(\mathcal{O}_{fr}(th)) \cup \pi_2(\mathcal{O}_{th}(th)) \cup \{N\}) \setminus \mathcal{N}
\end{aligned}$$

■

Lemma 17
Let $\sigma_1 \sim'_e \sigma_2$, $th \stackrel{def}{=} \mathcal{F}'_e(\sigma_1, \sigma_2)$, $\Xi(th, M, N) \neq \top$, and $th' \stackrel{def}{=} \Xi(th, M, N)$. Then $\sigma_1[z \mapsto M] \sim'_e \sigma_2[z \mapsto N]$ and $\mathcal{F}'_e(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N]) = th'$, where $z \notin \mathrm{dom}(\sigma_1)$. ■

By theorem 11 it is enough to show that frameless fenced bisimilarity is sound with respect to strong early environment sensitive bisimilarity.

Theorem 14 (Soundness)
Let S be a frameless fenced bisimulation. Then $R \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \sigma_P \sim'_e \sigma_Q \wedge \exists th.(th \vdash P\ S\ Q \wedge \mathcal{F}'_e(\sigma_P, \sigma_Q) = th)\}$ is a strong early environment sensitive bisimulation.

■

6.3.2 Completeness

To prove completeness of frameless framed bisimilarity with respect to strong early environment sensitive bisimilarity we need the following two lemmas.

Lemma 18
Let $\tilde{n} \cap \mathrm{fn}(P,\sigma) = \emptyset$ and $M \in \mathcal{S}(\tilde{n} \cup \mathcal{I}(\sigma))$. Then there exists $\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap \mathrm{fn}(P,\sigma) = \emptyset$ such that $e(\zeta\sigma) = M$.

Proof: The proof is by induction of the structure of M.

Basis:

Case $M = a \in \tilde{n}$.
Let $\zeta \stackrel{def}{=} a$ then $\mathrm{n}(\zeta) \cap \mathrm{fn}(P,\sigma) = \emptyset$ and $e(\zeta\sigma) = M$.

Case $M \in \mathcal{I}(\sigma)$.
by lemma 1 there exists $\zeta \in \Upsilon$ such that $\mathrm{n}(\zeta) = \emptyset$ and $e(\zeta\sigma) = M$.

Step:

Case $M = \{N\}^E_k \in W$, $k \in W \cap \mathcal{N}$, and $N \in W$, where $W \stackrel{def}{=} \mathcal{S}(\tilde{n} \cup \mathcal{I}(\sigma))$.
By induction there exist $\zeta_1, \zeta_2 \in \Upsilon$ such that $\mathrm{n}(\zeta_1) \cap \mathrm{fn}(P,\sigma) = \emptyset$, $e(\zeta_1\sigma) = k$, $\mathrm{n}(\zeta_2) \cap \mathrm{fn}(P,\sigma) = \emptyset$, and $e(\zeta_2\sigma) = N$. Let $\zeta \stackrel{def}{=} \{\zeta_2\}^E_{\zeta_1}$. Now $\mathrm{n}(\zeta) \cap \mathrm{fn}(P,\sigma) = \emptyset$ and $e(\zeta\sigma) = M$.

■

Lemma 19
Let $\sigma_1 \sim'_e \sigma_2$ and $th \stackrel{def}{=} \mathcal{F}'_e(\sigma_1,\sigma_2)$. If $\sigma_1[z \mapsto M] \sim'_e \sigma_2[z \mapsto N]$, where $z \notin \mathrm{dom}(\sigma_1)$, then

(*i*) $th \sqsubseteq th'$, and

(*ii*) $th' \vdash M \leftrightsquigarrow N$,

where $th' \stackrel{def}{=} \mathcal{F}'_e(\sigma_1[z \mapsto M], \sigma_2[z \mapsto N])$. ■

The following theorem states that a frameless framed relation returned from $\mathcal{F}_{EESB}$ is a frameless framed bisimulation.

Theorem 15 (Completeness)
Let R be a strong early environment sensitive bisimulation. Then $\mathcal{F}_{EESB}(R)$ is a frameless framed bisimulation. ■

We have shown soundness and completeness of frameless framed bisimilarity with respect to strong early environment sensitive bisimilarity.

Corollary 3 (Soundness and Completeness)
$\mathcal{F}'_e(\sigma_P, \sigma_Q) \vdash P \sim_{\mathit{ff}} Q$ if and only if $\sigma_P \rhd P \sim_{EESB} \sigma_Q \rhd Q$. ■

Note that if $th \vdash P \sim_{\mathit{ff}} Q$ then there always exist σ_P and σ_Q such that $\sigma_P \sim'_e \sigma_Q$ and $\mathcal{F}'_e(\sigma_P, \sigma_Q) = th$.

Soundness and completeness of frameless framed bisimilarity with respect to strong early environment sensitive bisimilarity can also be proven for an expression and message grammar with pairs and projection.

In the next chapter we present some modal logics and show that these can be used to characterize strong early and strong late environment sensitive bisimilarity.

7 Logical Characterizations of Environment Sensitive Bisimilarities

A common approach to reasoning about properties of security protocols has been to use logics. One of these is BAN-logic, which was introduced by Burrows et al. in [1]. In this chapter we present some logics for the Spi-calculus that make it possible to reason about properties of security protocols. We present three logics, $\mathcal{F}$, $\mathcal{EM}$, and $\mathcal{LM}$, for configurations. We show that strong early environment sensitive bisimilarity, $\sim''_{EESB}$ ($\sim_{EESB}$ based on the environment equivalence $\sim''_e$), can be characterized by $\mathcal{F}$ and $\mathcal{EM}$. We also show that strong late environment sensitive bisimilarity can be characterized by $\mathcal{LM}$. First we present the syntax and semantics of formulae in a logic Φ from which we shall construct the logics $\mathcal{F}$ and $\mathcal{EM}$. The syntax of formulae in $\mathcal{LM}$ is based on the syntax of formulae in Φ but $\mathcal{LM}$ is based on a different semantics. The syntax and semantics presented in this chapter is inspired by [12]. In this chapter we will consider an expression and message grammar without pairs and projection. We will continue to refer to the set of expressions and the set of messages as $\mathcal{L}$ and $\mathcal{M}$, respectively.

7.1 Syntax and Semantics of Formulae

We begin by giving the syntax of ***formulae***. Formulae, ranged over by ϕ, can contain ***formula messages***. The set of formula messages is denoted Ω and is ranged over by η. Formulae can be constructed using three kinds of connectives: normal formula connectives, ***negation*** and ***conjunction***, connectives to describe processes, ***silent action***, ***free input***, ***early input***, ***late input***, ***output***, and ***matching***, and connectives to describe environments. An environment is described by the number of environment variables in its domain, $\# = n$, whether or not messages of the environment can be completely decrypted with the keys $\tilde{k}$ from the knowledge of the environment, $x \mapsto \{a\}^E_{\tilde{k}}$ and $x \mapsto \{?\}^E_{\tilde{k}}$, respectively, and whether the cores of two messages of the environment are equal, $\mathrm{core}(x) = \mathrm{core}(z)$. Formula messages can consist of variables, environment variables, encryption, and decryption. Formulae and formula messages are given by the following grammars.

$$\begin{aligned}
\phi ::= {} & \neg\phi \mid \bigwedge_{i\in I} \phi_i \\
\mid {} & \langle\tau\rangle\phi \mid \langle a\zeta\rangle\phi \mid \langle a(u)\rangle^E\phi \mid \langle a(u)\rangle^L\phi \mid \langle\bar{a}\rangle\phi \mid [\eta = \eta]\phi \\
\mid {} & \# = n \mid x \mapsto \{a\}^E_{\tilde{k}} \mid x \mapsto \{?\}^E_{\tilde{k}} \mid \mathrm{core}(x) = \mathrm{core}(z) \\
\eta ::= {} & u \mid x \mid \{\eta\}^E_\eta \mid \{\eta\}^D_\eta
\end{aligned}$$

where I is a finite or infinite set of indices. In $\langle a(u)\rangle^E\phi$ and $\langle a(u)\rangle^L\phi$ u is bound in ϕ. The sets of ***free variables***, $\mathrm{fv}(\phi)$, and ***bound variables***, $\mathrm{bv}(\phi)$, of a formula are defined as expected. We will write $\phi\{\eta/u\}$ for the formula obtained be replacing every free occurrence of u in ϕ by η, renaming bound variables as necessary. We identify formulae up to renaming of bound variables. If the formulae ϕ_1 and ϕ_2 can be identified up to renaming of bound variables we write $\phi_1 \equiv \phi_2$. We use the shorthand notations $\phi_1 \vee \phi_2$ and tt for $\neg(\neg\phi_1 \wedge \neg\phi_2)$ and $\bigwedge_{i\in\emptyset}\phi_i$, respectively. The logic Φ consists of formulae without free variables, i.e. $\Phi = \{\phi \mid \mathrm{fv}(\phi) = \emptyset\}$.

We will use a function $T(\sigma, \zeta)$ that substitutes each name a in ζ to the environment variable x in σ that maps to a (T will only be used in a context where σ is bijective with respect to the names in ζ, i.e. $|\{x \in \mathrm{dom}(\sigma) \mid \sigma(x) = a\}| = 1$).

The following example illustrates how to express a security property in the proposed modal logic.

Example 4. We define a formula ϕ_a that can only be satisfied by a configuration $\sigma \rhd P$ if P never reveals the secret name a to the environment σ, i.e. a is not in the knowledge of σ and a is not in the knowledge of the environment of any derivatives of $\sigma \rhd P$. We define ϕ_a as follows.

$$\phi_a \stackrel{def}{=} \bigwedge_{i=0}^{\infty} [\alpha]^i \neg \left(\bigvee_{x\in\mathcal{Z}, \tilde{k}\subseteq\mathcal{N}} x \mapsto \{a\}^E_{\tilde{k}} \right)$$

where $[\alpha]\phi \stackrel{def}{=} [\tau]\phi \wedge \bigwedge_{a\in\mathcal{N},\zeta\in\Upsilon}[a\zeta]\phi \wedge \bigwedge_{a\in\mathcal{N}}[\bar{a}]\phi$. The configuration $\sigma \rhd P$ given by

$\sigma \stackrel{def}{=} \{c/x\}$ and $P \stackrel{def}{=} (\nu\ k)c(u).\bar{u}\{a\}^E_k.\mathbf{0}$ is an example of a configuration that satisfies ϕ_a. Likewise, the configuration $\{c_{AS}/x_1, c_{AB}/x_2, c_{SB}/x_3\} \rhd Sys(a)$ satisfies ϕ_a, where $Sys(a)$ is the protocol/process defined in example 1(given that $F(a)$ does not reveal a). ■

In addition to security properties classical process properties such as deadlock-freeness and liveness can also be expressed in the logic Φ.

In the example above we saw that the configuration $\sigma \rhd P$ satisfies the formula ϕ_a. We will now define this notion of satisfaction more precisely.

Definition 41 (The Satisfaction Relation)
The satisfaction relation between configurations and formulae of Φ is given by

$\sigma \rhd P \vDash \neg\phi$	if $\sigma \rhd P \nvDash \phi$
$\sigma \rhd P \vDash \bigwedge_{i\in I} \phi_i$	if $\sigma \rhd P \vDash \phi_i$ for all $i \in I$
$\sigma \rhd P \vDash \langle\tau\rangle\phi$	if there exists P' such that $\sigma \rhd P \xrightarrow[-]{\tau} \sigma \rhd P'$ and $\sigma \rhd P' \vDash \phi$
$\sigma \rhd P \vDash \langle a\zeta\rangle\phi$	if there exist $\tilde{b}, u, \sigma',$ and P' such that $\sigma \rhd P \xrightarrow[(\nu\ \tilde{b})\bar{a}\zeta]{a(u)} \sigma' \rhd P'$ and $\sigma' \rhd P' \vDash \phi$
$\sigma \rhd P \vDash \langle a(u)\rangle^E\phi$	if for all $\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap \mathrm{fn}(P,\sigma) = \emptyset$ and $e(\zeta\sigma) \neq \partial$ there exist $\tilde{b}, \sigma',$ and P' such that $\sigma \rhd P \xrightarrow[(\nu\ \tilde{b})\bar{a}\zeta]{a(u)} \sigma' \rhd P'$ and $\sigma' \rhd P' \vDash \phi\{T(\sigma',\zeta)/u\}$
$\sigma \rhd P \vDash \langle\bar{a}\rangle\phi$	if there exist $\tilde{b}, M, x, \sigma',$ and P' such that $\sigma \rhd P \xrightarrow[a(x)]{(\nu\ \tilde{b})\bar{a}M} \sigma' \rhd P'$ and $\sigma' \rhd P' \vDash \phi$
$\sigma \rhd P \vDash [\eta_1 = \eta_2]\phi$	if $e'([\eta_1 = \eta_2]\sigma) = tt$ implies $\sigma \rhd P \vDash \phi$
$\sigma \rhd P \vDash \# = n$	if $\lvert\mathrm{dom}(\sigma)\rvert = n$
$\sigma \rhd P \vDash x \mapsto \{a\}^E_{\tilde{k}}$	if $\sigma(x) = \{a\}^E_{\tilde{k}}$ and $\tilde{k} \subseteq \mathcal{K}(\sigma)$
$\sigma \rhd P \vDash x \mapsto \{?\}^E_{\tilde{k}}$	if $\sigma(x) = \{\mathrm{core}(\sigma,\sigma(x))\}^E_{\tilde{k}}, \mathrm{core}(\sigma,\sigma(x)) \notin \mathcal{N}$, and $\tilde{k} \subseteq \mathcal{K}(\sigma)$
$\sigma \rhd P \vDash \mathrm{core}(x) = \mathrm{core}(z)$	if $\mathrm{core}(\sigma,\sigma(x)) = \mathrm{core}(\sigma,\sigma(z))$

■

Note that the satisfaction relation is not defined for $\langle a(u)\rangle^L\phi$. We will later define another satisfaction relation that is defined for $\langle a(u)\rangle^L\phi$. We use the shorthand notation $\sigma \vDash \phi$ if $\sigma \rhd P \vDash \phi$ for all $P \in \mathcal{P}r$.

7.2 Characterization of $\sim''_{EESB}$

In this section we present the two logics $\mathcal{F}$ and $\mathcal{EM}$ and show that strong early environment sensitive bisimilarity can be characterized by them both. To prove this we will use a

technique similar to that used by Milner et al. in [12]. We will let Φ_0 denote the subset of formulae of Φ that can be generated using the rules of the grammar for formulae except the rules for $[\eta = \eta]\phi$, $\langle a\zeta\rangle\phi$, $\langle a(u)\rangle^E\phi$, and $\langle a(u)\rangle^L\phi$. $\mathcal{F}$ is Φ_0 extended with the rule for $\langle a\zeta\rangle\phi$ and $\mathcal{EM}$ is Φ_0 extended with the rules for $[\eta = \eta]\phi$ and $\langle a(u)\rangle^E\phi$. To prove that strong early environment sensitive bisimilarity can be characterized by the two logics $\mathcal{F}$ and $\mathcal{EM}$ we define a logical process equivalence for each of the two logics. For this we need the following definition.

Definition 42 (Characterization Relations)
Let Δ be a subset of Φ. Then $\Delta(\sigma \rhd P) \stackrel{def}{=} \{\phi \in \Delta \mid \sigma \rhd P \vDash \phi\}$ and the relation $=_\Delta$ is defined by $=_\Delta \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \Delta(\sigma_P \rhd P) = \Delta(\sigma_Q \rhd Q)\}$. ■

The following lemma will be used to prove that strong early environment sensitive bisimilarity can be characterized by $\mathcal{F}$ and $\mathcal{EM}$, respectively.

Lemma 20
Let σ be an environment. Then there exists a formula $\phi_\sigma \in \Phi_0$ such that $\sigma \vDash \phi_\sigma$ and if $\sigma' \rhd Q \vDash \phi_\sigma$ then $\sigma \sim''_e \sigma'$.

Proof: Assume $|\mathrm{dom}(\sigma)| = n$. Let $\phi_\sigma \stackrel{def}{=} \bigwedge_{i\in I} \phi_i$ be the least formula satisfying the following.

- $\# = n \equiv \phi_i$ for some $i \in I$,
- $x \mapsto \{a\}^E_k \equiv \phi_i$ for some $i \in I$ if $\mathrm{core}(\sigma, \sigma(x)) = a$ and $\sigma(x) = \{\mathrm{core}(\sigma, \sigma(x))\}^E_k$,
- $x \mapsto \{?\}^E_k \equiv \phi_i$ for some $i \in I$ if $\mathrm{core}(\sigma, \sigma(x)) \notin \mathcal{N}$ and $\sigma(x) = \{\mathrm{core}(\sigma, \sigma(x))\}^E_k$
- $\mathrm{core}(x) = \mathrm{core}(z) \equiv \phi_i$ for some $i \in I$ if $\mathrm{core}(\sigma, \sigma(x)) = \mathrm{core}(\sigma, \sigma(z))$, and
- $\neg(\mathrm{core}(x) = \mathrm{core}(z)) \equiv \phi_i$ for some $i \in I$ if $\mathrm{core}(\sigma, \sigma(x)) \neq \mathrm{core}(\sigma, \sigma(z))$.

By definition 22 it is easily seen that $\sigma \rhd P \vDash \phi_\sigma$ for all $P \in \mathcal{P}r$ and if $\sigma' \rhd Q \vDash \phi_\sigma$ then $\sigma \sim''_e \sigma'$. ■

Now, we are ready to prove that $=_\mathcal{F}$ and $\sim''_{EESB}$ coincide.

Theorem 16 (Coincidence of $=_\mathcal{F}$ and $\sim''_{EESB}$)
$\sigma_P \rhd P =_\mathcal{F} \sigma_Q \rhd Q$ if and only if $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$.

Proof: We will first prove that $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ implies $\sigma_P \rhd P =_\mathcal{F} \sigma_Q \rhd Q$. Assume $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ and $\sigma_P \rhd P \vDash \phi$. We must show that $\sigma_Q \rhd Q \vDash \phi$. The proof will be by structural induction on ϕ.

Basis:

Case $\phi \equiv tt$.
Trivial since every configuration satisfies tt.

Case $\phi \equiv \# = n$, $\phi \equiv x \mapsto \{a\}^E_{\tilde{k}}$, $\phi \equiv x \mapsto \{?\}^E_{\tilde{k}}$, and $\phi \equiv \mathrm{core}(x) = \mathrm{core}(z)$.
Trivial since $\sigma_P \sim''_e \sigma_Q$.

Step:

Case $\phi \equiv \neg\phi'$.
We have that $\sigma_P \rhd P \not\models \phi'$ and by induction we get $\sigma_Q \rhd Q \not\models \phi'$. Hence we deduce $\sigma_Q \rhd Q \models \phi$.

Case $\phi \equiv \bigwedge_{i\in I} \phi_i$ and $I \neq \emptyset$.
We have that $\sigma_P \rhd P \models \phi_i$ for all $i \in I$ and by induction we have that $\sigma_Q \rhd Q \models \phi_i$ for all $i \in I$. Hence $\sigma_Q \rhd Q \models \phi$.

Case $\phi \equiv \langle\tau\rangle\phi'$.
There exists P' such that $\sigma_P \rhd P \xrightarrow[-]{\tau} \sigma_P \rhd P'$ and $\sigma_P \rhd P' \models \phi'$. Since $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ there exists Q' such that $\sigma_Q \rhd Q \xrightarrow[-]{\tau} \sigma_Q \rhd Q'$ and $\sigma_P \rhd P' \sim''_{EESB} \sigma_Q \rhd Q'$. By induction we have that $\sigma_Q \rhd Q' \models \phi'$ and thus we get $\sigma_Q \rhd Q \models \phi$.

Case $\phi \equiv \langle a\zeta\rangle\phi'$.
We have that there exist $\tilde{c}$, u, σ'_P, and P' such that $\sigma_P \rhd P \xrightarrow[(\nu\ \tilde{c})\bar{a}\zeta]{a(u)} \sigma'_P \rhd P'$ and $\sigma'_P \rhd P' \models \phi'$. Since $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ there exist $\tilde{d}$, σ'_Q, and Q' such that $\sigma_Q \rhd Q \xrightarrow[(\nu\ \tilde{d})\bar{a}\zeta]{a(u)} \sigma'_Q \rhd Q'$ and $\sigma'_P \rhd P' \sim''_{EESB} \sigma'_Q \rhd Q'$. By induction we have that $\sigma'_Q \rhd Q' \models \phi'$ and thus we get $\sigma_Q \rhd Q \models \phi$.

Case $\phi \equiv \langle\bar{a}\rangle\phi'$.
There exist $\tilde{c}$, M, z, σ'_P, and P' such that $\sigma_P \rhd P \xrightarrow[a(z)]{(\nu\ \tilde{c})\bar{a}M} \sigma'_P \rhd P'$ and $\sigma'_P \rhd P' \models \phi'$. Since $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ there exist $\tilde{d}$, N, σ'_Q, and Q' such that $\sigma_Q \rhd Q \xrightarrow[a(z)]{(\nu\ \tilde{d})\bar{a}N} \sigma'_Q \rhd Q'$ and $\sigma'_P \rhd P' \sim''_{EESB} \sigma'_Q \rhd Q'$. By induction we have that $\sigma'_Q \rhd Q' \models \phi'$ and thus we get $\sigma_Q \rhd Q \models \phi$.

Finally, we prove that $\sigma_P \rhd P =_{\mathcal{F}} \sigma_Q \rhd Q$ implies $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$. We will do this by showing that S defined by

$$S \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \sigma_P \rhd P =_{\mathcal{F}} \sigma_Q \rhd Q\}$$

is a strong early environment sensitive bisimulation. Assume $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in S$. By lemma 20 it follows that $\sigma_P \sim''_e \sigma_Q$. Suppose $\sigma_P \rhd P \xrightarrow[-]{\tau} \sigma'_P \rhd P'$. Let $\{C_i\}_{i\in I}$ be

an enumeration of $\{\sigma'_Q \rhd Q' \mid \sigma_Q \rhd Q \xrightarrow[-]{\tau} \sigma'_Q \rhd Q'\}$ and assume $(\sigma'_P \rhd P', C_i) \notin S$ for all $i \in I$. For each $i \in I$ choose $\phi_i \in \mathcal{F}(\sigma'_P \rhd P') \setminus \mathcal{F}(C_i)$ (ϕ_i always exists since $\sigma_P \rhd P \not\models \phi$ implies $\sigma_P \rhd P \models \neg\phi$). Let $\phi \stackrel{def}{=} \langle\tau\rangle \bigwedge_{i\in I} \phi_i$ (note that here we use the fact that I can be infinite), then $\phi \in \mathcal{F}(\sigma_P \rhd P) \setminus \mathcal{F}(\sigma_Q \rhd Q)$. This is a contradiction since $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in S$. Therefore, there must exist $\sigma'_Q \rhd Q'$ such that $\sigma_Q \rhd Q \xrightarrow[-]{\tau} \sigma'_Q \rhd Q'$ and $(\sigma'_P \rhd P', \sigma'_Q \rhd Q') \in S$. The cases with $\sigma_P \rhd P \xrightarrow[(\nu\ b)\bar{a}\zeta]{a(u)} \sigma'_P \rhd P'$ and $\sigma_P \rhd P \xrightarrow[a(x)]{(\nu b)\bar{a}M} \sigma'_P \rhd P'$ are shown similarly. ■

And now, we prove that $=_{\mathcal{EM}}$ and $\sim''_{EESB}$ coincide.

Theorem 17 (Coincidence of $=_{\mathcal{EM}}$ and $\sim''_{EESB}$)
$\sigma_P \rhd P =_{\mathcal{EM}} \sigma_Q \rhd Q$ if and only if $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$.

Proof: We will first prove that $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ implies $\sigma_P \rhd P =_{\mathcal{EM}} \sigma_Q \rhd Q$. Assume $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ and $\sigma_P \rhd P \models \phi$. We must show that $\sigma_Q \rhd Q \models \phi$. The proof will be by structural induction on ϕ.

Basis: The same as in the basis case of the proof of theorem 16.

Step:

Case $\phi \equiv \langle a(u)\rangle^E \phi'$.
We have that for all $\zeta \in \Upsilon$, where $\mathrm{n}(\zeta) \cap \mathrm{fn}(P, \sigma_P) = \emptyset$ and $e(\zeta\sigma_P) \neq \partial$, there exist $\tilde{c}$, σ', and P' such that $\sigma_P \rhd P \xrightarrow[(\nu\ \tilde{c})\bar{a}\zeta]{a(u)} \sigma'_P \rhd P'$ and $\sigma'_P \rhd P' \models \phi'\{T(\sigma'_P, \zeta)/u\}$. Since $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$ there exist $\tilde{d}$, σ'_Q, and Q' such that $\sigma_Q \rhd Q \xrightarrow[(\nu\ \tilde{d})\bar{a}\zeta]{a(u)} \sigma'_Q \rhd Q'$ and $\sigma'_P \rhd P' \sim''_{EESB} \sigma'_Q \rhd Q'$. By induction and the fact that $T(\sigma'_Q, \zeta) = T(\sigma'_P, \zeta)$ we have that $\sigma'_Q \rhd Q' \models \phi'\{T(\sigma'_Q, \zeta)/u\}$ and hence $\sigma_Q \rhd Q \models \phi$.

Case $\phi \equiv [\eta_1 = \eta_2]\phi'$.
If $e'([\eta_1 = \eta_2]\sigma_P) = ff$ then $e'([\eta_1 = \eta_2]\sigma_Q) = ff$ by theorem 6 and the fact that $\sigma_P \sim''_e \sigma_Q$. If $e'([\eta_1 = \eta_2]\sigma_P) = tt$ we have $\sigma_P \rhd P \models \phi'$. By induction we get $\sigma_Q \rhd Q \models \phi'$. Since $\sigma_P \sim''_e \sigma_Q$ it follows by theorem 6 that $e'([\eta_1 = \eta_2]\sigma_Q) = tt$. Thus we have $\sigma_Q \rhd Q \models \phi$.

The remaining cases are proven in the same way as in the proof of theorem 16.

Finally, we prove that $\sigma_P \rhd P =_{\mathcal{EM}} \sigma_Q \rhd Q$ implies $\sigma_P \rhd P \sim''_{EESB} \sigma_Q \rhd Q$. This follows from theorem 16 and the fact that $\sigma_P \rhd P \models \langle a\zeta\rangle\phi$ if and only if $\sigma_P \rhd P \models \langle a(u)\rangle^E[u = T(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)], \zeta)]\phi$. ■

7.3 Characterization of $\sim_{ESB}$

In this section we present the logic $\mathcal{LM}$ and show that this can be used to characterize strong late environment sensitive bisimilarity. It turns out that with the definition of strong late environment sensitive bisimulation it is difficult to prove that a modal logic can be used to characterize strong late environment sensitive bisimilarity using the same technique as in the proofs of theorems 16 and 17. For this reason we define a new notion of strong late environment sensitive bisimulation called S-environment sensitive bisimulation, show that S-environment sensitive bisimilarity can be used to characterize strong late environment sensitive bisimilarity, and prove that $\mathcal{LM}$ can be used to characterize S-environment sensitive bisimilarity using the same technique as in the proofs of theorems 16 and 17.

7.3.1 S-Environment Sensitive Bisimulation

The notion of ***S-environment sensitive bisimulation*** is defined as follows.

Definition 43 (S-Environment Sensitive Bisimulation)
Let $S \subseteq \mathcal{N}$. A symmetric relation $R \subseteq \Gamma \times \Gamma$ is an S-environment sensitive bisimulation if $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$ implies $\sigma_P \sim''_e \sigma_Q$ and if $P \xrightarrow{\alpha} P'$ then

(i) if $\alpha = \tau$ then there exists Q' such that $Q \xrightarrow{\alpha} Q'$ and $(\sigma_P \rhd P', \sigma_Q \rhd Q') \in R$.

(ii) if $\alpha = a(u)$ and $a \in \mathcal{A}(\sigma_P)$ then there exists Q' such that $Q \xrightarrow{a(u)} Q'$ and for all $\zeta \in \Upsilon$, where $e(\zeta\sigma_P) \neq \partial$ and $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$, $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}) \in R$, where $\tilde{z} \cap \mathrm{dom}(\sigma_P) = \emptyset$.

(iii) if $\alpha = (\nu\ \tilde{c})\bar{a}M$, $a \in \mathcal{A}(\sigma_P)$, $\tilde{c} \subseteq S$, and $\tilde{c} \cap \mathrm{fn}(P, \sigma_P) = \emptyset$ then there exist $\tilde{d}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{d})\bar{a}N} Q'$, where $\tilde{d} \subseteq S$, $\tilde{d} \cap \mathrm{fn}(Q, \sigma_Q) = \emptyset$, and $(\sigma_P[z \mapsto M] \rhd P', \sigma_Q[z \mapsto N] \rhd Q') \in R$, where $z \notin \mathrm{dom}(\sigma_P)$.

■

From the definition of S-environment sensitive bisimulation we define the notion of ***S-environment sensitive bisimilarity***.

Definition 44 (S-Environment Sensitive Bisimilarity)
The configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ are S-environment sensitive bisimilar, written $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$, if there exists an S-environment sensitive bisimulation R such that $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. ■

The following example illustrates that in general $\sim^S_{ESB}$ and $\sim_{ESB}$ are not sound with respect to each other.

Example 5. To see that $\sim_{ESB}^{S}$ is not sound with respect to $\sim_{ESB}$ for every S consider the processes $P \stackrel{def}{=} (\nu\ n)\bar{a}n.\mathbf{0}$ and $Q \stackrel{def}{=} \mathbf{0}$ and the environment $\sigma \stackrel{def}{=} \{a/x\}$. If $S \stackrel{def}{=} \emptyset$ we have $\sigma \rhd P \sim_{ESB}^{S} \sigma \rhd Q$ but not $\sigma \rhd P \sim_{ESB} \sigma \rhd Q$.

To see that $\sim_{ESB}$ is not sound with respect to $\sim_{ESB}^{S}$ for every S consider the processes $P \stackrel{def}{=} (\nu\ k)(\nu\ m)\bar{a}\{m\}_k^E.\mathbf{0}$ and $Q \stackrel{def}{=} (\nu\ k)\bar{a}\{k\}_k^E.\mathbf{0}$ and the environment $\sigma \stackrel{def}{=} \{a/x\}$. We have $\sigma \rhd P \sim_{ESB} \sigma \rhd Q$ but if $S \stackrel{def}{=} \{k\}$ we do not have $\sigma \rhd P \sim_{ESB}^{S} \sigma \rhd Q$. ■

In the following we will show that if two configurations are strong late environment sensitive bisimilar then they are also S-environment sensitive bisimilar for some infinite set S containing the free names of the two configurations. To show this we need the following three lemmas.

Lemma 21
If $P \xrightarrow{\alpha} P'$ then

- if $\alpha = \tau$ then $\mathrm{fn}(P') \subseteq \mathrm{fn}(P)$.
- if $\alpha = a(u)$ then $\mathrm{fn}(P') \cup \{a\} \subseteq \mathrm{fn}(P)$.
- if $\alpha = (\nu\ \tilde{c})\bar{a}M$ then $\mathrm{fn}(P') \cup \{a\} \cup \mathrm{n}(M) \subseteq \mathrm{fn}(P) \cup \tilde{c}$.

Proof: This is easily shown using transition induction. ■

Lemma 22
Let $\sigma_{\mathcal{N}}$ be an injective name substitution defined as $\sigma_{\mathcal{N}} \stackrel{def}{=} \{\tilde{m}/\tilde{n}, \tilde{n}/\tilde{m}\}$. If $P \xrightarrow{\alpha} P'$ then $P\sigma_{\mathcal{N}} \xrightarrow{\alpha\sigma_{\mathcal{N}}} P'\sigma_{\mathcal{N}}$.

Proof: This is easily shown using transition induction. ■

Lemma 23
Let $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ and let $\sigma_{\mathcal{N}}$ be the injective name substitution defined by $\sigma_{\mathcal{N}} \stackrel{def}{=} \{\tilde{m}/\tilde{n}, \tilde{n}/\tilde{m}\}$. Then $(\sigma_P \rhd P)\sigma_{\mathcal{N}} \sim_{ESB} (\sigma_Q \rhd Q)\sigma_{\mathcal{N}}$.

Proof: This is proven using lemma 22. ■

Theorem 18
Let $S \subseteq \mathcal{N}$ be an infinite set. If $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ and $\mathrm{fn}(P, Q, \sigma_P, \sigma_Q) \subseteq S$, then $\sigma_P \rhd P \sim_{ESB}^{S} \sigma_Q \rhd Q$.

Proof: We will show that the relation R defined by

$$R \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q \wedge \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) \subseteq S \cup \mathcal{K}(\sigma_P)\}$$

is an S-environment sensitive bisimulation. Assume $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. Since $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ we have that $\sigma_P \sim_e'' \sigma_Q$.

$P \xrightarrow{\tau} P'$.

Since $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ there exists Q' such that $Q \xrightarrow{\tau} Q'$ and $\sigma_P \rhd P' \sim_{ESB} \sigma_Q \rhd Q'$. By lemma 21 we have that $\mathrm{fn}(P', Q', \sigma_P, \sigma_Q) \subseteq S$ and it follows that $(\sigma_P \rhd P', \sigma_Q \rhd Q') \in R$.

$P \xrightarrow{a(u)} P'$ and $a \in \mathcal{A}(\sigma_P)$.

Since $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ there exists Q' such that $Q \xrightarrow{a(u)} Q'$ and for all $\zeta \in \Upsilon$, where $e(\zeta\sigma_P) \neq \partial$ and $\mathrm{n}(\zeta) \cap \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) = \emptyset$, $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\} \sim_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}$. Assume $\zeta' \in \Upsilon$, $\mathrm{n}(\zeta') \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$, and $e(\zeta'\sigma_P) \neq \partial$. Then we have that $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd P'\{e(\zeta'\sigma_P)/u\} \sim_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd Q'\{e(\zeta'\sigma_Q)/u\}$ and by lemma 21 we get $\mathrm{fn}(P'\{e(\zeta'\sigma_P)/u\}, Q'\{e(\zeta'\sigma_Q)/u\}, \sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta')], \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta')]) \subseteq S \cup \mathcal{K}(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta')])$. This implies that $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd P'\{e(\zeta'\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd Q'\{e(\zeta'\sigma_Q)/u\}) \in R$.

$P \xrightarrow{(\nu\ \tilde{c})\bar{a}M} P'$, $a \in \mathcal{A}(\sigma_P)$, $\tilde{c} \subseteq S$, and $\tilde{c} \cap \mathrm{fn}(P, \sigma_P) = \emptyset$.

Since $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ there exist $\tilde{d}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{d})\bar{a}N} Q'$, where $\tilde{d} \cap \mathrm{fn}(Q, \sigma_Q) = \emptyset$, and $\sigma_P[z \mapsto M] \rhd P' \sim_{ESB} \sigma_Q[z \mapsto N] \rhd Q'$. If $\tilde{d} \subseteq S$ then by lemma 21 we have $\mathrm{fn}(P', Q', \sigma_P[z \mapsto M], \sigma_Q[z \mapsto N]) \subseteq S$ and it follows that $(\sigma_P[\tilde{z} \mapsto M] \rhd P', \sigma_Q[\tilde{z} \mapsto N] \rhd Q') \in R$. If $\tilde{d} \setminus S \neq \emptyset$ then let $\tilde{n} \stackrel{def}{=} \tilde{d} \setminus S$. There exists a tuple $\tilde{m}$ of distinct names such that $\tilde{m} \cap (\mathrm{fn}(P, Q, \sigma_P, \sigma_Q) \cup \tilde{c}) = \emptyset$, $\tilde{m} \subseteq S$, and $|\tilde{m}| = |\tilde{n}|$. Let $\sigma_{\mathcal{N}}$ be the name substitution defined by $\sigma_{\mathcal{N}} \stackrel{def}{=} \{\tilde{m}/\tilde{n}, \tilde{n}/\tilde{m}\}$. Since $\sigma_P[z \mapsto M] \rhd P' \sim_{ESB} \sigma_Q[z \mapsto N] \rhd Q'$ we get $(\sigma_P[z \mapsto M] \rhd P')\sigma_{\mathcal{N}} \sim_{ESB} (\sigma_Q[z \mapsto N] \rhd Q')\sigma_{\mathcal{N}}$ by lemma 23. It now follows that $\sigma_P[z \mapsto M] \rhd P' \sim_{ESB} \sigma_Q[z \mapsto N\sigma_{\mathcal{N}}] \rhd Q'\sigma_{\mathcal{N}}$. By lemma 22 we have $Q \xrightarrow{((\nu\ \tilde{d})\bar{a}N)\sigma_{\mathcal{N}}} Q'\sigma_{\mathcal{N}}$ and it can be seen that $\tilde{d}\sigma_{\mathcal{N}} \subseteq S$ and $\tilde{d}\sigma_{\mathcal{N}} \cap \mathrm{fn}(Q, \sigma_Q) = \emptyset$. By lemma 21 we get $\mathrm{fn}(P', Q'\sigma_{\mathcal{N}}, \sigma_P[z \mapsto M], \sigma_Q[z \mapsto N\sigma_{\mathcal{N}}]) \subseteq S$ and it follows that $(\sigma_P[z \mapsto M] \rhd P', \sigma_Q[z \mapsto N\sigma_{\mathcal{N}}] \rhd Q'\sigma_{\mathcal{N}}) \in R$. ■

Now, we will show that if two configurations are S-environment sensitive bisimilar for some infinite set $S \subseteq \mathcal{N}$ ($\mathcal{N} \setminus S$ also infinite) containing the free names of the two configurations then they are also strong late environment sensitive bisimilar. To prove this we need the following two lemmas.

Lemma 24
If $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$ and $V \subseteq \mathcal{K}(\sigma_P)$ then $\sigma_P \rhd P \sim^{S \cup V}_{ESB} \sigma_Q \rhd Q$.

Proof: This can be seen from the definition of S-environment sensitive bisimulation. ■

Lemma 25
Let $S \subseteq \mathcal{N}$, $\tilde{m} \cap S = \emptyset$, $\tilde{n} \subseteq S$, and $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$. Let $\sigma_{\mathcal{N}}$ be a name substitution defined as $\sigma_{\mathcal{N}} \stackrel{def}{=} \{\tilde{m}/\tilde{n}, \tilde{n}/\tilde{m}\}$. Then $(\sigma_P \rhd P)\sigma_{\mathcal{N}} \sim^{(S \setminus \tilde{n}) \cup \tilde{m}}_{ESB} (\sigma_Q \rhd Q)\sigma_{\mathcal{N}}$.

Proof: This is proven using lemma 22. ■

Theorem 19
Let $S \subseteq \mathcal{N}$ and $\sigma_P \rhd P, \sigma_Q \rhd Q \in \Gamma$ such that $\mathrm{fn}(P,Q,\sigma_P,\sigma_Q) \subseteq S$, $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$, and S and $\mathcal{N} \setminus S$ are infinite. Then $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$.

Proof: We will show that the relation R defined by

$$R \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \exists S \subseteq \mathcal{N}.(\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q \wedge \mathrm{fn}(P,Q,\sigma_P,\sigma_Q) \subseteq S \wedge |S| = \infty \wedge |\mathcal{N} \setminus S| = \infty)\}$$

is a strong late environment sensitive bisimulation. Assume $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. Then there exists $S \subseteq \mathcal{N}$ such that $\mathrm{fn}(P,Q,\sigma_P,\sigma_Q) \subseteq S$, $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$, and S and $\mathcal{N} \setminus S$ are infinite. Since $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$ we get $\sigma_P \sim''_e \sigma_Q$.

$P \stackrel{\tau}{\longrightarrow} P'$.
There exists Q' such that $Q \stackrel{\tau}{\longrightarrow} Q'$ and $\sigma_P \rhd P' \sim^S_{ESB} \sigma_Q \rhd Q'$. By lemma 21 we have $\mathrm{fn}(P',Q',\sigma_P,\sigma_Q) \subseteq S$ and therefore $(\sigma_P \rhd P', \sigma_Q \rhd Q') \in R$.

$P \stackrel{a(u)}{\longrightarrow} P'$ and $a \in \mathcal{A}(\sigma_P)$.
There exists Q' such that $Q \stackrel{a(u)}{\longrightarrow} Q'$ and for all $\zeta' \in \Upsilon$ with $e(\zeta'\sigma_P) \neq \partial$ and $\mathrm{n}(\zeta') \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$ it holds that $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd P'\{e(\zeta'\sigma_P)/u\} \sim^S_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd Q'\{e(\zeta'\sigma_Q)/u\}$.
Now, let $\zeta \in \Upsilon$ such that $e(\zeta\sigma_P) \neq \partial$ and $\mathrm{n}(\zeta) \cap \mathrm{fn}(P,Q,\sigma_P,\sigma_Q) = \emptyset$. If $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$ then we know that $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\} \sim^S_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}$. By lemma 24 we get $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\} \sim^{S \cup \mathrm{n}(\zeta)}_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}$. This implies $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}) \in R$ since we have $\mathrm{fn}(P'\{e(\zeta\sigma_P)/u\}, Q'\{e(\zeta\sigma_Q)/u\}, \sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)], \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)]) \subseteq S \cup \mathrm{n}(\zeta)$ by lemma 21.
If $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_P)) \neq \emptyset$ then let $\tilde{n} \stackrel{def}{=} \mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_P))$. There exist $\zeta' \in \Upsilon$ and $\tilde{m} \subseteq \mathcal{N}$ such that $\mathrm{n}(\zeta') \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$, $\mathrm{n}(\zeta) \setminus \tilde{n} \subseteq \mathrm{n}(\zeta')$, and $\zeta = \zeta'\sigma_{\mathcal{N}}$, where $\sigma_{\mathcal{N}}$ is a name substitution defined as $\sigma_{\mathcal{N}} \stackrel{def}{=} \{\tilde{m}/\tilde{n}, \tilde{n}/\tilde{m}\}$. We have $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd P'\{e(\zeta'\sigma_P)/u\} \sim^S_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd Q'\{e(\zeta'\sigma_Q)/u\}$, and by lemma 25 we get $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd P'\{e(\zeta'\sigma_P)/u\})\sigma_{\mathcal{N}} \sim^{(S\setminus\tilde{n})\cup\tilde{m}}_{ESB} (\sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta')] \rhd Q'\{e(\zeta'\sigma_Q)/u\})\sigma_{\mathcal{N}}$. Since $(\tilde{n} \cup \tilde{m}) \cap \mathrm{fn}(P,Q,\sigma_P,\sigma_Q) = \emptyset$ we deduce $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\} \sim^{(S\setminus\tilde{n})\cup\tilde{m}}_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}$. By lemma 24 we get $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\} \sim^{(S\setminus\tilde{n})\cup\tilde{m}\cup\mathrm{n}(\zeta)}_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}$. Since $\mathrm{fn}(P'\{e(\zeta\sigma_P)/u\}, Q'\{e(\zeta\sigma_Q)/u\}, \sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)], \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)]) \subseteq (S\setminus\tilde{n})\cup\tilde{m}\cup\mathrm{n}(\zeta)$ follows by lemma 21 we conclude that $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\} \in R$.

$P \stackrel{(\nu\ \tilde{c})\bar{a}M}{\longrightarrow} P'$, $a \in \mathcal{A}(\sigma_P)$, and $\tilde{c} \cap \mathrm{fn}(P,\sigma_P) = \emptyset$.
If $\tilde{c} \subseteq S$ then there exist $\tilde{d}$, N, and Q' such that $Q \stackrel{(\nu\ \tilde{d})\bar{a}N}{\longrightarrow} Q'$, $\tilde{d} \subseteq S$, $\tilde{d} \cap \mathrm{fn}(Q,\sigma_Q) = \emptyset$, and $\sigma_P[z \mapsto M] \rhd P' \sim^S_{ESB} \sigma_Q[z \mapsto N] \rhd Q'$. We deduce $(\sigma_P[z \mapsto M] \rhd P', \sigma_Q[z \mapsto N] \rhd Q') \in R$ since $\mathrm{fn}(P',Q',\sigma_P[z \mapsto M], \sigma_Q[z \mapsto N]) \subseteq S$ by lemma 21 and the fact

that $\tilde{c} \cup \tilde{d} \subseteq S$.
If $\tilde{c} \setminus S \neq \emptyset$ then let $\tilde{m} \stackrel{def}{=} \tilde{c} \setminus S$. Let $\tilde{n}$ be a set of names such that $\tilde{n} \subseteq S$, $\tilde{n} \cap (\mathrm{fn}(P, Q, \sigma_P, \sigma_Q) \cup \tilde{c}) = \emptyset$, and $|\tilde{n}| = |\tilde{m}|$. Let $\sigma_{\mathcal{N}}$ be the name substitution given by $\sigma_{\mathcal{N}} \stackrel{def}{=} \{\tilde{m}/\tilde{n}, \tilde{n}/\tilde{m}\}$. By lemma 25 we have $(\sigma_P \rhd P)\sigma_{\mathcal{N}} \sim_{ESB}^{(S\setminus\tilde{n})\cup\tilde{m}} (\sigma_Q \rhd Q)\sigma_{\mathcal{N}}$. Since $(\tilde{n} \cup \tilde{m}) \cap \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) = \emptyset$ we get $\sigma_P \rhd P \sim_{ESB}^{(S\setminus\tilde{n})\cup\tilde{m}} \sigma_Q \rhd Q$. By the fact that $\tilde{c} \subseteq (S \setminus \tilde{n}) \cup \tilde{m}$ there exist $\tilde{d}$, N, and Q' such that $Q \stackrel{(\nu\ \tilde{d})\bar{a}N}{\longrightarrow} Q'$, $\tilde{d} \subseteq (S \setminus \tilde{n}) \cup \tilde{m}$, $\tilde{d} \cap \mathrm{fn}(Q, \sigma_Q) = \emptyset$, and $\sigma_P[z \mapsto M] \rhd P' \sim_{ESB}^{(S\setminus\tilde{n})\cup\tilde{m}} \sigma_Q[z \mapsto N] \rhd Q'$. By lemma 21 we get $\mathrm{fn}(P', Q', \sigma_P[z \mapsto M], \sigma_Q[z \mapsto N]) \subseteq (S \setminus \tilde{n}) \cup \tilde{m}$. Therefore, we conclude $(\sigma_P[z \mapsto M] \rhd P', \sigma_Q[z \mapsto N] \rhd Q') \in R$.

■

From theorems 18 and 19 we can establish that strong late environment sensitive bisimilarity is an equivalence relation.

Corollary 4
Strong late environment sensitive bisimilarity is an equivalence relation.

Proof: We will only prove that strong late environment sensitive bisimilarity is transitive since it is clearly reflexive and symmetric. Assume $\sigma_P \rhd P \sim_{ESB} \sigma_R \rhd R$ and $\sigma_R \rhd R \sim_{ESB} \sigma_Q \rhd Q$. Let $S \subseteq \mathcal{N}$ be an infinite set such that $\mathrm{fn}(P, Q, R, \sigma_P, \sigma_Q, \sigma_R) \subseteq S$ and $\mathcal{N} \setminus S$ is infinite. By theorem 18 we have $\sigma_P \rhd P \sim_{ESB}^{S} \sigma_R \rhd R$ and $\sigma_R \rhd R \sim_{ESB}^{S} \sigma_Q \rhd Q$. Since S-environment sensitive bisimilarity is transitive we have that $\sigma_P \rhd P \sim_{ESB}^{S} \sigma_Q \rhd Q$, and by theorem 19 we get $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$. ■

7.3.2 Characterization of $\sim_{ESB}^{S}$ and $\sim_{ESB}$

We will characterize $\sim_{ESB}^{S}$ and $\sim_{ESB}$ by the logic $\mathcal{LM}$ which is defined as Φ_0 extended with the rules for $[\eta = \eta]\phi$ and $\langle a(u)\rangle^L\phi$. We define a new satisfaction relation between configurations and formulae of $\mathcal{LM}$.

Definition 45 (The S-Satisfaction Relation)
The S-satisfaction relation between configurations and formulae of $\mathcal{LM}$ is given by

$\sigma \rhd P \models_S \neg\phi$	if $\sigma \rhd P \not\models_S \phi$
$\sigma \rhd P \models_S \bigwedge_{i\in I} \phi_i$	if $\sigma \rhd P \models_S \phi_i$ for all $i \in I$
$\sigma \rhd P \models_S \langle\tau\rangle\phi$	if there exists P' such that $P \xrightarrow{\tau} P'$ and $\sigma \rhd P' \models_S \phi$
$\sigma \rhd P \models_S \langle a(u)\rangle^L\phi$	if $a \in \mathcal{A}(\sigma)$ and there exists P' such that $P \xrightarrow{a(u)} P'$ and for all $\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma)) = \emptyset$ and $e(\zeta\sigma) \neq \partial$, $\sigma[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma)/u\} \models_S \phi\{T(\sigma[\tilde{z} \mapsto \mathrm{n}(\zeta)], \zeta)/u\}$
$\sigma \rhd P \models_S \langle\bar{a}\rangle\phi$	if $a \in \mathcal{A}(\sigma)$ and there exist $\tilde{b}, M, x,$ and P' such that $x \notin \mathrm{dom}(\sigma), \tilde{b} \cap \mathrm{fn}(P, \sigma) = \emptyset, \tilde{b} \subseteq S, P \xrightarrow{(\nu\ \tilde{b})\bar{a}M} P',$ and $\sigma[x \mapsto M] \rhd P' \models_S \phi$
$\sigma \rhd P \models_S [\eta_1 = \eta_2]\phi$	if $e'([\eta_1 = \eta_2]\sigma) = tt$ implies $\sigma \rhd P \models_S \phi$
$\sigma \rhd P \models_S \# = n$	if $\lvert\mathrm{dom}(\sigma)\rvert = n$
$\sigma \rhd P \models_S x \mapsto \{a\}^E_{\tilde{k}}$	if $\sigma(x) = \{a\}^E_{\tilde{k}}$ and $\tilde{k} \subseteq \mathcal{K}(\sigma)$
$\sigma \rhd P \models_S x \mapsto \{?\}^E_{\tilde{k}}$	if $\sigma(x) = \{\mathrm{core}(\sigma, \sigma(x))\}^E_{\tilde{k}}, \mathrm{core}(\sigma, \sigma(x)) \notin \mathcal{N}$, and $\tilde{k} \subseteq \mathcal{K}(\sigma)$
$\sigma \rhd P \models_S \mathrm{core}(x) = \mathrm{core}(z)$	if $\mathrm{core}(\sigma, \sigma(x)) = \mathrm{core}(\sigma, \sigma(z))$

■

To prove that S-environment sensitive bisimilarity can be characterized by the logic $\mathcal{LM}$ we define a logical process equivalence for this logic. For this we need the following definition.

Definition 46 (S-Characterization Relations)
Let Δ be a subset of $\mathcal{LM}$ and let $S \subseteq \mathcal{N}$. Then $\Delta^S(\sigma \rhd P) \stackrel{def}{=} \{\phi \in \Delta \mid \sigma \rhd P \models_S \phi\}$ and the relation $=_{\Delta^s}$ is defined by $=_{\Delta^s} \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \Delta^S(\sigma_P \rhd P) = \Delta^S(\sigma_Q \rhd Q)\}$.

■

Now, we are ready to prove that $=_{\mathcal{LM}^s}$ and $\sim^S_{ESB}$ coincide.

Theorem 20 (Coincidence of $=_{\mathcal{LM}^s}$ and $\sim^S_{ESB}$)
$\sigma_P \rhd P =_{\mathcal{LM}^s} \sigma_Q \rhd Q$ if and only if $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$.

Proof: We will first prove that $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$ implies $\sigma_P \rhd P =_{\mathcal{LM}^s} \sigma_Q \rhd Q$. Assume $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$ and $\sigma_P \rhd P \models_S \phi$. We must show that $\sigma_Q \rhd Q \models_S \phi$. The proof will be by structural induction on ϕ.

Basis: The same as in the proof of theorems 16 and 17.

Step:

Case $\phi \equiv \langle a(u)\rangle^L\phi'$.

We have that $a \in \mathcal{A}(\sigma_P)$ and that there exists P' such that $P \xrightarrow{a(u)} P'$ and for all

$\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$ and $e(\zeta\sigma_P) \neq \partial$ it holds that $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\} \models_S \phi'\{T(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)], \zeta)/u\}$. Since $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$ we have that there exists Q' such that $Q \xrightarrow{a(u)} Q'$ and for all $\zeta \in \Upsilon$, where $\mathrm{e}(\zeta\sigma_Q) \neq \partial$ and $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_Q)) = \emptyset$, $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\} \sim^S_{ESB} \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}$, where $\tilde{z} \cap \mathrm{dom}(\sigma_P) = \emptyset$. By induction and the fact that $T(\sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)], \zeta) = T(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)], \zeta)$ we have that for all $\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_Q)) = \emptyset$ and $e(\zeta\sigma_Q) \neq \partial$ it holds that $\sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\} \models_S \phi'\{T(\sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)], \zeta)/u\}$ and hence $\sigma_Q \rhd Q \models_S \phi$.

Case $\phi \equiv \langle \bar{a} \rangle \phi'$.

We have that $a \in \mathcal{A}(\sigma_P)$ and there exist $\tilde{b}$, M, and P' such that $\tilde{b} \cap \mathrm{fn}(P, \sigma_P) = \emptyset$, $\tilde{b} \subseteq S$, $P \xrightarrow{(\nu\ \tilde{b})\bar{a}M} P'$, and $\sigma_P[x \mapsto M] \rhd P' \models_S \phi'$. Since $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$ we have that there exist $\tilde{d}$, N, and Q' such that $Q \xrightarrow{(\nu\ \tilde{d})\bar{a}N} Q'$, where $\tilde{d} \subseteq S$, $\tilde{d} \cap \mathrm{fn}(Q, \sigma_Q) = \emptyset$, and $\sigma_P[z \mapsto M] \rhd P' \sim^S_{ESB} \sigma_Q[z \mapsto N] \rhd Q'$, where $z \notin \mathrm{dom}(\sigma_P)$. By induction we have that $\sigma_Q[z \mapsto N] \rhd Q' \models_S \phi'$ and hence $\sigma_Q \rhd Q \models_S \phi$.

The remaining cases are proven in a way similar to that of the proof of theorem 17.

Finally, we prove that $\sigma_P \rhd P =_{\mathcal{LM}^s} \sigma_Q \rhd Q$ implies $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$. We will do this by showing that the relation R defined by

$$R \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \sigma_P \rhd P =_{\mathcal{LM}^s} \sigma_Q \rhd Q\}$$

is an S-environment sensitive bisimulation. Assume $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. By lemma 20 (naturally modified to $\models_S$) it follows that $\sigma_P \sim''_e \sigma_Q$. Suppose $P \xrightarrow{a(u)} P'$ and $a \in \mathcal{A}(\sigma_P)$. Let $\{Q_i\}_{i \in I}$ be an enumeration of $\{Q' \mid Q \xrightarrow{a(u)} Q'\}$ and assume that for each $i \in I$ there exists $\zeta_i \in \Upsilon$ with $\mathrm{n}(\zeta_i) \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$ and $e(\zeta_i\sigma_P) \neq \partial$ such that $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta_i)] \rhd P'\{e(\zeta_i\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta_i)] \rhd Q_i\{e(\zeta_i\sigma_Q)/u\}) \notin R$. For each $i \in I$ there exists ϕ_i such that $\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta_i)] \rhd P'\{e(\zeta_i\sigma_P)/u\} \models_S \phi_i$ and $\sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta_i)] \rhd Q_i\{e(\zeta_i\sigma_Q)/u\} \not\models_S \phi_i$. Let $\phi \stackrel{def}{=} \langle a(u) \rangle^L \bigwedge_{i \in I} [u = T(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta_i)], \zeta_i)]\phi_i$. Now, we have $\sigma_P \rhd P \models_S \phi$ and $\sigma_Q \rhd Q \not\models_S \phi$. This is a contradiction since $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. Therefore, there must exist Q' such that $Q \xrightarrow{a(u)} Q'$ and for all $\zeta \in \Upsilon$ with $\mathrm{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma_P)) = \emptyset$ and $e(\zeta\sigma_P) \neq \partial$ it holds that $(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd P'\{e(\zeta\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \mathrm{n}(\zeta)] \rhd Q'\{e(\zeta\sigma_Q)/u\}) \in R$. The remaining cases are shown in a way similar to that of the proof of theorem 17. ■

Finally, we conclude that strong late environment sensitive bisimilarity can be characterized by the logic $\mathcal{LM}$.

Corollary 5

Let $=_{\mathcal{LM}} \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \exists S \subseteq \mathcal{N}.(\sigma_P \rhd P =_{\mathcal{LM}^s} \sigma_Q \rhd Q \wedge \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) \subseteq S \wedge |S| = \infty \wedge |\mathcal{N} \setminus S| = \infty)\}$. Then $\sigma_P \rhd P =_{\mathcal{LM}} \sigma_Q \rhd Q$ if and only if $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$.

■

8 Conclusion

In this report we have presented a strong late version of the environment sensitive bisimilarity given by Boreale at al. and proved that this can be used as an alternative characterization of framed bisimilarity. We have proven that $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ if and only if $\mathcal{F}_e(\sigma_P, \sigma_Q) \vdash P \sim_f Q$. Our proof of this involved the notion of fenced bisimilarity defined by Elkjær et al. Furthermore, we presented the notions of frameless framed bisimulation and frameless fenced bisimulation. We have shown that frameless framed bisimilarity and frameless fenced bisimilarity coincide. This was proven using an adaptation of the proof technique used by Elkjær et al. in proving that framed bisimilarity and fenced bisimilarity coincide. We have shown that frameless framed bisimilarity can be used to characterize strong early environment sensitive bisimilarity. Finally, we proposed some modal logics for the Spi-calculus. We proved that these can be used to characterize a strong early version and our new strong late version of the environment sensitive bisimilarity given by Boreale at al. The definition of our new strong late version of the environment sensitive bisimulation makes it difficult to give a logical characterization of strong late environment sensitive bisimilarity directly. Therefore, we introduced a new notion of environment sensitive bisimulation called S-environment sensitive bisimulation and gave a logical characterization of S-environment sensitive bisimilarity. It turned out that when S has some special properties it holds that $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$ if and only if $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$. With this useful connection between S-environment sensitive bisimilarity and strong late environment sensitive bisimilarity we were able to give a logical characterization of strong late environment sensitive bisimilarity.

8.1 Future Work

At this point it would be interesting to study whether the results presented in chapters 5 and 6 about correspondence between strong bisimilarities also hold for weak versions of the bisimilarities. Since the lemmas needed in proving the results for the strong bisimilarities do not depend on transitions we do not need to show them again.

In chapter 7 we illustrated how a security property for security protocols could be expressed in the proposed modal logic. It would be interesting to see whether our logic can

be used to describe some of the classical protocols like the 'Wide Mouthed Frog Protocol'. Although our modal logic can be used to characterize environment sensitive bisimilarity it suffers from the fact that to describe properties of a configuration with an infinite sequence of transitions we need infinite formulae. It would be fitting to extend the logic with recursion in a way that makes it possible to describe configuration with an infinite sequence of transitions with finite formulae.

Bibliography

[1] & Abadi, M. & Burrows, M. & Needham, R. M. *A Logic of Authentication.* Proceedings of the Royal Society of London, 426:233-271, 1989.

[2] Abadi, Martín & Gordon, Andrew D. *A Bisimulation Method for Cryptographic Protocols.* Lecture Notes in Computer Science, 1381:12-26, 1998.

[3] Abadi, Martín & Gordon, Andrew D. *A Calculus for Cryptographic Protocols. The Spi-Calculus.* In Proceedings of the Fourth ACM Conference on Computer and Communications Security, pp. 36-47, 1997.

[4] Abadi, Martín & Gordon, Andrew D. *A Calculus for Cryptographic Protocols. The Spi-Calculus.* Journal of Information and Computation, 148(1):1-70, 1999.

[5] Boreale, Michele. *Symbolic Analysis of Cryptographic Protocols in the Spi-Calculus.* http://www.dsi.unifi.it/∼boreale/Reach-spi.ps.

[6] Boreale, Michele & De Nicola, Rocco & Pugliese, Rosario. *Proof Techniques for Cryptographic Processes (Extended version).* Proceedings of LICS 99:157-166, 1999.

[7] Elkjær, Anders Strandløv & Höhle, Michael & Hüttel, Hans & Nielsen, Kasper Overgård. *Towards Automatic Bisimilarity Checking in the Spi-Calculus.* Proceedings of CATS/DMTCS'99.

[8] Frendrup, Ulrik & Jensen, Jesper Nyholm. *Checking for Open Bisimilarity in the π-Calculus.* BRICS RS-01-8, 2001.

[9] Hennessy, Matthew C. B. & De Nicola, Rocco. *Testing Equivalence for Processes.* Lecture Notes in Computer Science, 154:548-560, 1983.

[10] Hüttel, Hans & Kleist, Josva & Nestmann, Uwe. *Towards a Symbolic Semantics for the $s\pi$-Calculus.* Draft of September 11, 2000, 11:03.

[11] Milner, Robin. *Communication and Concurrency.* Prentice Hall International, Englewood Cliffs, 1989. ISBN: 0-13-115007-3.

[12] Milner, Robin & Parrow, Joachim & Walker, David. *Modal Logics for Mobile Processes.* Journal of Theoretical Computer Science, 114(1):149-171, 1993.

[13] Park, David. *Concurrency and Automata on Infinite Sequences.* Lecture Notes in Computer Science, 104:167-183, 1981.

[14] Paulson, Lawrence C. *Proving Security Protocols Correct.* LICS: IEEE Symposium on Logic in Computer Science, 1999.

[15] Schneier, Bruce. *Applied Cryptography: Protocols, Algorithms, and Source Code in C.* John Wiley & Sons, second edition, 1996. ISBN: 0471117099.