Modal Logics for Cryptographic Processes

Ulrik Frendrup* Hans Hüttel† Jesper Nyholm Jensen‡

June 2, 2002

Abstract

We present three modal logics for the spi-calculus and show that they capture strong versions of the environment sensitive bisimulation introduced by Boreale et al. Our logics differ from conventional modal logics for process calculi in that they allow us to describe the knowledge of an attacker directly.

1 Introduction

In recent years the study of correctness issues of security protocols has become an important research topic. Following Dolev and Yao [5], a basic assumption is that all communication of a protocol may be visible to the hostile environment and that this hostile environment is capable of interfering with the protocol by altering or blocking any message and by creating new messages. Moreover, these are the only kinds of attacks – an attacker cannot exploit weaknesses of the encryption algorithm itself (the 'perfect encryption hypothesis').

In the Dolev-Yao setting, an important approach to reasoning about properties of security protocols is to use *modal logics*, an important example of which is the logic of authentication introduced by Burrows et al. in [1].

Another promising approach in the Dolev-Yao setting is that of using *process calculi*. A recent such calculus is the spi calculus of Abadi and Gordon [3], a dialect of the π-calculus [9]. In the spi calculus security protocols are described as process terms and the correctness relation is captured by a notion of behavioural equivalence [8]. Abadi and Gordon proposed may-testing equivalence as their choice of equivalence. However, may-testing equivalence does not allow for a simple proof technique. As a result, both Abadi and Gordon [2] and Boreale et al. [4] have introduced modified notions of bisimulation equivalence which capture both the interaction with and the knowledge of the environment.

In this paper we relate the two strands of research by presenting three modal logics for the environment-sensitive semantics of the spi calculus introduced by Boreale, De Nicola and Pugliese [4]. Our main result is that these logics capture strong versions of the environment sensitive bisimulations of [4] in both their late and early versions. In this way, our work can be viewed as extending the results on logics for the π-calculus [10]. An important consequence of our results is that nonbisimilar processes can be distinguished by our logics. If P in environment σ_P and Q in environment σ_Q are inequivalent, then there is some property ϕ satisfied by one process but not by the other in their respective environments.

Our modal logics are environment-sensitive; they provide us with the ability to describe both the knowledge of an attacker and the behaviour of a protocol. The logics are all based on a common

*frendrup@mail1.stofanet.dk

†Contact author. E-mail: hans@cs.auc.dk, BRICS, Department of Computer Science, Aalborg University, 9220 Aalborg Ø, Denmark.

‡jnyholm@math.auc.dk, Department of Mathematical Sciences, Aalborg University, 9220 Aalborg Ø, Denmark.

sublogic Φ from which we shall construct the logics $\mathcal{F}$, $\mathcal{EM}$ and $\mathcal{LM}$. We consider a version of the spi calculus without pairs; the generalization to the full calculus is straightforward.

In [6] Durgin, Pavlovic and Mitchell have introduced a modal logic for a process calculus based on ideas from strand spaces and the spi calculus. An important difference between our work and theirs is our explicit aim is to determine logics that correspond to the equivalence-based notion of correct in the spi calculus.

2 The spi calculus: Syntax

We shall consider a spi calculus which is a subset of the original calculus of [3] in that we omit numbers and pairs. Unlike [3, 4], where encryption is a message term constructor while decryption is a process construct, both are part of our message term language.

The syntactic categories of the spi calculus are: an infinite set of *names*, $a, b, k \ldots \in \mathcal{N}$, an infinite set of *variables*, $u, v, \ldots \in \mathcal{V}$, a set of *expressions* $L, M, N, \ldots \in \mathcal{L}$, a set of *guards*, $G \ldots \in \mathcal{G}$, and a set of *agents*, $A, B, \ldots \in \mathcal{A}g$.

Messages are defined as follows:

$$K, L ::= \ a \mid u \mid \{L\}^E_L \mid \{L\}^D_L$$

$\{L_1\}^E_{L_2}$ represents the term L_1 encrypted under key L_2. $\{L_1\}^D_{L_2}$ represents the term L_1 decrypted (if possible) with key L_2. The term $\{\ldots\{\{M\}^E_{k_1}\}^E_{k_2}\}\ldots\}^E_{k_n}$ successively encrypted under n keys $k_1, \ldots, k_n$ will be denoted by the shorthand $\{M\}^E_{\tilde{k}}$. The set of *messages*, $\mathcal{M}$, are the expressions of $\mathcal{L}$ that only consist of names and encryptions. They have the syntax

$$M, N ::= \ a \mid \{N\}^E_a$$

Guards have the structure

$$G ::= \ tt \mid G \wedge G \mid L = L \mid L : \mathcal{N}$$

Finally, agents are defined by

$$A ::= \ \mathbf{0} \mid L(u).A \mid \overline{L}L.A \mid GA \mid A + A \\ \mid A|A \mid (\nu\ a)A \mid \ !A$$

In an 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. $A\{M/u\}$ denotes the agent obtained by replacing every free occurrence of u in A by M, renaming bound names as necessary. We identify agents up to α-conversion of bound names and variables. If agents A_1 and A_2 can be identified in this way, we write $A_1 \equiv_\alpha A_2$. A *process* is an agent that does not contain any free variables; $\mathcal{P}r$ denotes the set of all processes. The set of processes is ranged over by P, Q, and R.

3 Environments

An environment records the knowledge of an observer/attacker. Following [4], an environment is a function $\sigma : \mathcal{Z} \to \mathcal{M}$, where $\mathcal{Z}$ is a set of environment variables such that $\mathcal{Z} \cap \mathcal{V} = \emptyset$. We write $\{M_1/x_1, M_2/x_2, \ldots, M_n/x_n\}$ for the environment σ defined by $\sigma x_i = M_i$ for all $i \in \{1, 2, \ldots, n\}$. $\sigma[x \mapsto M]$ denotes the environment that maps x to M and any other environment variable y to σy.

3.1 Environment messages

The messages that an environment σ can send to a process are evaluated *environment messages*.

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 $\mathrm{fz}(\zeta)$.

We evaluate environment messages using the function $e : \mathcal{L} \to \mathcal{M} \cup \{\perp\}$, defined in section Table 1 and let $\perp$ represent the value of any message that cannot be evaluated. Typically, such messages involve a decryption operation that cannot be performed.

3.2 The knowledge of an environment

Our semantics of the spi calculus is environment-sensitive; it depends on the information that can be deduced from the environment. We employ the characterization of the knowledge of an environment presented in [4, 11]. The analysis of a set of messages W is the set of messages that can be deduced from W by decryption.

Definition 1 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 knowledge of a set of messages W is the set of names of the analysis of W.

Definition 2 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 $\mathcal{A}(\sigma)$ and $\mathcal{K}(\sigma)$ for $\mathcal{A}(\text{range}(\sigma))$ and $\mathcal{K}(\text{range}(\sigma))$. 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 3 Let $W \subseteq \mathcal{M}$. The core of the message $M \in \mathcal{M}$ with respect to W, written $\text{core}(W, M)$, is defined by

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

■

For an environment σ and a message M we will use the shorthand notation $\text{core}(\sigma, M)$ for $\text{core}(\text{range}(\sigma), M)$.

3.3 Equivalence of environments

Following [4], two environments are equivalent if they have the same decryption power. If $\tilde{N}_i$ is a tuple of messages where $i \in I$ and $J \subseteq I$, we write $\tilde{N}[\tilde{J}]$ for the tuple $\{N_i \mid i \in J\}$.

Definition 4 Let σ and σ' be environments where $\text{dom}(\sigma) = \text{dom}(\sigma') = \{x_i \mid i \in I\}$ for some 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 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 $N_i' \in \mathcal{N}$.

■

4 The spi calculus: Semantics

We here present the environment sensitive semantics introduced in [4] and our notion of bisimilarity. The semantics has two levels.

4.1 Processes

At the process level transitions have the form $A \stackrel{\alpha}{\longrightarrow} A'$, where α is given by the grammar

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

The semantics of processes 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 3. The symmetric rules for Sum, Par, and Com have been omitted.

$$e(a) \stackrel{def}{=} a \qquad e(\{L\}_K^E) \stackrel{def}{=} \begin{cases} \{N\}_b^E & \text{if } e(K) = b \in \mathcal{N} \wedge e(L) = N \neq \perp \\ \perp & \text{otherwise} \end{cases}$$

$$e(u) \stackrel{def}{=} \perp \qquad e(\{L\}_K^D) \stackrel{def}{=} \begin{cases} N & \text{if } e(K) = b \in \mathcal{N} \wedge e(L) = \{N\}_b^E \\ \perp & \text{otherwise} \end{cases}$$

Table 1: The message evaluation function $e : \mathcal{L} \rightarrow \mathcal{M} \cup \{\perp\}$

$$e'(tt) \stackrel{def}{=} tt \qquad e'(G_1 \wedge G_2) \stackrel{def}{=} e'(G_1) \wedge e'(G_2)$$

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

Table 2: The guard evaluation function $e' : \mathcal{G} \rightarrow \{tt, ff\}$

Note that our semantics is a *late* operational semantics; this is apparent in the clause [Inp] where the variable u is left uninstantiated. Our choice of a late semantics makes it easier to formulate both late and early environment-sensitive bisimulation equivalence in Section 4.3

4.2 Environment sensitive semantics

At the environment sensitive level of our semantics, configurations consist of a process together with an environment.

Definition 5 The set of configurations, Γ, is defined as

$$\Gamma \stackrel{def}{=} \{\sigma :\rhd P \mid \sigma : \mathcal{Z} \rightarrow \mathcal{M}, P \in \mathcal{P}r\}$$

■

The environment sensitive semantics 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. 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, $\mathcal{A}ct_e$, is defined by the grammar

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

4.3 Environment sensitive bisimulation

Environment sensitive bisimilarity, introduced in [4] relates configurations of environment sensitive semantics. Unlike [4], we consider *strong* equivalences. First, we define a strong *early* environment sensitive bisimilarity where the matching of a transition may depend on the message sent by the environment.

Definition 6 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 $(\sigma'_P \rhd P', \sigma'_Q \rhd Q') \in R$. ■

Definition 7 The configurations $\sigma_P \rhd P$ and $\sigma_Q \rhd Q$ are strong early environment sensitive

[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 $e(L_2) = N \neq \perp$	[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]	$\dfrac{A_1 \xrightarrow{\alpha} A_1'}{A_1 \mid A_2 \xrightarrow{\alpha} A_1' \mid A_2}$ $\text{bn}(\alpha) \cap \text{fn}(A_2) = \emptyset$
[Com]	$\dfrac{A_1 \xrightarrow{(\nu\ \tilde{c})\bar{a}N} A_1' \quad A_2 \xrightarrow{a(u)} A_2'}{A_1 \mid A_2 \xrightarrow{\tau} (\nu\ \tilde{c})(A_1' \mid A_2'\{N/u\})}$ $\tilde{c} \cap \text{fn}(A_2) = \emptyset$	[Res]	$\dfrac{A \xrightarrow{\alpha} A'}{(\nu\ b)A \xrightarrow{\alpha} (\nu\ b)A'}$ $b \notin \text{n}(\alpha)$
[Open]	$\dfrac{A \xrightarrow{(\nu\ \tilde{c})\bar{a}N} A'}{(\nu\ b)A \xrightarrow{(\nu\ \{b\} \cup \tilde{c})\bar{a}N} A'}$ $b \in (\text{n}(N) \setminus \tilde{c})$ and $b \neq a$	[Rep]	$\dfrac{A \mid !A \xrightarrow{\alpha} A'}{!A \xrightarrow{\alpha} A'}$

Table 3: Late operational semantics for the Spi-calculus.

[E-Tau] $$\frac{P \xrightarrow{\tau} P'}{\sigma \rhd P \xrightarrow[-]{\tau} \sigma \rhd P'}$$

[E-Inp] $$\frac{P \xrightarrow{a(u)} P'}{\sigma \rhd P \xrightarrow[(\nu\ \tilde{c})\bar{a}\zeta]{a(u)} \sigma[\tilde{z} \mapsto \tilde{c}] \rhd P'\{N/u\}}$$

$e(\zeta\sigma) = N \neq \perp$, $\tilde{z} \cap \text{dom}(\sigma) = \emptyset$, $a \in \mathcal{A}(\sigma)$, $\tilde{c} = \text{n}(\zeta)$, and $\tilde{c} \cap \text{fn}(P, \sigma) = \emptyset$

[E-Out] $$\frac{P \xrightarrow{(\nu\ \tilde{c})\bar{a}N} P'}{\sigma \rhd P \xrightarrow[a(z)]{(\nu\ \tilde{c})\bar{a}N} \sigma[z \mapsto N] \rhd P'}$$

$a \in \mathcal{A}(\sigma), z \notin \text{dom}(\sigma),$ and $\tilde{c} \cap \text{fn}(\sigma) = \emptyset$

Table 4: Environment sensitive semantics.

bisimilar, written $\sigma_P \rhd P \sim_{EESB} \sigma_Q \rhd Q$, if there exists a strong early environment sensitive bisimulation R such that $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. ■

Alternatively, we could define a *late* version of environment sensitive bisimilarity where the matching of a transition is independent of the message sent by the environment. Here we capture the late instantiation by means of the late semantics at the process level.

Definition 8 A symmetric relation $R \subseteq \Gamma \times \Gamma$ is a strong late 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 $e(\zeta\sigma_P) \neq \perp$ and $\text{n}(\zeta) \cap \text{fn}(P, Q, \sigma_P, \sigma_Q) = \emptyset$, $(\sigma_P[\tilde{z} \mapsto \tilde{c}] \rhd P'\{e(\zeta\sigma_P)/u\}, \sigma_Q[\tilde{z} \mapsto \tilde{c}] \rhd Q'\{e(\zeta\sigma_Q)/u\}) \in R$, where $\tilde{z} \cap \text{dom}(\sigma_P) = \emptyset$ and $\tilde{c} = \text{n}(\zeta)$.

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

■

Definition 9 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 Logical formulae

The logics that we shall present all contain the usual propositional connectives and have two kinds of formulae. Common to all three logics is the set of *environment formulae*, ranged over by ϕ_σ. These are atomic formulae that describe the contents of an environment.

The logics differ from each other with respect to their *process formulae*, ranged over by ϕ_P. These are modal formulae that describe the behaviour of a process. More precisely, the difference lies in the input modalities which correspond to the matching conditions for early, resp. late bisimulation.

Any formula may contain *formula messages* from the set Ω, ranged over by η.

5.1 Logical formulae: Syntax

The syntax of formulae and formula messages is:

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

where I is an index set which may be infinite. We sometimes use additional propositional connectives, letting $\phi_1 \vee \phi_2$ and *tt* stand for $\neg(\neg\phi_1 \wedge \neg\phi_2)$ and $\bigwedge_{i\in\emptyset}\phi_i$, respectively.

Environment formulae ϕ_σ let us express the contents of an environment. Firstly, we can express whether messages of the environment can be completely decrypted with the keys $\tilde{k}$ from the knowledge of the environment ($x \mapsto \{a\}^E_{\tilde{k}}$) or not ($x \mapsto \{?\}^E_{\tilde{k}}$). This aspect of our logic resembles the construct P *sees* X in the belief logic of [1]. If a variable x is instantiated to a name b, the set of keys $\tilde{k}$ is empty and we use the shorthand $x \mapsto b$.

Secondly, as we aim to be able to express environments up to equivalence we need to be able to express that exactly n environment variables are bound by an environment ($\# = n$) and whether the core of a message is a name ($\mathrm{core}(x) : \mathcal{N}$).

Process formulae ϕ_P describe the behaviour of a process by means of the Hennessy-Milner-style modalities used in modal logics for the π-calculus [10]. In both the *early* input modality, $\langle a(u)\rangle^E\phi$, and the *late* input modality $\langle a(u)\rangle^L\phi$, u is bound in ϕ. However, their semantics differ so as to correspond to the matching conditions of early and late bisimilarity. In the former modality, u is instantiated in ϕ whereas u is the subject of a universal quantification over possible input terms in the latter.

The syntactic conventions are standard. The sets of *free variables*, $\mathrm{fv}(\phi)$, and *bound variables*, $\mathrm{bv}(\phi)$, of a formula are defined as expected. We write $\phi\{\eta/u\}$ for the formula obtained be replacing every free occurrence of u in ϕ by η, renaming bound variables as necessary, and identify formulae up to renaming of bound variables. The logic Φ consists of closed formulae, $\Phi = \{\phi \mid \mathrm{fv}(\phi) = \emptyset\}$. The following example illustrates how to express a security property in the proposed modal logic.

Example 1. Let $P \stackrel{def}{=} (\nu\ k_3)\bar{b}\{k_3\}^E_{k_3}$ and $\sigma_P \stackrel{def}{=} [x_1 \mapsto b, x_2 \mapsto k_1, x_3 \mapsto \{M\}^E_{k_2}]$. Process P can emit a secret key, k_3, encrypted with itself on the channel b to the environment σ_P. This can be described by the formula

$$x_1 \mapsto b \wedge x_2 \mapsto k_1 \wedge x_3 \mapsto \{?\}^E_{k_2} \wedge \langle\bar{b}\rangle x_4 \mapsto \{?\}^E_{k_3}$$

Notice the modality of the latter conjunct. ■

5.2 Logical formulae: Semantics

The satisfaction relation between configurations and all formulae of Φ apart from the late modality $\langle a(u)\rangle^L\phi$is given in Table 5. The late input modality $\langle a(u)\rangle^L\phi$ will be handled separately in section 6.2, as the semantics involves a universal quantification over a suitable set of names. Section 6.2 describes how these names must be chosen.

The function $T(\sigma, \zeta)$ 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. $|\{x \in \text{dom}(\sigma) \mid \sigma(x) = a\}| = 1$).

We use the shorthand notation $\sigma \vDash \phi$ if $\sigma \rhd P \vDash \phi$ for all $P \in \mathcal{P}r$.

6 A logical characterization of bisimilarity

The two notions of bisimilarity from Section 4.3 can be captured by our modal logics.

6.1 Characterization of $\sim_{EESB}$

We first present two early logics $\mathcal{F}$ and $\mathcal{EM}$ that both characterize strong early environment sensitive bisimilarity.

Let Φ_0 denote the set of those formulae of Φ that neither contain the match connective $[\eta = \eta]\phi$ nor the modalites $\langle a\zeta\rangle\phi$, $\langle a(u)\rangle^E\phi$, and $\langle a(u)\rangle^L\phi$.

- $\mathcal{F}$ is Φ_0 extended with $\langle a\zeta\rangle\phi$
- $\mathcal{EM}$ is Φ_0 extended with $[\eta = \eta]\phi$ and $\langle a(u)\rangle^E\phi$.

To prove that strong early environment sensitive bisimilarity can be characterized by the logics $\mathcal{F}$ and $\mathcal{EM}$ we define a logical process equivalence for each of the two logics. Here we need the following definition.

Definition 10 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 is essential as it shows that our environment formulae allow us to characterize environments up to equivalence.

Lemma 1 Let σ be an environment. Then there exists an environment 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 $|\text{dom}(\sigma)| = n$. Let $\phi_\sigma \stackrel{def}{=} \bigwedge_{i\in I}\phi_i$ be the formula whose conjuncts are defined as follows:

- $\# = n$ always occurs as a conjunct
- $x \mapsto \{a\}^E_{\tilde{k}}$ occurs for any x such that $\text{core}(\sigma, \sigma(x)) = a$ for $a \in \mathcal{N}$ and $\sigma(x) = \{a\}^E_{\tilde{k}}$,
- $x \mapsto \{?\}^E_{\tilde{k}} = \phi_i$ occurs for any x such that $\text{core}(\sigma, \sigma(x)) = M \notin \mathcal{N}$ for some M and $\sigma(x) = \{M\}^E_{\tilde{k}}$
- $\text{core}(x) : \mathcal{N} = \phi_i$ occurs for any x such that $\text{core}(\sigma, \sigma(x)) \in \mathcal{N}$

By Table 5 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 $\sigma \sim_e \sigma'$. ■

We can now show that $=_\mathcal{F}$ and $\sim_{EESB}$ coincide.

Theorem 1 $\sigma_P \rhd P =_\mathcal{F} \sigma_Q \rhd Q$ if and only if $\sigma_P \rhd P \sim_{EESB} \sigma_Q \rhd Q$.

PROOF: We 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 proceeds by structural induction on ϕ. Next, 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 do this by showing that

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

is a strong early environment sensitive bisimulation. ■

Next, we prove that $=_\mathcal{EM}$ and $\sim_{EESB}$ coincide.

Theorem 2 $\sigma_P \rhd P =_\mathcal{EM} \sigma_Q \rhd Q$ 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 $\sigma_P \rhd P \vDash \phi$. We must show that $\sigma_Q \rhd Q \vDash \phi$. The proof is

$\sigma \rhd P \vDash \neg\phi$	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 $e(\zeta\sigma) \neq \bot$ 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 $\tilde{k} \subseteq \mathcal{K}(\sigma)$
$\sigma \rhd P \vDash \mathrm{core}(x) : \mathcal{N}$	if $\mathrm{core}(\sigma,\sigma(x)) \in \mathcal{N}$

Table 5: The satisfaction relation

by structural induction on ϕ. Next, 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 1 and the fact that $\sigma_P \rhd P \vDash \langle a\zeta\rangle\phi$ if and only if $\sigma_P \rhd P \vDash \langle a(u)\rangle^E[u = T(\sigma_P[\tilde{z} \mapsto \mathrm{n}(\zeta)], \zeta)]\phi$. ■

6.2 Characterization of $\sim_{ESB}$

We now present the logic $\mathcal{LM}$ and show that it can be used to characterize strong late environment sensitive bisimilarity. It is somewhat involved to prove this result using the technique of the proofs of theorems 1 and 2 if we employ Definition 8 as is. In clause (ii) of the definition we must quantify over the infinitely many input messages $\zeta \in \Upsilon$, where $e(\zeta\sigma_1) \neq \bot$ and $\mathrm{n}(\zeta) \cap \mathrm{fn}(P, Q, \sigma_1, \sigma_2) = \emptyset$. Thus, the names in an input message ζ must be chosen with respect to both P and Q.

This leads us to define the auxiliary notion of S-environment sensitive bisimulation where $S \subseteq \mathcal{N}$ represents the set of names that input terms may contain. We show that S-environment sensitive bisimilarity may be used to characterize strong late environment sensitive bisimilarity for a suitably chosen S and subsequently prove that $\mathcal{LM}$ can be used to characterize S-environment sensitive bisimilarity using the same technique as in the proofs of theorems 1 and 2.

6.2.1 The logic $\mathcal{LM}$

In the late logic $\mathcal{LM}$ the *late input* modality is the only modality for input transitions.

$$\phi_P ::= \mid \langle\tau\rangle\phi \mid \langle a(u)\rangle^L\phi \mid \langle\bar{a}\rangle\phi \mid [\eta = \eta]\phi$$

6.2.2 S-environment sensitive bisimulation

Definition 11 (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 $e(\zeta\sigma_P) \neq \perp$ 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 $z \notin \mathrm{dom}(\sigma_P)$.

■

Definition 12 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 $(\sigma_P \rhd P, \sigma_Q \rhd Q) \in R$. ■

Generally, $\sim^S_{ESB}$ and $\sim_{ESB}$ do not coincide.

Example 2. Consider $P_1 \stackrel{def}{=} (\nu\ n)\bar{a}n$ and $Q_1 \stackrel{def}{=} \mathbf{0}$ and $\sigma_1 \stackrel{def}{=} \{a/x\}$. If $S \stackrel{def}{=} \emptyset$ we have $\sigma_1 \rhd P_1 \sim^S_{ESB} \sigma_1 \rhd Q_1$ but not $\sigma_1 \rhd P_1 \sim_{ESB} \sigma_1 \rhd Q_1$. Next, consider $P_2 \stackrel{def}{=} (\nu\ k)(\nu\ m)\bar{a}\{m\}^E_k$ and $Q_2 \stackrel{def}{=} (\nu\ k)\bar{a}\{k\}^E_k$ and $\sigma_2 \stackrel{def}{=} \{a/x\}$. We have $\sigma_2 \rhd P_2 \sim_{ESB} \sigma_2 \rhd Q_2$ but if $S \stackrel{def}{=} \{k\}$ we do not have $\sigma_2 \rhd P_2 \sim^S_{ESB} \sigma_2 \rhd Q_2$. ■

However, 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 2 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 $\mathrm{fn}(P') \cup \{a\} \cup \mathrm{n}(M) \subseteq \mathrm{fn}(P) \cup \tilde{c}$.

Lemma 3 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 $P\sigma_{\mathcal{N}} \xrightarrow{\alpha\sigma_{\mathcal{N}}} P'\sigma_{\mathcal{N}}$.

Lemma 4 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 $(\sigma_P \rhd P)\sigma_{\mathcal{N}} \sim_{ESB} (\sigma_Q \rhd Q)\sigma_{\mathcal{N}}$.

Theorem 3 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 $\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q$.

PROOF: The relation R defined by $R \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q\ , \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) \subseteq S \cup \mathcal{K}(\sigma_P)\}$ is an S-environment sensitive bisimulation. That transitions can be matched follows from Lemmas 2,3 and 4 ■

If two configurations are S-environment sensitive bisimilar for some infinite and co-infinite set $S \subseteq \mathcal{N}$ containing the free names of the two configurations then they are also strong late environment sensitive bisimilar.

Theorem 4 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 both infinite. Then $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$.

PROOF: The relation $R \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \exists S \subseteq \mathcal{N}.\ (\sigma_P \rhd P \sim^S_{ESB} \sigma_Q \rhd Q \wedge \mathrm{fn}(P, Q, \sigma_P, \sigma_Q) \subseteq S \wedge |S| = \infty \wedge |\mathcal{N} \setminus S| = \infty)\}$ is a strong late environment sensitive bisimulation. ■

6.2.3 Characterization of $\sim^S_{ESB}$ and $\sim_{ESB}$

We now characterize $\sim^S_{ESB}$ and consequently also $\sim_{ESB}$ by the logic $\mathcal{LM}$. To do this, we introduce a S-satisfaction relation between configurations and formulae of $\mathcal{LM}$ as given in Table 6. Here, the quantification over names for the late input modality must be found among S.

Next, we define a logical process equivalence for our logic with respect to an $S \subseteq \mathcal{N}$.

Definition 13 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 $=_{\Delta^S} \stackrel{def}{=} \{(\sigma_P \rhd P, \sigma_Q \rhd Q) \mid \Delta^S(\sigma_P \rhd P) = \Delta^S(\sigma_Q \rhd Q)\}$. ■

Theorem 5 $\sigma_P \rhd P =_{\mathcal{LM}^S} \sigma_Q \rhd Q$ 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. 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 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. ■

We therefore have that strong late environment sensitive bisimilarity can be characterized by the logic $\mathcal{LM}$.

Corollary 1 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 $\sigma_P \rhd P \sim_{ESB} \sigma_Q \rhd Q$.

■

7 An application

In this section we describe a simplified, flawed version of the Wide-Mouthed Frog protocol where the session key is revealed by the server. This flawed protocol should not be equivalent to the correct protocol. We demonstrate this by presenting a distinguishing modal formula.

In the correct version of the Wide-Mouthed Frog protocol the principals A and B share the keys k_{AS} and k_{BS}, respectively, with a server S. Before A sends a 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 M and sends k_{AB} to B encrypted with key k_{BS}. Now, A can send its secret message M to B encrypted with the key k_{AB}. This protocol can be expressed in the spi calculus as follows.

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

Here $F(M)$ is an agent representing the behaviour of B upon reception of M.

The flawed protocol, where S accidentally reveals the session key, can be expressed as follows.

$$\begin{aligned}
S' &\stackrel{def}{=} c_{AS}(u).\overline{c_{SB}}\{u\}^D_{k_{AS}}.\mathbf{0} \\
P'(N) &\stackrel{def}{=} (\nu\, k_{AS})(\nu\, k_{BS})(A(N) \mid B \mid S')
\end{aligned}$$

The two configurations $\sigma \rhd P(a)$ and $\sigma \rhd P'(a)$, where $\sigma \stackrel{def}{=} \{c_{AS}/x_1, c_{AB}/x_2, c_{SB}/x_3\}$, are not strong early environment sensitive bisimilar; the correct version will never, in the course of its 3 steps, allow the environment to obtain knowledge of any ciphertext $\{a\}^E_{\tilde{k}}$. This can be expressed by the following distinguishing formula:

$$\phi_a \stackrel{def}{=} \bigwedge_{i=0}^{3} [\alpha]^i \neg \left(\bigvee_{x \in \mathcal{Z}, \tilde{k} \subseteq \mathcal{N}} x \mapsto \{a\}^E_{\tilde{k}} \right),$$

$\sigma \rhd P \models_S \neg\phi$	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 $\text{n}(\zeta) \cap (S \cup \mathcal{K}(\sigma)) = \emptyset$ and $e(\zeta\sigma) \neq \perp$, $\sigma[\tilde{z} \mapsto \text{n}(\zeta)] \rhd P'\{e(\zeta\sigma)/u\} \models_S \phi\{T(\sigma[\tilde{z} \mapsto \text{n}(\zeta)], \zeta)/u\}$
$\sigma \rhd P \models_S \langle\bar{a}\rangle\phi$	if $a \in \mathcal{A}(\sigma)$ and there exist $\tilde{b}, M, x,$ and P' such that $x \notin \text{dom}(\sigma), \tilde{b} \cap \text{fn}(P, \sigma) = \emptyset, \tilde{b} \subseteq S, P \xrightarrow{(\nu\ \tilde{b})\bar{a}M} P',$ 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 $\lvert\text{dom}(\sigma)\rvert = n$
$\sigma \rhd P \models_S x \mapsto \{a\}^E_{\tilde{k}}$	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 $\sigma(x) = \{\text{core}(\sigma, \sigma(x))\}^E_{\tilde{k}}$, $\text{core}(\sigma, \sigma(x)) \notin \mathcal{N}$, and $\tilde{k} \subseteq \mathcal{K}(\sigma)$
$\sigma \rhd P \models_S \text{core}(x) = \text{core}(z)$	if $\text{core}(\sigma, \sigma(x)) = \text{core}(\sigma, \sigma(z))$

Table 6: The S-satisfaction relation relating configurations and formulae of $\mathcal{LM}$

where $[\alpha]\phi \stackrel{def}{=} [\tau]\phi \wedge \bigwedge_{a\in\mathcal{N},\zeta\in\Upsilon}[a\zeta]\phi \wedge \bigwedge_{a\in\mathcal{N}}[\overline{a}]\phi$ and the iterated modality $[\alpha]^i\psi$ is defined as expected by

$$\begin{aligned} [\alpha]^0\psi &= \psi \\ [\alpha]^{i+1}\psi &= [\alpha][\alpha]^i\psi \end{aligned}$$

8 Conclusions and further work

We have presented three modal logics which characterize early and late versions of the environment sensitive bisimilarity of [4]. The logics allow us to describe properties of the behaviour of a process via the use of Hennessy-Milner-style modalities and the knowledge of the environment using atomic formulae describing the bindings of an environment.

To overcome the obstacles of the definition of late bisimilarity we introduced the notion of S-environment sensitive bisimilarity where S is any set of names and a corresponding interpretation of the modal logic considered.

Although our modal logics characterize versions of environment sensitive bisimilarity they suffer from the fact we need infinite conjunction to describe an unbounded number of protocol runs. To overcome this, one can extend the logic with a fixed-point operator, obtaining a μ-calculus [7, 13].

As our results show inequivalent configurations can be distinguished by a formula in the appropriate logic. Another direction for further work is therefore to devise an algorithm for finding the simplest such distinguishing formula.

The equivalences studied in this paper are all strong. An obvious next step is therefore to devise logics that correspond to the weak, τ-abstracting notions of environment-sensitive bisimilarity [4]. We expect this extension to be straightforward.

References

[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*. Journal of Information and Computation, 148(1):1-70, 1999.

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

[5] Dolev, Danny & Yao. Andrew. *On the Security of Public Key Protocols*, Proceedings of the 22th Symposium on Foundations of Computer Science (FOCS):350-357, IEEE Computer Society Press, 1983.

[6] Durgin, Nancy & Mitchell, John & Pavlovic, Dusko. *Protocol composition and correctness*, Proceedings of Workshop on Issues in the Theory of Security.

[7] Kozen, Dexter. *Results on the propositional mu-calculus.* Theoretical Computer Science, 27(3):333-354, December 1983.

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

[9] Milner, Robin. *Communicating and Mobile Systems: the π-calculus*. Cambridge University Press, 1999.

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

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

[12] Schneier, Bruce. *Applied Cryptography*, Second edition, Wiley, 1999.

[13] Stirling, Colin P. & Bradfield, J.C. *Modal logics and mu-calculi*. In Handbook of Process Algebra, edited J. Bergstra, A. Ponse and S. Smolka, 293-332. Elsevier, North-Holland, 2001.