Relating two standard notions of secrecy *

Eugen Zălinescu, Véronique Cortier, and Michaël Rusinowitch

Loria UMR 7503 & INRIA Lorraine projet Cassis & CNRS, France

Abstract. Two styles of definitions are usually considered to express that a security protocol preserves the confidentiality of a data s. Reachability-based secrecy means that s should never be disclosed while equivalence-based secrecy states that two executions of a protocol with distinct instances for s should be indistinguishable to an attacker. Although the second formulation ensures a higher level of security and is closer to cryptographic notions of secrecy, decidability results and automatic tools have mainly focused on the first definition so far.
This paper initiates a systematic investigation of situations where syntactic secrecy entails strong secrecy. We show that in the passive case, reachability-based secrecy actually implies equivalence-based secrecy for signatures, symmetric and asymmetric encryption provided that the primitives are probabilistic. For active adversaries in the case of symmetric encryption, we provide sufficient (and rather tight) conditions on the protocol for this implication to hold.

1 Introduction

Cryptographic protocols are small programs designed to ensure secure communications. Since they are widely distributed in critical systems, their security is primordial. In particular, verification using formal methods attracted a lot of attention during this last decade. A first difficulty is to formally express the security properties that are expected. Even a basic property such as confidentiality admits two different acceptable definitions namely reachability-based (*syntactic*) secrecy and equivalence-based (*strong*) secrecy. Reachability-based secrecy is quite appealing: it says that the secret is never accessible to the adversary. For example, consider the following protocol where the agent A simply sends a secret s to an agent B, encrypted with B's public key.

$$A \rightarrow B : \{\mathtt{s}\}_{\mathrm{pub}(B)}$$

An intruder cannot deduce s, thus s is syntactically secret. Although this notion of secrecy may be sufficient in many scenarios, in others, stronger security requirements are desirable. For instance consider a setting where s is a vote and B behaves differently depending on its value. If the actions of B are observable, s remains syntactically secret but an attacker can learn the values of the

* This work appeared as the INRIA research report RR-5908 (available at http://www.inria.fr/rrrt/rr-5908.html).

INTERREG IIIC/e-Bird
Workshop "Trustworthy Software" 2006
http://drops.dagstuhl.de/opus/volltexte/2006/691

vote by watching B's actions. The design of equivalence-based secrecy is targeted at such scenarios and intuitively says that an adversary cannot observe the difference when the value of the secret changes. This definition is essential to express properties like confidentiality of a vote, of a password, or the anonymity of participants to a protocol.

Although the second formulation ensures a higher level of security and is closer to cryptographic notions of secrecy, so far decidability results and automatic tools have mainly focused on the first definition. The syntactic secrecy preservation problem is undecidable in general [12], it is co-NP-complete for a bounded number of sessions [16], and several decidable classes have been identified in the case of an unbounded number of sessions [12, 9, 7, 17, 15]. These results often come with automated tools, we mention for example ProVerif [5], CAPSL [11], and Avispa [4]. To the best of our knowledge, the only tool capable of verifying this property is the resolution-based algorithm of ProVerif [6] that has been extended to strong secrecy and only one decidability result is available [13]. In this article, Hüttel proves decidable for a fragment of the spi-calculus without recursion for framed bisimilarity, a related equivalence relation introduced by Abadi and Gordon [2].

In light of the above discussion, it may seem that the two notions of secrecy are separated by a sizable gap from both a conceptual but also from a practical point of view. These two notions have counterparts in the cryptographic setting (where messages are bitstrings and the adversary is any polynomial probabilistic Turing machine). Intuitively, the syntactic secrecy notion can be translated into a similar reachability-based secrecy notion and equivalence-based notion is close to indistinguishability. A quite surprising result [10] states that cryptographic syntactic secrecy actually implies indistinguishability in the cryptographic setting. This result relies in particular on the fact that the encryption schemes are probabilistic thus two encryptions of the same plaintext lead to different ciphertexts.

Motivated by the result of [10] and the large number of available systems for syntactic secrecy verification, we initiate in this paper a systematic investigation of situations where syntactic secrecy entails strong secrecy. Surprisingly, this happens in many interesting cases.

We offer results in both passive and active cases in the setting of the *applied pi calculus* [1]. We first treat in Section 2 the case of passive adversaries. We prove that syntactic secrecy is equivalent to strong secrecy. This holds for signatures, symmetric and asymmetric encryption. It can be easily seen that the two notions of secrecy are not equivalent in the case of deterministic encryption. Indeed, the secret $\mathtt{s}$ cannot be deduced from the encrypted message $\{\mathtt{s}\}_{\mathrm{pub}(B)}$ but if the encryption is deterministic, an intruder may try different values for $\mathtt{s}$ and check whether the ciphertext he obtained using B's public key is equal to the one he receives. Thus for our result to hold, we require that encryption is probabilistic. This is not a restriction since this is *de facto* the standard in almost all cryptographic applications. Next, we consider the more challenging case of active adversaries. We give sufficient conditions on the protocols for syn-

tactic secrecy to imply strong secrecy (Section 3). Intuitively, we require that the conditional tests are not performed directly on the secret since we have seen above that such tests provide information on the value of this secret. We again exhibit several counter-examples to motivate the introduction of our conditions. An important aspect of our result is that we do not make any assumption on the number of sessions: we put no restriction on the use of replication.

The interest of our contribution is twofold. First, conceptually, it helps to understand when the two definitions of secrecy are actually equivalent. Second, we can transfer many existing results (and the armada of automatic tools) developed for syntactic secrecy. For instance, since the syntactic secrecy problem is decidable for tagged protocols for an unbounded number of sessions [15]. By translating the tagging assumption to the applied-pi calculus, we can derive a first decidability result for strong secrecy for an unbounded number of sessions. Other decidable fragments might be derived from [12] for bounded messages (and nonces) and [3] for a bounded number of sessions.

2 Passive case

2.1 Syntax

Cryptographic primitives are represented by functional symbols. More specifically, we consider the signature $\Sigma = \{\text{enc}, \text{dec}, \text{enca}, \text{deca}, \langle\rangle, \pi_1, \pi_2, \text{sign}, \text{check}, \text{pub}, \text{priv}\}$. $\mathcal{T}(\Sigma, \mathcal{X}, \mathcal{N})$ denotes the set of terms built over Σ extended by a set of constants, the infinite set of *names* $\mathcal{N}$ and the infinite set of variables $\mathcal{X}$. A term is *closed* or *ground* if it does not contain any variable. The set of names occurring in a term m is denoted by $\text{fn}(m)$, the set of variables is denoted by $\mathcal{V}(m)$. The *positions* in a term t are defined recursively as usual (*i.e.* as sequences of positive integers), ϵ being the empty sequence. $\text{Pos}(t)$ will denote the set of positions of t and $\text{Pos}_{\text{v}}(t)$ the set of positions of variables in t. We denote by $t|_p$ the subterm of t at position p, by $u[v]_p$ the term obtained by replacing in u the subterm at position p by v. For a term u, we denote by h_u the function symbol, name or variable at position ϵ in u. We denote by $\leq_{st}$ (resp.$<_{st}$) the subterm (resp. strict) order. We may simply say that a term v *is* in a term u if v is a subterm of u. If $p = i_1.\cdots.i_n$, where $n \geq 1$, is a position then $\text{pr}(p) = i_1.\cdots.i_{n-1}$ is the *parent* position w.r.t. p. Denote by $\mathbb{N}_+^*$ the set of sequences of positive integers.

We equip the signature with an equational theory E:

$$\begin{cases} \pi_1(\langle z_1, z_2\rangle) = z_1 \\ \pi_2(\langle z_1, z_2\rangle) = z_2 \\ \text{dec}(\text{enc}(z_1, z_2, z_3), z_2) = z_1 \\ \text{deca}(\text{enca}(z_1, \text{pub}(z_2), z_3), \text{priv}(z_2)) = z_1 \\ \text{check}(z_1, \text{sign}(z_1, \text{priv}(z_2)), \text{pub}(z_2)) = \text{ok} \\ \text{retrieve}(\text{sign}(z_1, z_2)) = z_1 \end{cases}$$

The function symbols $\pi_1, \pi_2, \text{dec}, \text{deca}, \text{check}$ and retrieve are called *destructors*. Let $\mathcal{R}_E$ be the corresponding rewrite system (obtained by orienting the equations

from left to right). $\mathcal{R}_E$ is convergent. The normal form of a term t w.r.t. $\mathcal{R}_E$ is denoted by $t{\downarrow}$. Notice that E is also stable by substitution of names. As usual, we write $u \to v$ if there exists θ, a position p in u and $l \to r \in \mathcal{R}_E$ such that $u|_p = l\theta$ and $v = u[r\theta]_p$.

The symbol $\langle _, _ \rangle$ represents the pairing function and π_1 and π_2 are the associated projection functions. The term $\mathrm{enc}(m, k, r)$ represents the message m encrypted with the key k. The third argument r reflects that the encryption is probabilistic: two encryptions of the same messages under the same keys are different. The symbol dec stands for decryption. The symbols enca and deca are very similar but in an asymmetric setting, where $\mathrm{pub}(a)$ and $\mathrm{priv}(a)$ represent respectively the public and private keys of an agent a. The term $\mathrm{sign}(m, k)$ represents the signature of message m with key k. check enables to verify the signature and retrieve enables to retrieve the signed message from the signature.[1]

After the execution of a protocol, an attacker knows the messages sent on the network and also in which order they were sent. Such message sequences are organized as *frames* $\varphi = \nu\widetilde{n}.\sigma$, where $\sigma = \{{}^{m_1}/_{y_1}, \ldots, {}^{m_k}/_{y_k}\}$ is a ground substitution and $\widetilde{n}$ is a finite set of names. We denote by $\mathrm{dom}(\varphi) = \mathrm{dom}(\sigma) = \{y_1, \ldots, y_k\}$. The variables y_i enable us to refer to each message. The names in $\widetilde{n}$ are said to be *restricted*. Intuitively, these names are *a priori* unknown to the intruder. A term M is said *public* w.r.t. a frame $\nu\widetilde{n}.\sigma$ (or simply $\widetilde{n}$) if $\mathrm{fn}(M) \cap \widetilde{n} = \emptyset$. The set of restricted names $\widetilde{n}$ might be omitted when it is clear from the context. We usually write νn instead of $\nu\{n\}$, and the same for bigger sets.

2.2 Deducibility

Given a frame φ that represents the history of messages sent during the execution of a protocol, we define the *deduction* relation, denoted by $\varphi \vdash M$. Deducible messages are messages that can be obtained from φ by applying functional symbols and the equational theory E.

$$\frac{}{\nu\tilde{n}.\sigma \vdash x\sigma}\ x \in \mathrm{dom}(\sigma) \qquad \frac{}{\nu\tilde{n}.\sigma \vdash s}\ s \in \mathcal{N}\backslash\widetilde{n}$$

$$\frac{\nu\tilde{n}.\sigma \vdash t_1 \quad \cdots \quad \nu\tilde{n}.\sigma \vdash t_r}{\nu\tilde{n}.\sigma \vdash f(t_1, \ldots, t_r)} \qquad \frac{\nu\tilde{n}.\sigma \vdash t \quad t =_E t'}{\nu\tilde{n}.\sigma \vdash t'}$$

Example 1. The terms k and $\langle k, k' \rangle$ are deducible from the frame $\nu k, k', r.\{{}^{\mathrm{enc}(k,k',r)}/_x, {}^{k'}/_y\}$.

A message is usually said secret if it is not deducible. By opposition to our next notion of secrecy, we say that a term M is *syntactically secret* in φ if $\varphi \not\vdash M$.

[1] Signature schemes may disclose partial information on the signed message. To enforce the intruder capabilities, we assume that messages can always be retrieved out of the signature.

2.3 Static equivalence

Deducibility does not always suffice to express the abilities of an intruder.

Example 2. The set of deducible messages is the same for the frames $\varphi_1 = \nu k,n_0,n_1,r_0.\{^{\mathrm{enc}(n_0,k,r_0)}/_x, {}^{\langle n_0,n_1\rangle}/_y, {}^{k}/_z\}$ and $\varphi_2 = \nu k,n_0,n_1,r_1.\{^{\mathrm{enc}(n_1,k,r_1)}/_x, {}^{\langle n_0,n_1\rangle}/_y, {}^{k}/_z\}$, while an attacker is able to detect that the last message corresponds to distinct nonces. In particular, the attacker is able to distinguish the two "worlds" represented by φ_1 and φ_2.

We say that a frame $\varphi = \nu\widetilde{n}.\sigma$ *passes the test* (M, N) where M, N are two terms, denoted by $(M = N)\varphi$, if there exists a renaming of the restricted names in φ such that $(\mathrm{fn}(M) \cup \mathrm{fn}(N)) \cap \widetilde{n} = \emptyset$ and $M\sigma =_E N\sigma$. Two frames $\varphi = \nu\widetilde{n}.\sigma$ and $\varphi' = \nu\widetilde{m}.\sigma'$ are *statically equivalent*, written $\varphi \approx \varphi'$, if they pass the same tests, that is $\mathrm{dom}(\varphi) = \mathrm{dom}(\varphi')$ and for all terms M, N such that $(\mathcal{V}(M) \cup \mathcal{V}(N)) \subseteq \mathrm{dom}(\varphi)$ and $(\mathrm{fn}(M) \cup \mathrm{fn}(N)) \cap (\widetilde{n} \cup \widetilde{m}) = \emptyset$, we have $(M = N)\varphi$ iff $(M = N)\varphi'$.

Example 3. The frames φ_1 and φ_2 defined in Example 2 are not statically equivalent since $(\mathrm{dec}(x, z) = \pi_1(y))\varphi_1$ but $(\mathrm{dec}(x, z) \neq \pi_1(y))\varphi_2$.

Let $\mathtt{s}$ be a free name of a frame $\varphi = \nu\widetilde{n}.\sigma$. We say that $\mathtt{s}$ is *strongly secret* in φ if for every closed public terms M, M' w.r.t. φ, we have $\varphi({}^{M}/_{\mathtt{s}}) \approx \varphi({}^{M'}/_{\mathtt{s}})$ that is, the intruder cannot distinguish the frame instantiated by two terms of its choice. For simplicity we may omit $\mathtt{s}$ and write $\varphi(M)$ instead of $\varphi({}^{M}/_{\mathtt{s}})$.

2.4 Syntactic secrecy implies strong secrecy

Syntactic secrecy is usually weaker than strong secrecy! We first exhibit some examples of frames that preserves syntactic secrecy but not strong secrecy. They all rely on different properties.

Probabilistic encryption. The frame $\psi_1 = \nu\mathtt{s}, k, r.\{^{\mathrm{enc}(\mathtt{s},k,r)}/_x, {}^{\mathrm{enc}(n,k,r)}/_y\}$ does not preserve the strong secrecy of $\mathtt{s}$. Indeed, $\psi_1(n) \not\approx \psi_1(n')$ since $(x = y)\psi_1(n)$ but $(x \neq y)\psi_1(n')$. This would not happen if each encryption used a distinct randomness, that is, if the encryption was probabilistic.

Key position. The frame $\psi_2 = \nu\mathtt{s}, n.\{^{\mathrm{enc}(\langle n,n'\rangle,\mathtt{s},r)}/_x\}$ does not preserve the strong secrecy of $\mathtt{s}$. Indeed, $\psi_2(k) \not\approx \psi_2(k')$ since $(\pi_2(\mathrm{dec}(x, k)) = n')\psi_2(k)$ but $(\pi_2(\mathrm{dec}(x, k)) \neq n)\psi_2(k')$. If $\mathtt{s}$ occurs in key position in some ciphertext, the intruder may try to decrypt the ciphertext since $\mathtt{s}$ is replaced by public terms and check for some redundancy. It may occur that the encrypted message does not contain any verifiable part. In that case, the frame may preserve strong secrecy. It is for example the case of the frame $\nu n\{^{\mathrm{enc}(n,\mathtt{s},r)}/_x\}$. Such cases are however quite rare in practice.

No destructors. The frame $\psi_3 = \nu\mathtt{s}.\{^{\pi_1(\mathtt{s})}/_x\}$ does not preserve the strong secrecy of $\mathtt{s}$ simply because $(x = k)$ is true for $\psi_3(\langle k, k'\rangle)$ while not for $\psi_3(k)$.

Retrieve rule. The retrieve$(\mathrm{sign}(z_1, z_2)) = z_1$ may seem arbitrary since not all signature schemes enable to get the signed message out of a signature. It is actually crucial for our result. For example, the frame $\psi_4 = \nu\mathtt{s}.\{^{\mathrm{sign}(\mathtt{s},\mathrm{priv}(a))}/_x, {}^{\mathrm{pub}(a)}/_y\}$ does not preserve the strong secrecy of $\mathtt{s}$ because $(\mathrm{check}(n, x, y) = \mathrm{ok})$ is true for $\psi_4(n)$ but not for $\psi_4(n')$.

In these four cases, the frames preserve the syntactic secrecy of $\mathtt{s}$, that is $\psi_i \not\vdash \mathtt{s}$, for $1 \leq i \leq 4$.

This leads us to the following definition.

Definition 1. *A frame $\varphi = \nu\widetilde{n}.\sigma$ is* well-formed *w.r.t some name $\mathtt{s}$ if*

1. *Encryption is probabilistic, i.e. for any subterm $\mathrm{enc}(m, t, r)$ of ϕ, for any term $t' \in \phi$ and position p such that $t'|_p = r$ we have $p = q.3$ for some q and $t'|_q = \mathrm{enc}(m, t, r)$. The same condition holds for asymmetric encryption. In addition, if $\mathtt{s}$ occurs in m at a position p' such that no encryption appears along the path from the root to p' then r must be restricted, that is $r \in \widetilde{n}$.*
2. *$\mathtt{s}$ is not part of a key, i.e. for all $\mathrm{enc}(m, t, r)$, $\mathrm{enca}(m', t', r')$, $\mathrm{sign}(u, v)$, $\mathrm{pub}(w)$, $\mathrm{priv}(w')$ subterms of φ, $\mathtt{s} \notin \mathrm{fn}(t, t', v, w, w', n, n')$.*
3. *φ does not contain destructor symbols.*

Condition 1 requires that each innermost encryption above $\mathtt{s}$ contains a restricted randomness. This is not a restriction since $\mathtt{s}$ is meant to be a secret value and such encryptions have to be produced by honest agents and thus contain a restricted randomness.

For well-formed frames, syntactic secrecy is actually equivalent to strong secrecy.

Theorem 1. *Let $\varphi = \nu\widetilde{n}.\sigma$ be a well-formed frame w.r.t $\mathtt{s} \in \widetilde{n}$.*

$$\varphi \nvdash \mathtt{s} \text{ iff } \nu\widetilde{n}\backslash\{\mathtt{s}\}.\sigma({}^{M}/_{\mathtt{s}}) \approx \nu\widetilde{n}\backslash\{\mathtt{s}\}.\sigma({}^{M'}/_{\mathtt{s}})$$

for all M, M' closed public terms w.r.t. φ.

Proof. We present the skeleton of the proof; all details can be found in Appendix A. Let $\varphi = \nu\widetilde{n}.\sigma$ be a well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$. If $\varphi \vdash \mathtt{s}$, this trivially implies that $\mathtt{s}$ is not strongly secret. Indeed, there exists a public term M w.r.t. φ such that $M\sigma =_E \mathtt{s}$ (this can be easily shown by induction on the deduction system). Let n_1, n_2 be fresh names such that $n_1, n_2 \notin \widetilde{n}$ and $n_1, n_2 \notin \mathrm{fn}(\varphi)$. Since $M\sigma({}^{n_1}/_{\mathtt{s}}) =_E n_1$ the frames $\nu\widetilde{n}\backslash\{\mathtt{s}\}.\sigma({}^{n_1}/_{\mathtt{s}})$ and $\nu\widetilde{n}\backslash\{\mathtt{s}\}.\sigma({}^{n_2}/_{\mathtt{s}})$ are distinguishable with the test $(M = n_1)$.

We assume now that $\varphi \nvdash \mathtt{s}$. We first show that any syntactic equality satisfied by the frame $\varphi({}^{M}/_{\mathtt{s}})$ is already satisfied by φ.

Lemma 1. *Let $\varphi = \nu\widetilde{n}.\sigma$ be a well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$, u, v terms such that $\mathcal{V}(u), \mathcal{V}(v) \subseteq \mathrm{dom}(\varphi)$ and M a closed term, u, v and M public w.r.t. $\widetilde{n}$. If $\varphi \nvdash \mathtt{s}$, $u\sigma({}^{M}/_{\mathtt{s}}) = v\sigma({}^{M}/_{\mathtt{s}})$ implies $u\sigma = v\sigma$. Let t be a subterm of a term in σ that does not contain $\mathtt{s}$. If $\varphi \nvdash \mathtt{s}$, $t = v\sigma({}^{M}/_{\mathtt{s}})$ implies $t = v\sigma$.*

The key lemma is that any reduction that applies to a deducible term t where $\mathtt{s}$ is replaced by some M, directly applies to t.

Lemma 2. *Let $\varphi = \nu\widetilde{n}.\sigma$ be a well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$ such that $\varphi \nvdash \mathtt{s}$. Let u be a term with $\mathcal{V}(u) \subseteq \mathrm{dom}(\varphi)$ and M be a closed term in normal form, u and M public w.r.t. $\widetilde{n}$. If $u\sigma({}^{M}/_{\mathtt{s}}) \to v$, for some term v , then there exists a well-formed frame $\varphi' = \nu\widetilde{n}.\sigma'$ w.r.t. $\mathtt{s}$*

- *extending φ, that is $x\sigma' = x\sigma$ for all $x \in \mathrm{dom}(\sigma)$,*
- *preserving deducible terms: $\varphi \vdash w$ iff $\varphi' \vdash w$,*
- *and such that $v = v'\sigma'({}^{M}/_{\mathtt{s}})$ for some v' public w.r.t. $\widetilde{n}$.*

This lemma allows us to conclude the proof of Theorem 1. Fix arbitrarily two public closed terms M, M'. We can assume w.l.o.g. that M and M' are in normal form. Let $u \neq v$ be two public terms such that $\mathcal{V}(u), \mathcal{V}(v) \subseteq \mathrm{dom}(\varphi)$ and $u\sigma({}^{M}/_{\mathtt{s}}) =_E v\sigma({}^{M}/_{\mathtt{s}})$. Then there are $u_1, \ldots, u_k$ and $v_1, \ldots, v_l$ such that $u\sigma({}^{M}/_{\mathtt{s}}) \to u_1 \to \ldots \to u_k$, $v\sigma({}^{M}/_{\mathtt{s}}) \to v_1 \to \ldots \to v_l$, $u_k = u\sigma({}^{M}/_{\mathtt{s}})\downarrow$, $v_l = v\sigma({}^{M}/_{\mathtt{s}})\downarrow$ and $u_k = v_l$.

Applying repeatedly Lemma 2 we obtain that there exist public terms $u'_1, \ldots, u'_k$ and $v'_1, \ldots, v'_l$ and well-formed frames $\varphi^{u_i} = \nu\widetilde{n}.\sigma^{u_i}$, for $i \in \{1, \ldots, k\}$ and $\varphi^{v_j} = \nu\widetilde{n}.\sigma^{v_j}$, for $j \in \{1, \ldots, l\}$ (as in the lemma) such that $u_i = u'_i\sigma^{u_i}$ and $v_j = v'_j\sigma^{v_j}$.

We consider $\varphi' = \nu\widetilde{n}.\sigma'$ where $\sigma' = \sigma^{u_k} \cup \sigma^{v_l}$. Since only subterms of φ have been added to φ', it is easy to verify that φ' is still a well-formed frame and for every term w, $\varphi \vdash w$ iff $\varphi' \vdash w$. In particular $\varphi' \nvdash \mathtt{s}$.

By construction we have that $u'_k\sigma^{u_k}({}^{M}/_{\mathtt{s}}) = v'_l\sigma^{v_l}({}^{M}/_{\mathtt{s}})$. Then, by Lemma 1, we deduce that $u'_k\sigma^{u_k}(\mathtt{s}) = v'_l\sigma^{v_l}(\mathtt{s})$ that it $u\sigma =_E v\sigma$. By stability of substitution of names, we have $u\sigma({}^{M'}/_{\mathtt{s}}) =_E v\sigma({}^{M'}/_{\mathtt{s}})$. We deduce that $\nu\widetilde{n}\backslash\{\mathtt{s}\}.\sigma({}^{M}/_{\mathtt{s}}) \approx \nu\widetilde{n}\backslash\{\mathtt{s}\}.\sigma({}^{M'}/_{\mathtt{s}})$.

3 Active case

To simplify the analyze of the active case, we restrict our attention to pairing and symmetric encryption: the alphabet Σ is now reduced to $\Sigma = \{\mathrm{enc}, \mathrm{dec}, \langle\rangle, \pi_1, \pi_2\}$ and E is limited to the first three equations.

3.1 Modeling protocols within the applied pi calculus

The applied pi calculus [1] is a process algebra well-suited for modeling cryptographic protocols, generalizing the spi-calculus [2]. We shortly describe its syntax and semantics. This part is mostly borrowed from [1].

Processes, also called plain processes, are defined by the grammar:

$P, Q, R :=$ processes

$\mathbf{0}$	null process	$P \mid Q$	parallel composition
$!P$	replication	$\nu n.P$	name restriction
$if\ M = N\ then\ P\ else\ Q$	conditional	$c(z).P$	message input
$\overline{c}\langle M\rangle.P$	message output		

where n is a name, M, N are terms, and c is a name or a variable. The null process $\mathbf{0}$ does nothing. Parallel composition executes the two processes concurrently. Replication $!P$ creates unboundedly new instances of P. Name restriction $\nu n.P$ builds a new, private name n, binds it in P and then executes P. The conditional $if\ M = N\ then\ P\ else\ Q$ behaves like P or Q depending on the result of the test $M = N$. If Q is the null process then we use the notation $[M = N].P$ instead. Finally, the process $c(z).P$ inputs a message and executes P binding the variable z to the received message, while the process $\overline{c}\langle M\rangle.P$ outputs the message M and then behaves like P. We may omit P if it is $\mathbf{0}$. In what follows, we restrict our attention to the case where c is name since it is usually sufficient to model cryptographic protocols.

Extended processes are defined by the grammar:

$A, B :=$ extended processes			
P	plain process	$A \mid B$	parallel composition
$\nu n.A$	name restriction	$\nu x.A$	variable restriction
$\{^{M}/_{x}\}$	active substitution		

Active substitutions generalize *let*, in the sense that $\nu x.(\{^{M}/_{x}\}|P)$ corresponds to $let\ x = M\ in\ P$, while unrestricted, $\{^{M}/_{x}\}$ behaves like a permanent knowledge, permitting to refer globally to M by means of x. We identify variable substitutions $\{^{M_1}/_{x_1}, \ldots, {}^{M_k}/_{x_k}\}$, $k \geq 0$ with extended processes $\{^{M_1}/_{x_1}\}| \ldots |\{^{M_k}/_{x_k}\}$. In particular the empty substitution is identified with the null process.

We denote by $\mathrm{fv}(A)$, $\mathrm{bv}(A)$, $\mathrm{fn}(A)$, and $\mathrm{bn}(A)$ the sets of free and bound variables and free and bound names of A, respectively, defined inductively as usual for the pi calculus' constructs and using $\mathrm{fv}(\{^{M}/_{x}\}) = \mathrm{fv}(M) \cup \{x\}$ and $\mathrm{fn}(\{^{M}/_{x}\}) = \mathrm{fn}(M)$ for active substitutions. An extended process is *closed* if it has no free variables except those in the domain of active substitutions.

Extended processes built up from the null process (using the given constructions, that is, parallel composition, restriction and active substitutions) are called *frames*[2]. To every extended process A we associate the frame $\varphi(A)$ obtained by replacing all embedded plain processes with $\mathbf{0}$.

An *evaluation context* is an extended process with a hole not under a replication, a conditional, an input or an output.

Structural equivalence ($\equiv$) is the smallest equivalence relation on extended processes that is closed by α-conversion of names and variables, by application of evaluation contexts and such that the standard structural rules for the null process, parallel composition and restriction (such as associativity and commutativity of $|$, commutativity and binding-operator-like behavior of ν) together with the following ones hold.

$$\begin{array}{rcll} \nu x.\{^{M}/_{x}\} & \equiv & \mathbf{0} & \text{ALIAS} \\ \{^{M}/_{x}\} \mid A & \equiv & \{^{M}/_{x}\} \mid A\{^{M}/_{x}\} & \text{SUBST} \\ \{^{M}/_{x}\} & \equiv & \{^{N}/_{x}\} \quad \text{if } M =_E N & \text{REWRITE} \end{array}$$

[2] We see later in this section why we use the same name as for the notion defined in section 2.

If $\widetilde{n}$ represents the (possibly empty) set $\{n_1, \ldots, n_l\}$, we abbreviate by $\nu\widetilde{n}$ the sequence $\nu n_1.\nu n_2 \ldots \nu n_l$. Every closed extended process A can be brought to the form $\nu\widetilde{n}.\{^{M_1}/_{x_1}\}|\ldots|\{^{M_k}/_{x_k}\}|P$ by using structural equivalence, where P is a plain closed process, $k \geq 0$ and $\{\widetilde{n}\} \subseteq \cup_i \mathrm{fn}(M_i)$. Hence the two definitions of frames are equivalent up to structural equivalence on closed extended processes. To see this we apply rule SUBST until all terms are ground (this is assured by the fact that the considered extended processes are closed and the active substitutions are cycle-free). Also, another consequence is that if $A \equiv B$ then $\varphi(A) \equiv \varphi(B)$.

Two semantics can be considered for this calculus, defined by structural equivalence and by *internal reduction* and *labeled reduction*, respectively. These semantics lead to *observational equivalence* (which is standard and not recalled here) and *labeled bisimilarity* relations. The two bisimilarity relations coincide [1] and we use here the latter since it permits to take implicitly into account the observer, hence it has the advantage of relying on static equivalence rather than quantification over contexts.

Internal reduction is the largest relation on extended processes closed by structural equivalence and application of evaluation contexts such that:

$$\overline{c}\langle x\rangle.P \mid c(x).Q \rightarrow P \mid Q \qquad \text{COMM}$$

$$if\ M = M\ then\ P\ else\ Q \rightarrow P \qquad \text{THEN}$$

$$if\ M = N\ then\ P\ else\ Q \rightarrow Q \qquad \text{ELSE}$$

for any ground terms M and N such that $M \neq_E N$

On the other hand, *labeled reduction* is defined by the following rules:

$$c(x).P \xrightarrow{c(M)} P\{^M/_x\} \quad \text{IN} \qquad\qquad \overline{c}\langle u\rangle.P \xrightarrow{\overline{c}\langle u\rangle} P \quad \text{OUT-ATOM}$$

$$\frac{A \xrightarrow{\overline{c}\langle u\rangle} A'}{\nu u.A \xrightarrow{\nu u.\overline{c}\langle u\rangle} A'}\ u \neq c \quad \text{OPEN-ATOM} \qquad\qquad \frac{A \xrightarrow{\alpha} A'}{\nu u.A \xrightarrow{\alpha} \nu u.A'}\ \begin{array}{l}u \text{ does not}\\ \text{occur in } \alpha\end{array} \quad \text{SCOPE}$$

$$\frac{A \xrightarrow{\alpha} A'}{A|B \xrightarrow{\alpha} A'|B}\ (*) \quad \text{PAR} \qquad\qquad \frac{A \equiv B \quad B \xrightarrow{\alpha} B' \quad B' \equiv A'}{A \xrightarrow{\alpha} A'} \quad \text{STRUCT}$$

where u is a metavariable that ranges over names and variables, and the condition (*) of the rule PAR is $\mathrm{bv}(\alpha) \cap \mathrm{fv}(B) = \mathrm{bn}(\alpha) \cap \mathrm{fn}(B) = \emptyset$.

Definition 2. Labeled bisimilarity *($\approx_l$) is the largest symmetric relation $\mathcal{R}$ on closed extended processes such that $A\,\mathcal{R}\,B$ implies:*

1. *$\varphi(A) \approx \varphi(B)$;*
2. *if $A \rightarrow A'$ then $B \rightarrow^* B'$ and $A'\,\mathcal{R}\,B'$, for some B';*
3. *if $A \xrightarrow{\alpha} A'$ and $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(\varphi(A))$ and $\mathrm{bn}(\alpha) \cap \mathrm{fn}(B) = \emptyset$ then $B \rightarrow^* \xrightarrow{\alpha} \rightarrow^*$ B' and $A'\,\mathcal{R}\,B'$, for some B'.*

We denote $A \Rightarrow B$ if $A \rightarrow B$ or $A \xrightarrow{\alpha} B$. Also we use the notation $\nu\mathtt{s}\varphi$ for $\nu(\widetilde{n} \cup \{\mathtt{s}\}).\sigma$, where $\varphi = \nu\widetilde{n}.\sigma$.

Definition 3. *A frame φ is* valid *w.r.t. a process P if there is A such that $P \Rightarrow^* A$ and $\varphi \equiv \varphi(A)$.*

Definition 4. *Let P be a closed plain process without variables as channels and* $\mathtt{s}$ *a free name of P, but not a channel name. We say that* $\mathtt{s}$ *is* syntactically secret *in P if, for every valid frame φ w.r.t. P,* $\mathtt{s}$ *is not deducible from $\nu\mathtt{s}\varphi$. We say that* $\mathtt{s}$ *is* strongly secret *if for any closed terms M, M' such that* $\mathrm{bn}(P) \cap (\mathrm{fn}(M) \cup \mathrm{fn}(M')) = \emptyset$, $P({}^{M}/_{\mathtt{s}}) \approx_l P({}^{M'}/_{\mathtt{s}})$.

Let $\mathcal{M}_o(P)$ be the set of *outputs* of P, that is the set of terms m such that $\overline{c}\langle m\rangle$ is a message output construct for some channel name c in P, and let $\mathcal{M}_t(P)$ be the set of *operands of tests* of P, where a *test* is a couple $M = N$ occurring in a conditional and its *operands* are M and N. Let $\mathcal{M}(P) = \mathcal{M}_o(P) \cup \mathcal{M}_t(P)$ be the set of *messages* of P. Examples are provided at the end of this section.

The following lemma intuitively states that any message contained in active frame is an output instantiated by messages deduced from previous messages.

Lemma 3. *Let P be a closed plain process, and A be a closed extended process such that $P \Rightarrow^* A$. There are $k \geq 0$, an extended process $B = \nu\widetilde{n}.\sigma_k|P_B$, where P_B is some plain process, and θ a substitution public w.r.t. $\widetilde{n}$ such that: $A \equiv B$, $\{\widetilde{n}\} \subseteq \mathrm{bn}(P)$, for every side of a test or an output M of P_B there is a message M_0 in P (a side of a test or an output respectively), such that $M = M_0\theta\sigma_k$, and, $\sigma_i = \sigma_{i-1} \cup \{{}^{m_i\theta_i\sigma_{i-1}}/_{y_i}\}$, for all $1 \leq i \leq k$, where m_i is an output in P, θ_i is a substitution public w.r.t. $\widetilde{n}$ and σ_0 is the empty substitution.*

The proof is done by induction on the number of reductions in $P \Rightarrow^* A$. Intuitively, B is obtained by applying the SUBST rule (from left to right) as most as possible until there are no variables left in the plain process. Note that B is unique up to the structural rules different from ALIAS, SUBST and REWRITE. We say that $\varphi(B)$ is the *standard frame* w.r.t. A.

As a running example we consider the Yahalom protocol:

$$\begin{array}{l} A \Rightarrow B : A, N_a \\ B \Rightarrow S : B, \{A, N_a, N_b\}_{K_{bs}} \\ S \Rightarrow A : \{B, K_{ab}, N_a, N_b\}_{K_{as}}, \{A, K_{ab}\}_{K_{bs}} \\ A \Rightarrow B : \{A, K_{ab}\}_{K_{bs}} \end{array}$$

In this protocol, two participants A and B wish to establish a shared key K_{ab}. The key is created by a trusted server S which shares the secret keys K_{as} and K_{bs} with A and B respectively. The protocol is modeled by the following process:

$$P_Y(k_{ab}) = \nu k_{as}, k_{bs}.(!P_A)|(!P_B)|(!\nu k.P_S(k))|P_S(k_{ab})$$

where

$$\begin{array}{l} P_A = \nu n_a.\overline{c}\langle a, n_a\rangle.c(z_a).[b = u_b].[n_a = u_{n_a}].\overline{c}\langle \pi_2(z_a)\rangle \\ P_B = c(z_b).\nu n_b, r_b.\overline{c}\langle b, \mathrm{enc}(\langle \pi_1(z_b), \langle \pi_2(z_b), n_b\rangle\rangle, k_{bs}, r_b)\rangle.c(z'_b).[a = \pi_1(\mathrm{dec}(z'_b, k_{bs}))] \\ P_S(x) = c(z_s).\nu r_s, r'_s.\overline{c}\langle \mathrm{enc}(\langle \pi_1(z_s), \langle x, v_n\rangle\rangle, k_{as}, r_s), \mathrm{enc}(\langle v_a, x\rangle, k_{bs}, r'_s)\rangle \end{array}$$

and $u_b = \pi_1(\mathrm{dec}(\pi_1(z_a), k_{as}))$ $\quad u_{n_a} = \pi_1(\pi_2(\pi_2(\mathrm{dec}(\pi_1(z_a), k_{as}))))$
$v_a = \pi_1(\mathrm{dec}(\pi_2(z_s), k_{bs}))$ $\quad v_n = \pi_2(\mathrm{dec}(\pi_2(z_s), k_{bs}))$

For this protocol the set of outputs and operands of tests are respectively:

$$\mathcal{M}_o(P_Y) = \{\langle a, n_a\rangle, z_a, \pi_2(z_a), \langle b, \mathrm{enc}(\langle \pi_1(z_b), \langle \pi_2(z_b), n_b\rangle\rangle, k_{bs}, r_b)\rangle, z'_b, \\ \mathrm{enc}(\langle \pi_1(z_s), \langle x, v_n\rangle\rangle, k_{as}, r_s), \mathrm{enc}(\langle v_a, x\rangle, k_{bs}, r'_s)\}$$

and $\mathcal{M}_t(P_Y) = \{b, u_b, n_a, u_{n_a}, a, \pi_1(\mathrm{dec}(z'_b, k_{bs}))\}$.

3.2 Our hypotheses

In what follows, we assume $\mathtt{s}$ to be the secret. We restrict ourself to processes with ground terms in key position. Indeed, if keys contained variables, they could also contain the secret and lead to the same kind of attacks as in the passive case. For example, let $P_1 = \nu k, r, r'.(\overline{c}\langle \mathrm{enc}(\mathtt{s}, k, r)\rangle \mid c(z).\overline{c}\langle \mathrm{enc}(a, \mathrm{dec}(z, k), r')\rangle)$. The name $\mathtt{s}$ in P_1 is syntactically secret but not strongly secret. Indeed,

$$\begin{aligned} P_1 &\equiv \nu k, r, r'.(\nu z.(\{^{\mathrm{enc}(\mathtt{s},k,r)}/_z\} \mid \overline{c}\langle z\rangle \mid c(z).\overline{c}\langle \mathrm{enc}(a, \mathrm{dec}(z, k), r')\rangle)) \\ &\to \nu k, r, r'.(\{^{\mathrm{enc}(\mathtt{s},k,r)}/_z\} \mid \overline{c}\langle \mathrm{enc}(a, \mathtt{s}, r')\rangle) \qquad \text{(COMM rule)} \\ &\equiv \nu k, r, r'.(\nu z'.(\{^{\mathrm{enc}(\mathtt{s},k,r)}/_z, {}^{\mathrm{enc}(a,\mathtt{s},r')}/_{z'}\} \mid \overline{c}\langle z'\rangle)) \\ &\xrightarrow{\nu z'.\overline{c}\langle z'\rangle} \nu k, r, r'.\{^{\mathrm{enc}(\mathtt{s},k,r)}/_z, {}^{\mathrm{enc}(a,\mathtt{s},r')}/_{z'}\}, \end{aligned}$$

and the resulting frame does not preserve the strong secrecy of $\mathtt{s}$ (see the frame ψ_2 of section 2.4).

Also, as in the passive case, destructors above the secret must be forbidden. Indeed, in $P_2 = \overline{c}\langle \pi_1(\mathtt{s})\rangle \equiv \nu z.(\{^{\pi_1(\mathtt{s})}/_z\} | \overline{c}\langle z\rangle) \xrightarrow{\nu z.\overline{c}\langle z\rangle} \{^{\pi_1(\mathtt{s})}/_z\}$, $\mathtt{s}$ is syntactically secret but not strongly secret (see the frame ψ_3 of Section 2.4).

Without loss of generality with respect to cryptographic protocols, we assume that terms occurring in processes are in normal form and that no destructor appears above constructors. Indeed, terms like $\pi_1(\mathrm{enc}(m, k, r))$ are usually not used to specify protocols. We also assume that tests do not contain constructors. Indeed a test $[\langle M_1, M_2\rangle = N]$ can be rewritten as $[M_1 = N_1].[M_2 = N_2]$ if $N = \langle N_1, N_2\rangle$, and $[M_1 = \pi_1(N)].[M_2 = \pi_2(N)]$ if N does not contain constructors, and will never hold otherwise. Similar rewriting applies for encryption, except for the test $[\mathrm{enc}(M_1, M_2, M_3) = N]$ if N does not contain constructors. It can be rewritten in $[\mathrm{dec}(N, M_2) = M_1]$ but this is not equivalent. However since the randomness of encryption is not known to the agent, explicit tests on the randomness should not occur in general.

This leads us to consider the following class of processes. But first, we say that an occurrence q_{enc} of an encryption in a term t is an *agent encryptions* w.r.t. a set of names $\widetilde{n}$ if $t|_{q_{\mathrm{enc}}} = \mathrm{enc}(u, v, r)$ for some u, v, r and $r \in \widetilde{n}$.

Definition 5. *A process P is* well-formed *w.r.t. a name $\mathtt{s}$ if it is closed and if:*

1. *any occurrence of $\mathrm{enc}(m, k, r)$ in some term $t \in \mathcal{M}$ is an agent encryption w.r.t. $\mathrm{bn}(P)$, and for any term $t' \in \mathcal{M}$ and position p such that $t'|_p = r$ there is a position q such that $q.3 = p$ and $t'|_q = \mathrm{enc}(m, k, r)$;*

2. *for every term* $\mathrm{enc}(m,k,r)$ *or* $\mathrm{dec}(m,k)$ *occurring in* P*,* k *is ground;*
3. *any left or right side of a test* $M \in \mathcal{M}_t$ *is a name, a constant or has the form* $\pi^1(\mathrm{dec}(\ldots\pi^n(\mathrm{dec}(\pi^{n+1}(z),k_n))\ldots,k_1))$*, with* $n \geq 0$*, where the* π^i *are words on* $\{\pi_1,\pi_2\}$ *and* z *is a variable.*
4. *there are no destructors above constructors, nor above* $\mathtt{s}$*.*

Conditional tests should not test on $\mathtt{s}$. For example, consider the following process:

$$P_3 = \nu k,r.(\overline{c}\langle \mathrm{enc}(\mathtt{s},k,r)\rangle \mid c(z).[\mathrm{dec}(z,k)=a].\overline{c}\langle \mathrm{ok}\rangle)$$

where a is a non restricted name. $\mathtt{s}$ in P_3 is syntactically secret but not strongly secret. Indeed, $P_3 \to \nu k,r.(\{^{\mathrm{enc}(\mathtt{s},k,r)}/_z\} \mid [\mathtt{s}=a].\overline{c}\langle \mathrm{ok}\rangle)$. The process $P_3(^a/_\mathtt{s})$ reduces further while $P_3(^b/_\mathtt{s})$ does not.

That is why we have to prevent hidden tests on $\mathtt{s}$. Such tests may occur nested in equality tests. For example, let

$$\begin{aligned} P_4 = \nu k,r,r_1,r_2.(&\overline{c}\langle \mathrm{enc}(\mathtt{s},k,r)\rangle \mid \overline{c}\langle \mathrm{enc}(\mathrm{enc}(a,k',r_2),k,r_1)\rangle \\ &\mid c(z).[\mathrm{dec}(\mathrm{dec}(z,k),k')=a].\overline{c}\langle \mathrm{ok}\rangle) \\ \to P_4' = \nu k,r,r_1,r_2.(&\{^{\mathrm{enc}(\mathtt{s},k,r)}/_z\} \mid \overline{c}\langle \mathrm{enc}(\mathrm{enc}(a,k',r_2),k,r_1)\rangle \mid [\mathrm{dec}(\mathtt{s},k')=a].\overline{c}\langle \mathrm{ok}\rangle) \end{aligned}$$

Then $P_4(^{\mathrm{enc}(a,k',r')}/_\mathtt{s})$ is not equivalent to $P_4(^n/_\mathtt{s})$, since the process $P_4'(^{\mathrm{enc}(a,k',r')}/_\mathtt{s})$ emits the message ok while $P_4'(^n/_\mathtt{s})$ does not. This relies on the fact that the decryption $\mathrm{dec}(z,k)$ allows access to $\mathtt{s}$ in the test.

For the rest of the section we assume z is a new fixed variable.

To prevent hidden tests on the secret, we compute an over-approximation of the ciphertexts that may contain the secret, by marking with a symbol $\mathtt{x}$ all positions under which the secret may appear in clear.

We first introduce a function f_{ep} that extracts the least encryption over $\mathtt{s}$ and "clean" the pairing function above $\mathtt{s}$. Formally, we define the partial function

$$f_{ep}\colon \mathcal{T} \times \mathbb{N}_+^* \hookrightarrow \mathcal{T} \times \mathbb{N}_+^*$$

$f_{ep}(u,p) = (v,q)$ where v and q are defined as follows: $q \leq p$ is the position (if it exists) of the lowest encryption on the path p in u. If q does not exist or if p is not a maximal position in u, then $f_{ep}(u,p) = \perp$. Otherwise, v is obtained from $u|_q$ by replacing all arguments of pairs that are not on the path p with new variables. More precisely, q is a sequence of the form $i \cdot i_1 \cdots i_k$. We introduce two functions pair_1 and pair_2 defined as follows: $\mathsf{pair}_1(M,N) = \langle M,N\rangle$ and $\mathsf{pair}_2(M,N) = \langle N,M\rangle$. Let $v' = u|_q$. v' must be of the form $\mathrm{enc}(M_1,M_2,M_3)$ with $M_i = \mathsf{pair}_{i_1}(\ldots(\mathsf{pair}_{i_k}(a,N_{i_k}),\ldots),N_{i_1})$ for some constant or variable a and some terms N_{i_j} (remember that q leads to the lowest encryption on the path p). Then v is defined by $v = \mathrm{enc}(M_1',M_2',M_3')$ with $M_j' = M_j$ for $j \neq i$ and $M_i' = \mathsf{pair}_{i_1}(\ldots(\mathsf{pair}_{i_k}(a,x_k),\ldots),x_1)$, where the x_j are fresh variables.

For example,

$$f_{ep}(\mathrm{enc}(\mathrm{enc}(\langle\langle a,b\rangle,c\rangle,k_2,r_2),k_1,r_1),1.1.2) = (\mathrm{enc}(\langle z_{1.1},c\rangle,k_2,r_2),1).$$

The function f_e is the composition of the first projection with f_{ep}.

With the function f_{ep}, we can extract from the outputs of a protocol P the set of ciphertexts where $\mathtt{s}$ appears in clear below the encryption.

$$\mathcal{E}_0(P) = \{f_e(m[\mathtt{x}]_p, p) \mid m \in \mathcal{M}_o(P) \ \wedge \ m|_p = \mathtt{s}\}.$$

For example, $\mathcal{E}_0(P_Y) = \{\mathrm{enc}(\langle z_1, \langle \mathtt{x}, z_{1.2}\rangle\rangle, k_{as}), \mathrm{enc}(\langle z_1, \mathtt{x}\rangle, k_{bs})\}$, where P_Y is the process corresponding to the Yahalom protocol defined in previous section.

However $\mathtt{s}$ may appear in other ciphertexts later on during the execution of the protocol after decryptions and encryptions. Thus we also extract from outputs the destructor parts (which may open encryptions). Namely, we define the partial function

$$f_{dp} \colon \mathcal{T} \times \mathbb{N}_+^* \hookrightarrow \mathcal{T} \times \mathbb{N}_+^*$$

$f_{dp}(u, p) = (v, q)$ where v and q are defined as follows: $q \leq p$ is the occurrence of the highest destructor above p (if it exists). Let $r \leq p$ be the occurrence of the lowest decryption above p (if it exists). Then $v = (u[\mathrm{z}]_{r.1})|_q$. If q or r do not exist then $f_{dp}(u, p) = \perp$.

For example, $f_{dp}(\mathrm{enc}(\pi_1(\mathrm{dec}(\pi_2(y), k_1)), k_2, r_2), 1.1.1.1) = (\pi_1(\mathrm{dec}(\mathrm{z}, k_1)), 1)$

The function f_d is the composition of the first projection with f_{dp}. By applying the function f_d to messages of a well-formed process P we always obtain terms d of the form $d = d_1(\ldots d_n)$ where $d_i = \pi^i(\mathrm{dec}(\mathrm{z}, k_i))$ with $1 \leq i \leq n$, k_i are ground terms and π^i is a (possibly empty) sequence of projections $\pi_{j_1}(\pi_{j_2}(\ldots(\pi_{j_l})\ldots))$.

With the function f_d, we can extract from the outputs of a protocol P the meaningful destructor part.

$$\mathcal{D}_o(P) = \{f_d(m, p) \mid m \in \mathcal{M}_o(P) \ \wedge \ p \in \mathrm{Pos_v}(m)\}$$

For example, $\mathcal{D}_o(P_Y) = \{\pi_2(\mathrm{dec}(\mathrm{z}, k_{bs})), \pi_1(\mathrm{dec}(\mathrm{z}, k_{bs}))\}$.

We are now ready to mark (with $\mathtt{x}$) all the positions where the secret might be transmitted (thus tested). We also define inductively the sets $\mathcal{E}_i(P)$ as follows. For each element e of $\mathcal{E}_i$ we can show that there is an unique term in normal form denoted by $\overline{e}$ such that $\mathcal{V}(\overline{e}) = \{\mathrm{z}\}$ and $\overline{e}(e)\!\downarrow = \mathtt{x}$. For example, let $e_1 = \mathrm{enc}(\langle z_1, \langle \mathtt{x}, z_2\rangle\rangle, k_{as})$, then $\overline{e_1} = \pi_1(\pi_2(\mathrm{dec}(\mathrm{z}, k_{as})))$. We define

$$\begin{aligned}
\overline{\mathcal{E}_i}(P) &= \{u \mid \exists e \in \mathcal{E}_i(P), u \leq_{st} \overline{e} \ \text{ and } \exists q \in \mathrm{Pos}(u), h_{u|_q} = \mathrm{dec}\} \\
\mathcal{E}_{i+1}(P) &= \{m'[\mathtt{x}]_q \mid \exists m \in \mathcal{M}_o(P), p \in \mathrm{Pos_v}(m) \text{ s.t. } f_{ep}(m, p) = (m', p'), \\
&\qquad\qquad f_{dp}(m', p'') = (d, q), p = p'.p'', \text{ and } d_1 \in \overline{\mathcal{E}}_i(P)\}
\end{aligned}$$

For example,

$$\begin{aligned}
&\overline{\mathcal{E}_0}(P_Y) = \{\pi_1(\pi_2(\mathrm{dec}(\mathrm{z}, k_{as}))), \pi_2(\mathrm{dec}(\mathrm{z}, k_{as})), \mathrm{dec}(\mathrm{z}, k_{as}), \pi_2(\mathrm{dec}(\mathrm{z}, k_{bs})), \mathrm{dec}(\mathrm{z}, k_{bs})\} \\
&\mathcal{E}_1(P_Y) = \{\mathrm{enc}(\langle z_1, \langle z_{1.2}, \mathtt{x}\rangle\rangle, k_{as})\} \\
&\overline{\mathcal{E}_1}(P_Y) = \{\pi_2(\pi_2(\mathrm{dec}(\mathrm{z}, k_{as}))), \pi_2(\mathrm{dec}(\mathrm{z}, k_{as})), \mathrm{dec}(\mathrm{z}, k_{as})\}
\end{aligned}$$

and $\mathcal{E}_i(P_Y) = \emptyset$ for $i \geq 2$.

Fact The set $\mathcal{E}(P) = \cup_{i \geq 0} \mathcal{E}_i(P)$ is finite up-to renaming of the variables.

Proof. For every $i \geq 1$, every term $m \in \mathcal{E}_i(P)$, $\mathrm{Pos}(m)$ is included in the (finite) set of positions occurring in terms of $\mathcal{M}_0$.

We can now define an over-approximation of the set of tests that may be applied over the secret.

$$\begin{aligned}\mathcal{M}_t^{\mathtt{s}}(P) = \{M \in \mathcal{M}_t(P) \mid p \in \mathrm{Pos_v}(M) \\ \text{and } \ d = f_{dp}(M,p) \neq \bot \quad \text{and } \exists e \in \mathcal{E}, \exists i, \text{ s.t.} \\ d_i = \pi^i(\mathrm{dec(z)}, k), e = \mathrm{enc}(u,k) \text{ and } \mathtt{x} \in d_i(e)\downarrow\}\end{aligned}$$

For example, $\mathcal{M}_t^{\mathtt{s}}(P_Y) = \{\pi_1(\pi_2(\pi_2(\mathrm{dec}(\pi_1(z_a), k_{as}))))\}$.

Definition 6. *We say that a well-formed process P w.r.t.* $\mathtt{s}$ does not test over $\mathtt{s}$ *if the following conditions are satisfied:*

1. *for all $e \in \mathcal{E}(P)$, for all $d = d_1(\ldots d_n) \in \mathcal{D}_o(P)$, if $d_i = \pi^i(\mathrm{dec(z)}, k)$ and $e = \mathrm{enc}(u,k)$ and $\mathtt{x} \in d_i(e)\downarrow$ then $i = 1$ and $\overline{e} \not<_{st} d_1$*
2. *if $M = N$ or $N = M$ is a test and $M \in \mathcal{M}_t^{\mathtt{s}}(P)$ then N is a restricted name.*

Note that $\mathcal{E}(P)$ can be computed in polynomial time from P and that whether P *does not test over* $\mathtt{s}$ is decidable. We show in the next section that the first condition is sufficient to ensure that frames obtained from P are well-formed. It ensures in particular that there are no destructors right above $\mathtt{s}$. If some d_i cancels some encryption in some e and $\mathtt{x} \in d_i(e)\downarrow$ then all its destructors should reduce in the normal form computation (otherwise some destructors (namely projections from d_i) remain above $\mathtt{x}$). Also we have $i = 1$ since otherwise a d_i may have consumed the lowest encryption above $\mathtt{x}$, thus the other decryption may block, and again there would be destructors left above $\mathtt{x}$.

The second condition requires that whenever a side of a test $M = N$ is potentially dangerous (that is M or $N \in \mathcal{M}_t^{\mathtt{s}}(P)$) then the other side should be a restricted name.

3.3 Main result

We are now ready to prove that syntactic secrecy is actually equivalent to strong secrecy for protocols that are well-formed and does not test over the secret.

Theorem 2. *Let P be well-formed process w.r.t. a free name* $\mathtt{s}$*, which is not a channel name, such that P does not test over* $\mathtt{s}$*. We have $\nu\mathtt{s}\varphi \nvdash \mathtt{s}$ for any valid frame φ w.r.t. P if and only if $P({}^{M}/_{\mathtt{s}}) \approx_l P({}^{M'}/_{\mathtt{s}})$, for all ground terms M, M' public w.r.t.* $\mathrm{bn}(P)$.

Proof. Again, we only provide a sketch of the proof. Showing that strong secrecy implies syntactic secrecy is simple so we concentrate here on the converse implication. Let P be well-formed process w.r.t. a nonce $\mathtt{s}$ with no test over $\mathtt{s}$ and assume that P is syntactically secret w.r.t. $\mathtt{s}$.

Let M, M' be to public terms w.r.t. $\mathrm{bn}(P)$. To prove that $P({}^{M}/_{\mathtt{s}})$ and $P({}^{M'}/_{\mathtt{s}})$ are labeled bisimilar, we need to show that each move of $P({}^{M}/_{\mathtt{s}})$ can be matched by $P({}^{M'}/_{\mathtt{s}})$ such that the corresponding frames are bisimilar (and conversely). By hypothesis, P is syntactically secret w.r.t. $\mathtt{s}$ thus for any valid frame φ w.r.t. P, we have $\nu\mathtt{s}\varphi \nvdash \mathtt{s}$. In order to apply our previous result in the passive setting (Theorem 1), we need to show that all the valid frames are well-formed. However, frames may now contain destructors in particular if the adversary sends messages that contain destructors. Thus we first need to extend our definition of well-formedness for frames.

Definition 7. *We say that a frame $\varphi = \nu\widetilde{n}.\sigma$ is* extended well-formed *w.r.t.* $\mathtt{s}$ *if for every occurrence $q_{\mathtt{s}}$ of $\mathtt{s}$ in $t{\downarrow}$, where $t = x\sigma$ for some $x \in \mathrm{dom}(\sigma)$, there exists an agent encryption w.r.t. $\widetilde{n}$ above $\mathtt{s}$. Let $q_{\mathrm{enc}} < q_{\mathtt{s}}$ the occurrence of the lowest encryption. It must verify that $\{h_{t|_q} \mid q_{\mathrm{enc}} < q < q_{\mathtt{s}}\} \subseteq \{\langle,\rangle\}$.*

This definition ensures in particular that there is no destructor directly above $\mathtt{s}$.

Theorem 1 can easily be generalized to extended well-formed frames.

Proposition 1. *Let $\varphi = \nu(\widetilde{n} \uplus \{\mathtt{s}\}).\sigma$ be an extended well-formed frame w.r.t $\mathtt{s}$. $\varphi \nvdash \mathtt{s}$ iff $\nu\widetilde{n}.\sigma({}^{M}/_{\mathtt{s}}) \approx \nu\widetilde{n}.\sigma({}^{M'}/_{\mathtt{s}})$ for all M, M' closed public terms w.r.t. φ.*

The proof is obtained by adapting the proof of Theorem 1.

The first step of the proof of Theorem 2 is to show that any frame produced by the protocol is a extended well-formed frame. We actually prove directly a stronger result, crucial in the proof: the secret $\mathtt{s}$ always occurs under an honest encryption and this subterm is an instance of a term in $\mathcal{E}$.

Lemma 4. *Let P be a well-formed process with no test over $\mathtt{s}$ and $\varphi = \nu\widetilde{n}.\sigma$ be a valid frame w.r.t. P such that $\nu\mathtt{s}\varphi \nvdash \mathtt{s}$. Consider the corresponding standard frame $\nu\widetilde{n}.\overline{\sigma} = \nu\widetilde{n}.\{t_j \mid 1 \leq j \leq k\}$. For every occurrence $q_{\mathtt{s}}$ of $\mathtt{s}$ in $t_j{\downarrow}$, we have $f_e(t_j{\downarrow}, q_{\mathtt{s}}) = e[{}^{w}/_{\mathtt{x}}]$ for some $e \in \mathcal{E}$ and some term w. In addition $\nu\widetilde{n}.\sigma_j{\downarrow}$ is an extended well-formed frame w.r.t. $\mathtt{s}$.*

The lemma is proved by induction on j and relies deeply on the construction of the $\mathcal{E}_l$.

The second step of the proof consists in showing that any successful test in the process $P({}^{M}/_{\mathtt{s}})$ is also successful in P thus in $P({}^{M'}/_{\mathtt{s}})$.

Lemma 5. *Let P be a well-formed process with no test over $\mathtt{s}$, $\varphi = \nu\widetilde{n}.\sigma$ a valid frame for P such that $\nu\mathtt{s}\varphi \nvdash \mathtt{s}$ and θ a public substitution. If $T_1 = T_2$ is a test in P, then $T_1\theta\sigma({}^{M}/_{\mathtt{s}}) =_E T_2\theta\sigma({}^{M}/_{\mathtt{s}})$ implies $T_1\theta\sigma =_E T_2\theta\sigma$.*

This lemma is proved by case analysis, depending on whether $T_1, T_2 \in \mathcal{M}_t^{\mathtt{s}}$ and whether $\mathtt{s}$ occurs or not in $\mathrm{fn}\,(T_1\theta\sigma)$ and $\mathrm{fn}\,(T_2\theta\sigma)$.

To prove that $P({}^{M}/_{\mathtt{s}})$ and $P({}^{M'}/_{\mathtt{s}})$ are labeled bisimilar, we introduce the following relation $\mathcal{R}$ between extended processes defined as follows: $A\,\mathcal{R}\,B$ if there is an extended process A_0 and terms M, M' such that $P \Rightarrow^* A_0$, $A = A_0({}^{M}/_{\mathtt{s}})$ and $B = A_0({}^{M'}/_{\mathtt{s}})$.

Then we show that $\mathcal{R}$ satisfies the three points of the definition of labeled bisimilarity using in particular Lemma 5. Hence we have also $\mathcal{R} \subseteq \approx_l$. Since we have clearly that $P({}^{M}/_{\mathtt{s}})\,\mathcal{R}\,P({}^{M'}/_{\mathtt{s}})$, it follows that $P({}^{M}/_{\mathtt{s}}) \approx_l P({}^{M'}/_{\mathtt{s}})$.

3.4 Examples

We have seen in Section 3.2 that P_Y is a well-formed process w.r.t. k_{ab} and does not test over k_{ab}. Applying Theorem 2, if P_Y preserves the syntactic secrecy of k_{ab}, we can deduce that the Yahalom protocol preserves the strong secrecy of k_{ab} that is

$$P_Y({}^{M}/_{k_{ab}}) \approx_l P_Y({}^{M'}/_{k_{ab}})$$

for any public terms M, M' w.r.t. $\mathrm{bn}(P_Y)$. We did not formally prove that the Yahalom protocol preserves the syntactic secrecy of k_{ab} but this was done with several tools in slightly different settings (e.g.[8, 14]).

We have also verified that the Needham-Schroeder symmetric key protocol and the Wide-Mouthed-Frog protocol are both well-formed process w.r.t. k_{ab} and do not test over k_{ab}, where k_{ab} is the exchanged key. Again, the syntactic secrecy of k_{ab} has been proved by several tools (e.g. [8]) in slightly different settings for both protocols. Using Theorem 2, we can deduce that they both preserve the strong secrecy of k_{ab}.

4 Conclusion

We have shown how syntactic secrecy actually implies strong secrecy in both passive and active setting under some conditions, motivated by counterexamples.

We plan to further investigate the active case by considering in particular other primitives like asymmetric encryption and signatures and trying to relax our conditions for specific classes of protocols such as ping-pong protocols. We hope to derive in that way new decidability results for strong secrecy, based on the known ones for syntactic secrecy.

References

1. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115. ACM Press, January 2001.
2. M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: The spi calculus. In *4th ACM Conference on Computer and Communications Security (CCS'97)*, pages 36–47. ACM Press, 1997.
3. R. Amadio and D. Lugiez. On the reachability problem in cryptographic protocols. In *12th International Conference on Concurrency Theory (CONCUR'00)*, volume 1877 of *LNCS*, pages 380–394, 2000.
4. The AVISPA Project. http://www.avispa-project.org/.
5. B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Computer Security Foundations Workshop (CSFW'01)*, pages 82–96. IEEE Comp. Soc. Press, 2001.
6. B. Blanchet. Automatic Proof of Strong Secrecy for Security Protocols. In *IEEE Symposium on Security and Privacy (SP'04)*, pages 86–100, 2004.
7. B. Blanchet and A. Podelski. Verification of cryptographic protocols: Tagging enforces termination. In *Foundations of Software Science and Computation Structures (FoSSaCS'03)*, volume 2620 of *LNCS*, April 2003.

8. L. Bozga, Y. Lakhnech, and M. Périn. HERMES: An automatic tool for verification of secrecy in security protocols. In *15th Int. Conference on Computer Aided Verification (CAV'03)*, volume 2725 of *LNCS*, pages 219–222. Springer, 2003.
9. H. Comon-Lundh and V. Cortier. New decidability results for fragments of first-order logic and application to cryptographic protocols. In *International Conference on Rewriting Techniques and Applications (RTA'2003)*, LNCS 2706, pages 148–164. Springer-Verlag, 2003.
10. V. Cortier and B. Warinschi. Computationally Sound, Automated Proofs for Security Protocols. In *European Symposium on Programming (ESOP'05)*, volume 3444 of *LNCS*, pages 157–171. Springer, April 2005.
11. G. Denker, J. Millen, and H. Rueß. The CAPSL Integrated Protocol Environment. Technical Report SRI-CSL-2000-02, SRI International, Menlo Park, CA, 2000.
12. N. Durgin, P. Lincoln, J. Mitchell, and A. Scedrov. Undecidability of bounded security protocols. In *Workshop on Formal Methods and Security Protocols*, 1999.
13. H. Hüttel. Deciding framed bisimilarity. In *INFINITY'02*, August 2002.
14. L. C. Paulson. Relations between secrets: Two formal analyses of the Yahalom protocol. *Journal of Computer Security*, 9(3):197–216, 2001.
15. R. Ramanujam and S.P.Suresh. Tagging makes secrecy decidable for unbounded nonces as well. In *23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'03)*, Mumbai, 2003.
16. M. Rusinowitch and M. Turuani. Protocol Insecurity with Finite Number of Sessions and Composed Keys is NP-complete. *Theoretical Computer Science*, 299:451–475, 2003.
17. K. N. Verma, H. Seidl, and Th. Schwentick. On the complexity of equational horn clauses. In *22th International Conference on Automated Deduction (CADE 2005)*, LNCS, pages 337–352. Springer-Verlag, 2005.

A Passive case

We prove here Lemmas 1 and 2 of Section 2.

We define $\mathrm{Pos}_{\mathrm{nv}}(u) = \{p \in \mathrm{Pos}(u) \mid u|_p \notin \mathcal{V}(u)\}$ to be the set of non-variable positions of u. We also define the partial function $\mathrm{sf} : \mathbb{N}_+^* \times \mathbb{N}_+^* \hookrightarrow \mathbb{N}_+^*$, $\mathrm{sf}(p,q) = r$ if $p = q.r$ and $\mathrm{sf}(p,q) = \perp$ otherwise.

We first start by an initial lemma that states that in a well-formed frame w.r.t. $\mathtt{s}$, either every occurrence of $\mathtt{s}$ is under some encryption or $\mathtt{s}$ is deducible.

Lemma 6. *Let $\varphi = \nu\widetilde{n}.\sigma$ be a well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$ and let p be an occurrence of $\mathtt{s}$ in $y\sigma(\mathtt{s})$ for some $y \in \mathrm{dom}(\sigma)$. If $\varphi \nvdash \mathtt{s}$ then there exists a position $q < p$ such that $y\sigma(\mathtt{s})|_q$ is an encryption, that is $h_{y\sigma(\mathtt{s})|_q} \in \{\mathrm{enc}, \mathrm{enca}\}$; In addition, $\mathtt{s}$ occur in the plaintext subterm of the encrypted term, that is $q \cdot 1 \leq p$.*

Proof. Assume by contradiction that there is an occurrence of $\mathtt{s}$ such that there is no encryption above $\mathtt{s}$. Then, from Properties 2 and 3 of well-formed frames, we have that there are only pairs and signatures as function symbols above $\mathtt{s}$. Hence $\mathtt{s}$ is deducible. Thus there exists a position $q < p$ such that $y\sigma(\mathtt{s})|_q$ is an encryption. By property 2 of well-formed frames, $\mathtt{s}$ must occur in the plain-text part of the encryption that is $q \cdot 1 \leq p$.

We are now ready to prove Lemma 1.

Lemma 1. *Let $\varphi = \nu\widetilde{n}.\sigma$ be a well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$, u, v terms such that $\mathcal{V}(u), \mathcal{V}(v) \subseteq \mathrm{dom}(\varphi)$ and M a closed term, u, v and M public w.r.t. $\widetilde{n}$. If $\varphi \nvdash \mathtt{s}$, $u\sigma({}^{M}/_{\mathtt{s}}) = v\sigma({}^{M}/_{\mathtt{s}})$ implies $u\sigma = v\sigma$. Let t be a subterm of a term in σ that does not contain $\mathtt{s}$. If $\varphi \nvdash \mathtt{s}$, $t = v\sigma({}^{M}/_{\mathtt{s}})$ implies $t = v\sigma$.*

Proof. Suppose that $u\sigma({}^{M}/_{\mathtt{s}}) = v\sigma({}^{M}/_{\mathtt{s}})$ and $u\sigma(\mathtt{s}) \neq v\sigma(\mathtt{s})$. Then there is an occurrence p of $\mathtt{s}$, say in $u\sigma$, such that $v\sigma|_p \neq \mathtt{s}$. Consider the variable $y \in \mathcal{V}(u) \subseteq \mathrm{dom}(\sigma)$ and its occurrence p_y in u such that $p = p_y \cdot p'$ for some p'.

By Lemma 6, there is an encryption position q in $y\sigma(\mathtt{s})$ such that $q \cdot 1 \leq p'$. We assume q to be the innermost encryption above $\mathtt{s}$, that is q is maximal. Hence by Property 1 of well-formed frames, the term at position $q \cdot 3$ is a restricted name. It results that $p_y \cdot q \cdot 3 \notin \mathrm{Pos}_{\mathrm{nv}}(v)$, since v is public. Thus there is a variable $y' \in \mathcal{V}(v) \subseteq \mathrm{dom}(\sigma)$ at position $p_{y'}$ in v such that $p_{y'} \leq p_y \cdot q \cdot 3$. Let $m = y\sigma(\mathtt{s})$ and $m' = y'\sigma(\mathtt{s})$. Let q' such that $p_y \cdot q = p_{y'} \cdot q'$. Since $m|_{q \cdot 3} = m'|_{q' \cdot 3}$, we have, by the properties of probabilistic encryptions, that $m|_q = m'|_{q'}$. Since $p_y \cdot q = p_{y'} \cdot q'$ this means in particular that $u\sigma|_p = v\sigma|_p = \mathtt{s}$, which contradicts the fact that $v\sigma(\mathtt{s})|_p \neq \mathtt{s}$.

Let t be a subterm of a term in σ that does not contain $\mathtt{s}$. The proof that $t = v\sigma({}^{M}/_{\mathtt{s}})$ implies $t = v\sigma$ is done similarly.

We now prove key Lemma 2 of Section 2.

Lemma 2. *Let $\varphi = \nu\widetilde{n}.\sigma$ be a well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$ such that $\varphi \nvdash \mathtt{s}$. Let u be a term with $\mathcal{V}(u) \subseteq \mathrm{dom}(\varphi)$ and M be a closed term in normal form, u and M public w.r.t. $\widetilde{n}$. If $u\sigma({}^{M}/_{\mathtt{s}}) \to v$, for some term v , then there exists a well-formed frame $\varphi' = \nu\widetilde{n}.\sigma'$ w.r.t. $\mathtt{s}$*

– *extending* φ*, that is* $x\sigma' = x\sigma$ *for all* $x \in \mathrm{dom}(\sigma)$*,*
– *preserving deducible terms:* $\varphi \vdash w$ *iff* $\varphi' \vdash w$*,*
– *and such that* $v = v'\sigma'({}^{M}/_{\mathtt{s}})$ *for some* v' *public w.r.t.* $\widetilde{n}$*.*

Proof. Let u, v, M be public terms, M being closed and in normal form such that $u\sigma({}^{M}/_{\mathtt{s}}) \to v$, as in the statement of the lemma. Let $l \to r \in \mathcal{R}_E$ be the rule that was applied in the above reduction and let p be the position at which it was applied, *i.e.* $u\sigma({}^{M}/_{\mathtt{s}})|_p = l\theta$.

This position p must be in $u\sigma$ since M is in normal form. In addition, since the head function symbol of l is a destructor, by Condition 3 of well-formed frames, p must be in u.

So let $t = u|_p$. We have $t\sigma({}^{M}/_{\mathtt{s}}) = l\theta$.

Assume that there is a substitution θ_0 such that $t\sigma = l\theta_0$. This will be proved in Claim 1 below.

For our equational theory E, r is either a constant or a variable. If r is a constant then we take $v' = u[r]_p$ and $\sigma' = \sigma$. It is easy to verify that the conditions of Lemma 2 are satisfied in this case.

Suppose now that r is a variable z_0. Then, consider the[3] unique position q of z_0 in l. This position q is also in $l\theta_0$, that is, in $t\sigma$. So we can have that q is a position in t, but not in $t\sigma$, or, that q is a position in $t\sigma$, but not in t (or $t|_p$ is a variable). Hence we can have:

1. If q is a position in t, but not in $t\sigma$ (that is, there is no $y \in \mathrm{dom}(\varphi)$ above z_0) then we consider $v' = u[t|_q]_p$ and $\sigma' = \sigma$. In this case also, it is easy to verify that the conditions of the Lemma 2 are satisfied.
2. If q is a position in $t\sigma$, but not in t (that is, there is some $y \in \mathrm{dom}(\varphi)$ above z_0). Then we consider $v' = u[y']_p$ and $\sigma' = \sigma \cup \{r\theta_0/y'\}$, where $y' \notin \mathrm{dom}(\sigma)$. We have that $t\sigma =_E r\theta_0$, so $\varphi \vdash r\theta_0$. We also have that v' is public w.r.t. φ'. We have $v'\sigma' = (u[y]_p)\sigma' = u\sigma'[y\sigma']_p = u\sigma[r\theta_0]_p$. Hence $u\sigma \to v'\sigma'$.
   From $t\sigma = l\theta_0$ and $t\sigma({}^{M}/_{\mathtt{s}}) = l\theta$, we deduce that $\theta_0[{}^{M}/_{\mathtt{s}}] = \theta$, hence $r\theta_0[{}^{M}/_{\mathtt{s}}] = r\theta$. Thus $v'\sigma'({}^{M}/_{\mathtt{s}}) = u\sigma({}^{M}/_{\mathtt{s}})[r\theta]_p = v$.
   Since there is some $y \in \mathrm{dom}(\varphi)$ above z_0, we have that then $r\theta_0$ is a subterm of φ. Since φ is well-formed, we deduce that $r\theta_0$ satisfies the conditions of Definition 1. So φ' is also well-formed.

Claim 1: Let us now prove that there exists θ_0 such that $t\sigma = l\theta_0$. Otherwise we should have one of the following cases:

1. there is a position in l which is not a position in $t\sigma$;
2. there is a variable z in l having at least two occurrences, say at positions p_1, p_2, for which $t\sigma|_{p_1} \neq t\sigma|_{p_2}$.

Let us examine in detail the two cases:

1. Consider a minimal position (w.r.t. the prefix order) in l which is not a position in $t\sigma$. Then at the predecessor position an $\mathtt{s}$ occurs (since minimal

[3] For our equational theory there is exactly one occurrence of z_0 in l.

positions in l must be positions in $t\sigma({}^{M}/_{\mathtt{s}})$, but not in $t\sigma$). This position is not ϵ (*i.e.* it does not correspond to the head of l) since otherwise M would not be in normal form. Now, for all other cases, by examining all rules in $\mathcal{R}_E$, we observe that at least one of Conditions 2 or 3 of Definition 1 (of well-formed frames) is not satisfied, which contradicts the hypothesis that φ is a well-formed frame.

2. Let $t_1 = t\sigma|_{p_1}$ and $t_2 = t\sigma|_{p_2}$. We have $t_1 \neq t_2$, but $t_1({}^{M}/_{\mathtt{s}}) = t_2({}^{M}/_{\mathtt{s}})$.
   We can have the following cases, according to whether the positions p_1 and p_2 are positions of t or not:
   (a) If p_1 and p_2 are positions of t. Then we can define $w_1 = t|_{p_1}$ and $w_2 = t|_{p_2}$. We have $w_1\sigma \neq w_2\sigma$, but $w_1\sigma({}^{M}/_{\mathtt{s}}) = w_2\sigma({}^{M}/_{\mathtt{s}})$. Since w_1 and w_2 are public, the disequality is contradicted by Lemma 1.
   (b) If p_1 is not a position of t. Let p_y be the position in t such that $p_y < p_1$ and $t|_{p_y} = y$ for some $y \in \mathrm{dom}(\sigma)$.
      – A special case is when the rule $\mathrm{check}(z_1, \mathrm{sign}(z_1, \mathrm{priv}(z_2)), \mathrm{pub}(z_2)) = \mathrm{ok}$ is applied with $z = z_1$.
        Since the positions of z_1 in l are 1 and $2 \cdot 1$, and $p_y < p_1$ we have that $p_1 = 2 \cdot 1$, $p_2 = 1$ and $p_y = 2$ ($p_y = \epsilon$ implies that σ contains a destructor symbol). Hence $t\sigma|_{p_1} = y\sigma|_1$. Using the equality $\mathrm{retrieve}(\mathrm{sign}(z_1, z_2)) = z_1$ we notice that $y\sigma|_1$ is actually equal to $\mathrm{retrieve}(y\sigma)$. Considering $w_1 = t|_1$ and $w_2 = \mathrm{retrieve}(y)$, we have $w_1\sigma({}^{M}/_{\mathtt{s}}) = w_2\sigma({}^{M}/_{\mathtt{s}})$. Since w_1 and w_2 are public, this implies by Lemma 1 that $w_1\sigma = w_2\sigma$ thus $t_1 = t_2$, a contradiction.
      – Otherwise, by examining all the other cases and using the fact that φ is well-formed, we verify that $t' = t\sigma|_{p_1}$ is a subterm of σ that does not contains $\mathtt{s}$. Now either p_2 is also not a position of t, then symmetrically $t|_{p_2}$ does not contain $\mathtt{s}$ hence $t_1 = t_1({}^{M}/_{\mathtt{s}}) = t_2({}^{M}/_{\mathtt{s}}) = t_2$, a contradiction. Or p_2 is a position of t, then $t|_{p_2}$ is a public term, and the disequality is contradicted by (the second part of) Lemma 1.

B Active Case

B.1 Proof of Lemma 3

Lemma 3. *Let P be a closed plain process, and A be a closed extended process such that $P \Rightarrow^* A$. There are $k \geq 0$, an extended process $B = \nu\widetilde{n}.\sigma_k|P_B$, where P_B is some plain process, and θ a substitution public w.r.t. $\widetilde{n}$ such that: $A \equiv B$, $\{\widetilde{n}\} \subseteq \mathrm{bn}(P)$, for every side of a test or an output M of P_B there is a message M_0 in P (a side of a test or an output respectively, such that $M = M_0\theta\sigma_k$, and, $\sigma_i = \sigma_{i-1} \cup \{{}^{m_i\theta_i\sigma_{i-1}}/_{y_i}\}$, for all $i \in \{1, \ldots, k\}$, where m_i is an output in P, θ_i is a substitution public w.r.t. $\widetilde{n}$ and σ_0 is the empty substitution.*

Proof. We provide an inductive and constructive proof. We reason by induction on the number of reductions in $P \Rightarrow^* A$.

The base case is evident.

Assume that $P \Rightarrow^l A_l$ and that there are k, B_l and θ as in the statement of the lemma. Suppose that $A_l \Rightarrow A_{l+1}$ and regard what kind of reduction rule was used in this last step:

- If it is an internal reduction then, since static equivalence is closed by structural equivalence and by internal reduction (see Lemma 1 in [1]), it is sufficient to consider as searched values the same as for A_l.
- If it is a labeled reduction then we prove the following property: $\alpha \neq \overline{c}\langle x\rangle$ (for any a and x) and there is an extended process $B_{l+1} = \varphi(B_{l+1})|P_{l+1}$ such that $B_{l+1} \equiv A_{l+1}$ and
  - if $\alpha = \nu x.\overline{c}\langle x\rangle$ then $P_{l+1} = P_l$ and $\varphi(B_{l+1}) = \nu\widetilde{n}.\sigma_{k+1}$, where $\sigma_{k+1} = \sigma_k \cup \{^{M_l}/_x\}$ and M_l is an output in P_l.
  - if $\alpha = c(M)$ then $\varphi(B_{l+1}) = \varphi(B_l)$ and for every message (a side of a test or an output) M_{l+1} in P_{l+1} there is a message (a side of a test or an output, respectively) M_l in P_l, such that $M_{l+1} = M_l\theta'\sigma_k$, for some substitution θ' public w.r.t. $\nu\widetilde{n}$.
  - if $\alpha = \overline{c}\langle n\rangle$ or $\alpha = \nu n.\overline{c}\langle n\rangle$ then $P_{l+1} = P_l$, and $\varphi(B_{l+1}) = \varphi(B_l)$ or $\varphi(B_{l+1}) = \nu\{\widetilde{n}\}\backslash\{n\}.\sigma_k$, respectively.

  It is easy to see that this property is sufficient to prove the inductive step. The property can be verified, by showing, using induction on the shape of the derivation tree, that for any extended processes A', A'', B' such that $A' \xrightarrow{\alpha} A''$, $A' \equiv B'$, $B' = \nu\widetilde{n}.\sigma|Q$ there is B'' such that $A'' \equiv B''$ and $B' = \nu\widetilde{n}'.\sigma'|Q'$ where
  - if $\alpha = c(M)$ then $\widetilde{n}' = \widetilde{n}$, $\sigma' = \sigma$ and $N'' = N'\{^M/_x\}$ for each term N'' of B'' where N' is the corresponding term in B' and $c(x)$ is an input in B';
  - if $\alpha = \nu x.\overline{c}\langle x\rangle$ then $Q' = Q$, $\widetilde{n}' = \widetilde{n}$, and $\sigma' = \sigma \cup \{^M/_x\}$ where $\overline{c}\langle M\rangle$ is an input in B';
  - if $\alpha = \overline{c}\langle x\rangle$, $\alpha = \overline{c}\langle n\rangle$ or $\alpha = \nu n.\overline{c}\langle n\rangle$ then $\widetilde{n}' = \widetilde{n}$ for the first two cases, and $\{\widetilde{n}'\} = \{\widetilde{n}\}\backslash\{n\}$ for the third one, $\sigma' = \sigma$ and $Q' = Q$.

B.2 Passive case revisited

We have to generalize our result to extended well-formed frames.

Proposition 1. *Let $\varphi = \nu(\widetilde{n} \uplus \{\mathtt{s}\}).\sigma$ be an extended well-formed frame w.r.t $\mathtt{s}$. $\varphi \nvdash \mathtt{s}$ iff $\nu\widetilde{n}.\sigma(^M/_{\mathtt{s}}) \approx \nu\widetilde{n}.\sigma(^{M'}/_{\mathtt{s}})$ for all M, M' closed public terms w.r.t. φ.*

As for the proof of Theorem 1, we first proof some lemmas similar to Lemmas 1 and 2.

Lemma 7. *Let $\varphi = \nu\widetilde{n}.\sigma$ be an extended well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$. If $\varphi \nvdash \mathtt{s}$ then for all public terms u, v, M w.r.t. $\widetilde{n}$, M being ground, $u\sigma(^M/_{\mathtt{s}}) = v\sigma(^M/_{\mathtt{s}})$ implies $u\sigma = v\sigma$.*

Proof. Suppose that $u\sigma(^M/_{\mathtt{s}}) = v\sigma(^M/_{\mathtt{s}})$ and $u\sigma \neq v\sigma$. Then there is an occurrence p of $\mathtt{s}$, suppose in $u\sigma$, such that $v\sigma|_p \neq \mathtt{s}$. Consider the variable $y \in \mathcal{V}(u) \subseteq \mathrm{dom}(\sigma)$ and its occurrence p_y in u such that $p_y \leq p$. Let $p' = \mathrm{sf}(p, p_y)$.

Since φ is an extended well-formed frame, we have that there is an agent encryption at occurrence q in $y\sigma$ such that $q \leq p'$. Hence the term at position $q.3$ is a restricted name. It results that $q.3 \notin \mathrm{Pos_v}(v)$, since v is public. That is there is variable $y' \in \mathcal{V}(v) \subseteq \mathrm{dom}(\sigma)$ with the occurrence $p_{y'}$ such that $p_{y'} \leq p_y.q.3$. Let $m = y\sigma$ and $m' = y'\sigma$. Let $q' = \mathrm{sf}(p_y.q, p_{y'})$. Since $m|_{q.3} = m'|_{q'.3}$, we have, by unicity of the randomness in agent encryptions, that $m|_q = m'|_{q'}$. This means in particular that $m|_{p'} = m'|_{p''}$, where $p'' = q'.\mathrm{sf}(p', q)$. But since $m|_{p'} = \mathtt{s}$ and $p = p_{y'}.q'.\mathrm{sf}(p', q)$, this contradicts the fact that $v\sigma|_p \neq \mathtt{s}$.

The following lemma is proved similarly.

Lemma 8. *Let $\varphi = \nu\widetilde{n}.\sigma$ be an extended well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$ such that $\varphi \nvdash \mathtt{s}$, u be a subterm of a term of σ such that $\sigma \cup \{{}^{u}/_{y}\}$ is still a well-formed frame, and v be a public term w.r.t. $\widetilde{n}$. Then, for all public ground term M, $u({}^{M}/_{\mathtt{s}}) = v\sigma({}^{M}/_{\mathtt{s}})$ implies $u = v$.*

The following lemma is similar to Lemma 2.

Lemma 9. *Let $\varphi = \nu\widetilde{n}.\sigma$ be an extended well-formed frame w.r.t. $\mathtt{s} \in \widetilde{n}$ such that $\varphi \nvdash \mathtt{s}$ and u, M public terms w.r.t. $\widetilde{n}$, M being ground and in normal form. If $u\sigma({}^{M}/_{\mathtt{s}}) \to v$, then there exists an extended well-formed frame $\varphi' = \nu\widetilde{n}.\sigma'$ such that*

- $\mathrm{dom}(\sigma) \subseteq \mathrm{dom}(\sigma')$, $y\sigma' = y\sigma, \forall y \in \mathrm{dom}(\sigma)$,
- *for all term w, $\varphi \vdash w$ iff $\varphi' \vdash w$,*
- *and there exists a public term v' w.r.t. $\widetilde{n}$ such that $v = v'\sigma'$.*

Proof. Let u, v, M be terms such that $u\sigma({}^{M}/_{\mathtt{s}}) \to v$, as in the statement of the lemma. Let $l \to r \in \mathcal{R}_E$ be the rule that was applied in the above reduction and p be the position at which it was applied, i.e. $u\sigma({}^{M}/_{\mathtt{s}})|_p = l\theta$. Since M is in normal form, p must be a position of $u\sigma$.

Assume that there is a substitution θ_0 such that $u\sigma|_p = l\theta_0$. This will be proved later. Since $\varphi = \nu\widetilde{n}.\sigma$ be an extended well-formed frame, we know there is an agent encryption above $\mathtt{s}$ at position $q_{\mathrm{enc}} < p$ such that there is only pairing along the path between q_{enc} and p. We deduce that $p \in \mathrm{Pos_{nv}}(u)$. So let $t = u|_p$. We have $t\sigma({}^{M}/_{\mathtt{s}}) = l\theta$.

For our equational theory, r is a variable z_0.

Consider the[4] position q of z_0 in l. The position q is also in $l\theta_0$, that is, in $t\sigma$.

1. If q is a position in t but not in $t\sigma$ (that is, there is no y_i above z_0) then take $v' = u[t|_q]_p$ and $\sigma' = \sigma$. It is easy to verify that the conditions of the Lemma 9 are satisfied.
2. If q is a position in $t\sigma$, but not in t (that is, there is a y_i above z_0). Then take $v' = u[y]_p$ and $\sigma' = \sigma \cup \{r\theta_0/y\}$, where $y \notin \mathrm{dom}(\sigma)$. We have that $t\sigma =_E r\theta_0$, so $\varphi \vdash r\theta_0$. We also have that v' is public w.r.t. φ'.
   We have $v'\sigma' = (u[y]_p)\sigma' = u\sigma'[y\sigma']|_p = u\sigma[r\theta_0]_p$. And hence $u\sigma \to v'\sigma'$.

[4] For our equational theory there is exactly one occurrence of z_0 in l.

¿From $t\sigma = l\theta_0$ and $t\sigma(^M/_{\mathtt{s}}) = l\theta$, we deduce that $\theta_0(^M/_{\mathtt{s}}) = \theta$ hence $r\theta_0(^M/_{\mathtt{s}}) = r\theta$. Thus $v'\sigma'(^M/_{\mathtt{s}}) = u\sigma(^M/_{\mathtt{s}})[r\theta]_p = v$.
Since there is a y_i above z_0, we have that then $r\theta_0$ is a subterm of φ. Since φ is an extended well-formed frame and $\varphi \nvdash \mathtt{s}$, we deduce that $r\theta_0$ verifies the condition of well-formedness. Thus φ' is an extended well-formed frame.

Let us now prove that there exists indeed a θ_0 such that $t\sigma = l\theta_0$. Assume by contradiction that it is not the case. At least one of the following cases must occur:

1. there is a position in l which is not a position in $t\sigma$;
2. there is a variable z in l having at least two occurrences, say at positions p_1, p_2 in l, for which $t\sigma|_{p_1} \neq t\sigma|_{p_2}$.

Let us examine in detail the two cases:

1. This is in fact an impossible case. Indeed, φ is an extended well-formed frame and $\varphi \nvdash \mathtt{s}$, it must be the case that $l = \mathrm{dec}(\mathrm{enc}(z_0, z_2, z_3), z_2)$ but since there is at least one encryption above $\mathtt{s}$, all positions of l are in $t\sigma$.
2. Again, it must be the case that $l = \mathrm{dec}(\mathrm{enc}(z_0, z_2, z_3), z_2)$.
   (a) Either both p_1 and p_2 are both positions in t. Then we can consider $w_1 = t|_{p_1}$ and $w_2 = t|_{p_2}$. We have $w_1\sigma \neq w_2\sigma$, but $w_1\sigma(^M/_{\mathtt{s}}) = w_2\sigma(^M/_{\mathtt{s}})$. Since w_1 and w_2 are public, the inequality is contradicted by Lemma 7.
   (b) Or $p_1, p_2 \notin \mathrm{Pos}(t)$. Let p_y be the position in t such that $p_y < p_1$ and $t|_{p_y} = y$ for some $y \in \mathrm{dom}(\sigma(\mathtt{s}))$. applied We must have that $p_1 = 1.2$, $p_2 = 2$ and $p_y = 1$. Hence $t\sigma|_{p_1} = y\sigma|_2$, that is, it is a subterm $t|_2$ of a term of σ, and $t\sigma|_{p_2} = t|_2)\sigma$. $t|_2$ being a public term, we can apply Lemma 8 and derive a contradiction.

The proof of Proposition 1 ends like the proof of Theorem 1.

B.3 Proof of the main result

Let u, v be two terms. Define $\mathrm{Pos}(u, v) = \{p \in \mathrm{Pos}(u) \mid u|_p = v\}$.

We denote by $u \to^q v$ the reduction $u \to v$ such that $u|_q = l\theta$ and $v = u[r\theta]_q$, where q is a position in u, a rule $l \to r \in \mathcal{R}_E$, and θ is a substitution. Consider a position p in u. The function nfp_1 computes the corresponding position in v of the function symbol (or variable or name) at position p in u. Accordingly, the function nfp computes the corresponding position in $u{\downarrow}$. The function nfp^{-1} will do the opposite: to a position in $u{\downarrow}$ it associates the corresponding position in u. We say that a function symbol at position p is *consumed w.r.t. the reduction* $u \to^q v$ if $\mathrm{nfp}_1(u, p, q)$ is undefined. Similarly, we say that the same occurrence is *consumed w.r.t. the normal form* $u{\downarrow}$ if $\mathrm{nfp}(u, p)$ is undefined. We will say only that an occurrence is consumed when it is clear from the context which definition is used. Formally, we define the function $\mathrm{nfp}_1 \colon \mathcal{T} \times \mathbb{N}_+^* \times \mathbb{N}_+^* \hookrightarrow \mathbb{N}_+^*$

$$\mathrm{nfp}_1(u, p, q) = \begin{cases} p', & \text{if } u \to^q v \\ \perp, & \text{otherwise,} \end{cases}$$

where

$$p' = \begin{cases} p, & \text{if } p \not\geq q, \\ \bot, & \text{if } p \geq q \ \wedge \ p \not\geq q.q_r, \\ q.\,\mathrm{sf}(p, q.q_r), & \text{if } p \geq q.q_r, \end{cases}$$

where $l \to r$ is the rule that was applied and q_r is the position of r in l. Observe that for the equational theory E there's at most one rule that can be applied and there's exactly one occurrence of r in l. The function $\mathrm{nfp}\colon \mathcal{T} \times \mathbb{N}_+^* \hookrightarrow \mathbb{N}_+^*$ is defined by $\mathrm{nfp}(u,p) = p_k$ where $u \to^{q_1} \cdots \to^{q_k} u_k$, $u_k = u{\downarrow}$, $p_i = \mathrm{nfp}_1(u, p_{i-1}, q_i)$, for $1 \leq i \leq k$ and $p_0 = p$. The definition is correct since $\mathcal{R}_E$ is convergent. We define $\mathrm{nfp}^{-1}\colon \mathcal{T} \times \mathbb{N}_+^* \hookrightarrow \mathbb{N}_+^*$, $\mathrm{nfp}^{-1}(u,p) = p'$ iff $\mathrm{nfp}(u,p') = p$.

Lemma 4. *Let P be a well-formed process with no test over $\mathtt{s}$ and $\varphi = \nu\widetilde{n}.\sigma$ be a valid frame w.r.t. P such that $\nu\mathtt{s}\varphi \nvdash \mathtt{s}$. Consider the corresponding standard frame $\nu\widetilde{n}.\overline{\sigma} = \nu\widetilde{n}.\{t_j \mid 1 \leq j \leq k\}$. For every occurrence $q_\mathtt{s}$ of $\mathtt{s}$ in $t_j{\downarrow}$, we have $f_e(t_j{\downarrow}, q_\mathtt{s}) = e[^w/_\mathtt{x}]$ for some $e \in \mathcal{E}$ and some term w. In addition $\nu\widetilde{n}.\sigma_j{\downarrow}$ is an extended well-formed frame w.r.t. $\mathtt{s}$.*

Proof. We reason by induction on j.

Base case: $j = 1$. We have that $t_1 = m_1\theta_1$. The position $q_\mathtt{s}$ in fact a position in m_1 $\mathtt{s}$ can't appear in θ since $\mathtt{s}$ is restricted and θ is a public substitution. There must an encryption above $\mathtt{s}$ in m_1, since otherwise $\mathtt{s}$ would be deducible. Then the result follows immed iately from the properties of well-formed processes and the definition of $\mathcal{E}_0$ (take $w = \mathtt{s}$).

Inductive step. Let $p_\mathtt{s} = \mathrm{nfp}^{-1}(t_j, q_\mathtt{s})$. If $p_\mathtt{s}$ is in m_j then, as in the previous paragraph, $f_e(t_j{\downarrow}, q_\mathtt{s})[^\mathtt{x}/_\mathtt{s}] \in \mathcal{E}_0$.

Let $p_\mathtt{s} = \mathrm{nfp}^{-1}(t_j, q_\mathtt{s})$. If $p_\mathtt{s}$ is in m_j then, as in the previous paragraph, $f_e(t_j{\downarrow}, q_\mathtt{s})[^\mathtt{x}/_\mathtt{s}] \in \mathcal{E}_0$.

If $p_\mathtt{s}$ is in σ_{j-1}, then let z be the variable in m_j at position say p_z, where $p_z < p_\mathtt{s}$ and let y_{j_1} be the variable of $z\theta_j$ on the path to $p_\mathtt{s}$ at position say p_{y_1}. We have that $j_1 \leq j-1$. Let $p_\mathtt{s}^1 = \mathrm{sf}(p_\mathtt{s}, p_{y_1})$ and $q_\mathtt{s}^1 = \mathrm{nfp}(t_{j_1}, p_\mathtt{s}^1)$. By recursion hypothesis, σ_{j-1} is a well-formed frame and $f_e(t_{j_1}{\downarrow}, q_\mathtt{s}^1) = e[^w/_\mathtt{x}]$ with $e \in \mathcal{E}_l$, for some term w and some $l \geq 0$. It follows that $q_{\mathrm{enc}}^1 = \max\{\, q \in \mathrm{Pos}(t_{j_1}{\downarrow}) \mid q < q_\mathtt{s} \ \wedge \ h_{(t_{j_1}{\downarrow})|_q} = \mathrm{enc}\,\}$ exists. Let $p_{\mathrm{enc}}^1 = \mathrm{nfp}^{-1}(t_{j_1}, q_{\mathrm{enc}}^1)$.

If $p_{y_1}.p_{\mathrm{enc}}^1$ is not consumed in $t_j{\downarrow}$ then it follows that $\mathrm{nfp}(t_j, p_{y_1}.p_{\mathrm{enc}}^1)$ is the lowest encryption in $t_j{\downarrow}$ (since it corresponds to q_{enc}^1). It follows that $f_e(t_j{\downarrow}, q_\mathtt{s}) = f_e(t_{j_1}{\downarrow}, q_\mathtt{s}^1)$.

If $p_{y_1}.p_{\mathrm{enc}}^1$ is consumed in $t_j{\downarrow}$, consider the occurrence of dec in t_j, say p_{dec}, that consumes it. Since p_{enc}^1 is not consumed in $t_{j_1}{\downarrow}$ it follows that p_{dec} is in $z\theta_j$ or in m_j, and all encryptions above p_{enc}^1 in t_{j_1} are consumed in t_j. If p_{dec} is in $z\theta_j$ then all encryptions above p_{enc}^1 in t_{j_1} are consumed by decryptions that are in $z\theta_j$. This means that in $(z\theta_j\sigma_{j-1}){\downarrow}$ there's no encryption above $\mathtt{s}$, and in particular no agent encryption, which contradicts that σ_{j-1} is a encryption above extended well-formed frame. Hence p_{dec} is in m_j.

Let u, v, k, k', n be terms such that $\mathrm{dec}(u,k) = t_j|_{p_{\mathrm{dec}}}$ and $\mathrm{enc}(v,k',n) = t_j|_{p_{y_1}.p_{\mathrm{enc}}^1}$. We have that $k =_E k'$ since p_{dec} consumes $p_{y_1}.p_{\mathrm{enc}}^1$. Since p_{dec} is from

the output m_j and p^1_{enc} is also from an output being an agent encryption we have that k and k' are in normal form, hence $k = k'$. We then have $\text{dec}(u, k) \to^* \text{dec}(\text{enc}(v, k, n), k) \to^* v\downarrow$.

Let $(d, p) = f_d(m, p_z)$ and consider d_i such that the decryption p_{dec} is in d_i. Since $\mathtt{s}$ is in $t_j\downarrow$ it follows that $\mathtt{x}$ is in $d_i(e)\downarrow$. From the first condition of processes that do not test over $\mathtt{s}$ we have that $i = 1$ and $\overline{e} \not<_{st} d_1$. Since p_{dec} consumes $p_{y_1}.p^1_{\text{enc}}$, above p_{dec} in d_1 there are only projections, below enc in e there are only pairs and $\overline{e} \not<_{st} d_1$ it follows that $d_1 \leq_{st} \overline{e}$. Hence $d_1 \in \overline{\mathcal{E}}_l$.

Suppose that there is no encryption above p_{dec} in m_j. Then since d_1 is consumed and above d_1 in m_j there are only pairs, it follows that $\mathtt{s}$ is deducible from σ_j (t_j that is). Thus there is at least one encryption above p_{dec} in m_j. Let p_{enc} be the lowest decryption above p_{dec} in m_j. And let $(m', p'_{\text{enc}}) = f_{ep}(m_j, p_z)$. Then $m'[\mathtt{x}]_p \in \mathcal{E}_{l+1}$.

Since p_{enc} is not consumed in $t_j\downarrow$ and in m' all function symbols above p are not destructors we have that $f_e(t_j, p_{\mathtt{s}}) \to^* (m'[\mathtt{x}]_p)[\mathtt{x} \to d_1(f_e(\text{enc}(v, k, n), p'_{\mathtt{s}}))]$ where $p'_{\mathtt{s}} = \text{sf}(p^1_{\mathtt{s}}, p^1_{\text{enc}})$. Hence $f_e(t_j\downarrow, q_{\mathtt{s}}) = (m'[\mathtt{x}]_p)[^{w'}/_{\mathtt{x}}]$, where $w' = d_1(f_e(\text{enc}(v, k, n), p'_{\mathtt{s}})\downarrow$. That is we have the first part of the lemma.

In order to prove that $\sigma\downarrow$ is a well-formed frame we show that $m'[\mathtt{x}]_p$ and w' contain only pairs as function symbols, except for the head of $m'[\mathtt{x}]_p$ which is an encryption. We have that all function symbols, except the head in $m'[\mathtt{x}]_p$, are pairs (it follows from the definition of m'). The term w' is a subterm of $f_e(\text{enc}(v\downarrow, k, n), q'_{\mathtt{s}})$ which contains only pairs as function symbols (except for the head), since σ_{j_1} is well-formed frame.

Lemma 10. *Let P be a well-formed process with no test over $\mathtt{s}$, let $\varphi = \nu\widetilde{n}.\sigma$ a valid frame w.r.t. P such that $\varphi \nvdash \mathtt{s}$, and $T \in \mathcal{M}_t(P)$ a side of a test. Let θ a public substitution. If $T \notin \mathcal{M}^{\mathtt{s}}_t$ and $\mathtt{s} \in \text{fn}((T\theta\sigma)\downarrow)$ then $(T\theta\sigma)\downarrow = u\sigma'$ where σ' is an extended well-formed frame as in Lemma 9 and u is some term (not necessarily public).*

Proof. Suppose that $T \notin \mathcal{M}^{\mathtt{s}}_t$ and $\mathtt{s} \in \text{fn}(T\theta\sigma(\mathtt{s})\downarrow)$. Hence T is not ground and denote by z the variable of T and by p_z its position. Consider an occurrence $q_{\mathtt{s}}$ of $\mathtt{s}$ in $T\theta\sigma(\mathtt{s})\downarrow$. Denote $t_z = z\theta\sigma(\mathtt{s})\downarrow$. We then have that $\mathtt{s} \in \text{fn}(t_z)$.

Let $p_{\mathtt{s}} = \text{nfp}^{-1}(T\theta\overline{\sigma}(\mathtt{s}), q_{\mathtt{s}})$. Let y_j be the variable of $z\theta$ on the path to $p_{\mathtt{s}}$ at position say p_y, with $1 \leq j \leq k$ (see Lemma 3). Applying Lemma 4 to t_j we obtain that $f_e(t_j\downarrow, q_{\mathtt{s}}) = e[^{w}/_{\mathtt{x}}]$ with $e \in \mathcal{E}_l$, for some term w and some $l \geq 0$. Consider the lowest encryption q_{enc} in $t_j\downarrow$ above $q'_{\mathtt{s}}$, where $q'_{\mathtt{s}}$ is the corresponding positions of $q'_{\mathtt{s}}$ in $t_j\downarrow$. If this encryption is consumed then it must be consumed be a dec from T since otherwise $\mathtt{s}$ would be deducible. It follows that there is $1 \leq i \leq k$ such that $d_i = \pi^i(\text{dec}(\text{z}, k))$, where $f_d(T, p_z) = d_1(\ldots d_k)$ and $e = \text{enc}(u, k, r)$. Moreover $\mathtt{x} \in d_i(e)\downarrow$. Thus $T \in \mathcal{M}^{\mathtt{s}}_t$, but this contradicts the supposition. Hence q_{enc} is not consumed in $T\theta\sigma(\mathtt{s})\downarrow$. Then it is sufficient to consider the position $\text{nfp}^{-1}(t_j, q_{\text{enc}})$ (it is in some σ_{j_1}) in t_j in order to find the required u and σ'.

Lemma 5. *Let P be a well-formed process with no test over $\mathtt{s}$, $\varphi = \nu\widetilde{n}.\sigma$ a valid frame for P such that $\nu\mathtt{s}\varphi \nvdash \mathtt{s}$ and θ a public substitution. If $T_1 = T_2$ is a test in P, then $T_1\theta\sigma({}^{M}/_{\mathtt{s}}) =_E T_2\theta\sigma({}^{M}/_{\mathtt{s}})$ implies $T_1\theta\sigma =_E T_2\theta\sigma$.*

Proof. We say a test T is in case A, B or C if

- there is no $\mathtt{s}$ in $T\theta\sigma(\mathtt{s})\downarrow$,
- there is $\mathtt{s}$ in $T\theta\sigma(\mathtt{s})\downarrow$, $T \notin \mathcal{M}_t^{\mathtt{s}}$, or
- there is $\mathtt{s}$ in $T\theta\sigma(\mathtt{s})\downarrow$, $T \in \mathcal{M}_t^{\mathtt{s}}$, respectively.

Suppose that $T_1\theta\sigma({}^{M}/_{\mathtt{s}})\downarrow = T_2\theta\sigma({}^{M}/_{\mathtt{s}})\downarrow$ and $T_1\theta\sigma(\mathtt{s})\downarrow \neq T_2\theta\sigma(\mathtt{s})\downarrow$. We consider all possible cases T_1 and T_2 could be in:

- AA. The supposition is clearly false.
- BA, BB. By Lemma 10 we have that $(T_1\theta\sigma(\mathtt{s}))\downarrow = u\sigma'(\mathtt{s})$. Suppose there is an occurrence of $\mathtt{s}$ in $(T_1\theta\sigma(\mathtt{s}))\downarrow$ such that the term at the corresponding position in $(T_2\theta\sigma(\mathtt{s}))\downarrow$ is not $\mathtt{s}$. There is an agent encryption $\mathrm{enc}(v, w, n)$ above $\mathtt{s}$ in $(T_1\theta\sigma(\mathtt{s}))\downarrow$. The name n in $(T_2\theta\sigma(\mathtt{s}))\downarrow$ may come from $\sigma(\mathtt{s})$, from θ or from T_2. But it cannot come from T_2 (see the definition of well-formed processes), it cannot come from θ since n is restricted and θ is public, and it cannot come from σ since σ is well-formed (and hence encryption is probabilistic).
- CA, CB, CC. Since $T_1 \in \mathcal{M}_t^{\mathtt{s}}$, condition 2 of processes that do not test over $\mathtt{s}$ says that T_2 is a restricted name. Thus T_2 cannot be in cases B or C: since $\mathtt{s}$ doesn't appear in tests, T_2 should be non ground. If T_2 is in case A then there is a contradiction since T_2 should be a subterm of M but this is impossible since M is public, while T_2 is restricted.

Theorem 2. *Let P be well-formed process w.r.t. a free name $\mathtt{s}$, which is not a channel name, such that P does not test over $\mathtt{s}$. We have $\nu\mathtt{s}\varphi \nvdash \mathtt{s}$ for any valid frame φ w.r.t. P if and only if $P({}^{M}/_{\mathtt{s}}) \approx_l P({}^{M'}/_{\mathtt{s}})$, for all ground terms M, M' public w.r.t.* $\mathrm{bn}(P)$.

Proof. Consider the relation $\mathcal{R}$ between extended processes defined as follows: $A\,\mathcal{R}\,B$ if there is an extended process $A_0(\mathtt{s})$ such that $P(\mathtt{s}) \Rightarrow^* A_0(\mathtt{s})$ and ground terms M, M' public w.r.t. $\nu(\widetilde{n} \cup \{\mathtt{s}\})$ such that $A = A_0({}^{M}/_{\mathtt{s}})$ and $B = A_0({}^{M'}/_{\mathtt{s}})$.

We show that $\mathcal{R}$ satisfies the three points of the definition of labeled bisimilarity. Suppose $A\,\mathcal{R}\,B$, that is $A_0({}^{M}/_{\mathtt{s}})\,\mathcal{R}\,A_0({}^{M'}/_{\mathtt{s}})$ for some A_0, M, M' as above. In what follows we write $X(t)$ for $X({}^{t}/_{\mathtt{s}})$, where X ranges over processes and frames and t is M or M'. We prove that the following questions have affirmative answer:

1. $\varphi(A_0(M)) \approx \varphi(A_0(M'))$? We know that $\varphi(A_0(\mathtt{s}))$ is a valid frame (from the definition of $\mathcal{R}$), hence $\varphi(A_0(\mathtt{s})) \nvdash \mathtt{s}$ (from the hypothesis). Let $\varphi'(\mathtt{s}) \equiv \varphi(A_0(\mathtt{s}))$ having only ground and normalized terms. Then, by Lemma 4, we have that $\varphi'(\mathtt{s})$ is an extended well-formed frame. We can then use Proposition 1 to obtain that $\varphi(A_0(M)) \approx \varphi(A_0(M'))$, since we have $\varphi(A_0(M)) = \varphi(A_0(\mathtt{s}))(M)$ (and the same for M').

2. if $A_0(M) \to A'$ then $A' \equiv A'_0(M)$, $A_0(M') \to A'_0(M')$ and $A'_0(M)\,\mathcal{R}\,A'_0(M')$, for some A'_0? We distinguish two cases, according to whether the used rule was the COMM rule or one of the THEN and ELSE rules:
   - if the COMM rule was used then $A_0(M) \equiv C(M)[\overline{c}\langle z\rangle.Q(M)|c(z).R(M)]$, where C is an evaluation context and $A' = C(M)[Q(M)|R(M)]$. Then $A_0(\mathtt{s}) \equiv C(\mathtt{s})[\overline{c}\langle z\rangle.$
     $Q(\mathtt{s})|c(z).R(\mathtt{s})]$. Take $A'_0(\mathtt{s}) = C(\mathtt{s})[Q(\mathtt{s})|R(\mathtt{s})]$. We have that $P(\mathtt{s}) \Rightarrow^* A'_0(\mathtt{s})$ and so, by definition of $\mathcal{R}$, we have that $A'_0(M)\,\mathcal{R}\,A'_0(M')$.
   - otherwise, $A_0(M) \equiv C(M)[\text{if } T'(M) = T''(M) \text{ then } Q(M) \text{ else } R(M)]$. Then $A_0(\mathtt{s}) \equiv C(\mathtt{s})[\text{if } T'(\mathtt{s}) = T''(\mathtt{s}) \text{ then } Q(\mathtt{s}) \text{ else } R(\mathtt{s})]$. From Lemma 3 we know that $T'(\mathtt{s}) = T'_0\theta\sigma(\mathtt{s})$ and $T''(\mathtt{s}) = T''_0\theta\sigma(\mathtt{s})$, where $T'_0 = T''_0$ is a test in P and $\nu\widetilde{n}.\sigma \equiv \varphi(A_0(\mathtt{s}))$ is the standard frame w.r.t. $A_0(\mathtt{s})$. Take $A'_0(\mathtt{s}) = C(\mathtt{s})[Q(\mathtt{s})]$ if $T'_0\theta\sigma(\mathtt{s}) =_E T''_0\theta\sigma(\mathtt{s})$ and $A'_0(\mathtt{s}) = C(\mathtt{s})[R(\mathtt{s})]$ otherwise. From Lemma 5 we have that $T'_0\theta\sigma(\mathtt{s}) =_E T''_0\theta\sigma(\mathtt{s})$ iff $T'_0\theta\sigma(M) =_E T''_0\theta\sigma(M)$. Hence $A_0(M) \to A'_0(M)$, $A_0(M') \to A'_0(M')$ and $A_0(\mathtt{s}) \to A'_0(\mathtt{s})$. And we also have $A'_0(M)\,\mathcal{R}\,A'_0(M')$ from the definition of $\mathcal{R}$.
3. if $A_0(M) \xrightarrow{\alpha} A'$ and $\mathrm{fv}(\alpha) \subseteq \mathrm{dom}(\varphi(A_0(M)))$ and $\mathrm{bn}(\alpha) \cap \mathrm{fn}(A_0(M')) = \emptyset$ then $A' \equiv A'_0(M)$, $A_0(M') \xrightarrow{\alpha} A'_0(M')$ and $A'_0(M)\,\mathcal{R}\,A'_0(M')$, for some A'_0? According to the form of α, we consider the following cases:
   - $\alpha = c(T)$. Suppose $A_0(M) \equiv C(M)[c(z).Q(M)]$. Then take $A'_0(\mathtt{s}) = C(\mathtt{s})[Q(\mathtt{s})$
     $\{^T/_z\}]$.
   - $\alpha = \overline{c}\langle u\rangle$. Suppose $A_0(M) \equiv C(M)[\overline{c}\langle u\rangle.Q(M)]$. Then take $A'_0(\mathtt{s}) = C(\mathtt{s})[Q(\mathtt{s})]$.
   - $\alpha = \nu u.\overline{c}\langle u\rangle$. Suppose $A_0(M) \equiv C(M)[\nu u.A_1(M)]$, where $A_1(M) \xrightarrow{\overline{c}\langle u\rangle} A'_1(M)$. Then take $A'_0(\mathtt{s}) = C(\mathtt{s})[A_1(\mathtt{s})]$.

The above discussion proves that $\mathcal{R} \subseteq \approx_l$. Since we have clearly that $P(^M/_{\mathtt{s}})\,\mathcal{R}\,P(^{M'}/_{\mathtt{s}})$, it follows that $P(^M/_{\mathtt{s}}) \approx_l P(^{M'}/_{\mathtt{s}})$.

C Examples

For sake of simplicity, we may omit the symbol $\langle,\rangle$ for pairing. In that case, we assume a right priority that is $a, b, c = \langle\langle a, b\rangle, c\rangle$.

C.1 Needham-Schroeder symmetric key protocol

The protocol is described below:

$$\begin{array}{l} A \Rightarrow S : A, B, N_a \\ S \Rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}} \\ A \Rightarrow B : \{K_{ab}, A\}_{K_{bs}} \end{array}$$

Our target secret is K_{ab}.

The corresponding process is:

$$P_{NS}(k_{ab}) = \nu k_{as}.\nu k_{bs}.(!A)|(!c(z_b))|(!\nu k.S(k))|S(k_{ab})$$

where

$$\begin{aligned} A = \nu n_a.\overline{c}\langle a, b, n_a\rangle.c(z_a).[\pi_1(\mathrm{dec}(z_a, k_{as})) = n_a]. \\ [\pi_1(\pi_2(\mathrm{dec}(z_a, k_{as}))) = b].\overline{c}\langle \pi_2(\pi_2(\pi_2(\mathrm{dec}(z_a, k_{as}))))\rangle \\ S(x) = c(z_s).\nu r, r'.\overline{c}\langle \mathrm{enc}(\langle \pi_2(\pi_2(z_s)), \pi_1(\pi_2(z_s)), k_{ab}, \\ \mathrm{enc}(\langle x, \pi_1(z_s)\rangle, k_{bs}, r')\rangle, k_{as}, r)\rangle \end{aligned}$$

Note that other processes should be added to considered corrupted agents or roles A, B and S talking to other agents but this would not really change the following sets of messages.

The output messages are:

$$\mathcal{M}_o = \left\{ \begin{array}{l} a, b, n_a \\ \pi_2(\pi_2(\pi_2(\mathrm{dec}(z_a, k_{as})))) \\ \mathrm{enc}(\langle \pi_2(\pi_2(z_s)), \pi_1(\pi_2(z_s)), \\ k_{ab}, \mathrm{enc}(\langle k_{ab}, \pi_1(z_s)\rangle, k_{bs}, r')\rangle, k_{as}, r) \end{array} \right\}$$

The tests are:

$$\left\{ \begin{array}{l} \pi_1(\mathrm{dec}(z_a, k_{as})) = n_a \\ \pi_1(\pi_2(\mathrm{dec}(z_a, k_{as}))) = b \end{array} \right\}$$

We define $\max \overline{\mathcal{E}_i} = \{\overline{e} \mid e \in \mathcal{E}_i\}$ in order to increase readability, and since it is easy to deduce $\overline{\mathcal{E}_i}$ from $\max \overline{\mathcal{E}_i}$.

$$\mathcal{D}_o = \{\pi_2(\pi_2(\pi_2(\mathrm{dec}(z, k_{as}))))\}$$

$$\mathcal{E}_0 = \{\mathrm{enc}(\langle z_1, \langle z_2, \langle \mathtt{x}, z_3\rangle\rangle\rangle, k_{as}, r), \mathrm{enc}(\langle \mathtt{x}, z_4\rangle, k_{bs}, r')\}$$

$$\max \overline{\mathcal{E}}_0 = \{\pi_1(\pi_2(\pi_2(\mathrm{dec}(z, k_{as})))), \pi_1(\mathrm{dec}(z, k_{bs}))\}$$

$$\mathcal{D}_o \cap \overline{\mathcal{E}}_0 = \emptyset$$

$$\mathcal{M}_t^{k_{ab}} = \emptyset$$

We deduce that P_{NS} is a well-formed process w.r.t. k_{ab}. Applying Theorem 2 and since the Needham-Schroeder symmetric key protocol preserves the syntactic secrecy of k_{ab}, we deduce that the protocol preserves the strong secrecy of k_{ab} that is

$$P_{NS}({}^{M}/_{k_{ab}}) \approx_l P_{NS}({}^{M'}/_{k_{ab}})$$

for any public terms M, M' w.r.t. $\mathrm{bn}(P_{NS})$.

C.2 Wide Mouthed Frog Protocol (modified)

The protocol is described below:

$$\begin{array}{l} A \Rightarrow B : N_a \\ B \Rightarrow S : \{N_a, A, K_{ab}\}_{K_{bs}} \\ S \Rightarrow A : \{N_a, B, K_{ab}\}_{K_{as}} \end{array}$$

Again, the target secret is K_{ab}.

The corresponding process is:

$$P_{NS}(k_{ab}) = \nu k_{as}.\nu k_{bs}.(!A)|(!S)|(!\nu k.B(k))|B(k_{ab})$$

where

$$\begin{aligned} A &= \nu n_a.\overline{c}\langle n_a\rangle.c(z_a).[\pi_1(\mathrm{dec}(z_a, k_{as})) = n_a] \\ B(x) &= c(z_b).\nu r.\overline{c}\langle \mathrm{enc}(\langle z_b, a, x\rangle, k_{bs}, r)\rangle \\ S &= c(z_s).[\pi_1(\pi_2(\mathrm{dec}(z_s, k_{bs}))) = a]. \\ &\qquad \nu r'.\overline{c}\langle \mathrm{enc}(\langle \pi_1(\mathrm{dec}(z_s, k_{bs})), b, \pi_2(\pi_2(\mathrm{dec}(z_s, k_{bs})))\rangle, k_{as}, r')\rangle \end{aligned}$$

Note that other processes should be added to considered corrupted agents or roles A, B and S talking to other agents but this would not really change the following sets of messages.

The output messages are:

$$\mathcal{M}_o = \left\{ \begin{array}{l} n_a \\ \mathrm{enc}(\langle z_b, a, k_{ab}\rangle, k_{bs}, r) \\ \mathrm{enc}(\langle \pi_1(\mathrm{dec}(z_s, k_{bs})), b, \\ \pi_2(\pi_2(\mathrm{dec}(z_s, k_{bs})))\rangle, k_{as}, r') \end{array} \right\}$$

The tests are:

$$\left\{ \begin{array}{l} \pi_1(\mathrm{dec}(z_a, k_{as})) = n_a \\ \pi_1(\pi_2(\mathrm{dec}(z_s, k_{bs}))) = a \end{array} \right\}$$

$$\mathcal{D}_o = \{\pi_1(\mathrm{dec}(z, k_{bs})), \pi_2(\pi_2(\mathrm{dec}(z, k_{bs})))\}$$

$$\mathcal{E}_0 = \{\mathrm{enc}(\langle z_1, \langle z_2, \mathtt{x}\rangle, k_{bs}, r)\rangle\}$$

$$\max \overline{\mathcal{E}}_0 = \{\pi_2(\pi_2(\mathrm{dec}(z, k_{bs})))\}$$

$$\mathcal{E}_1 = \{\mathrm{enc}(\langle z_1, \langle z_2, \mathtt{x}\rangle, k_{as}, r)\rangle\}$$

$$\max \overline{\mathcal{E}}_1 = \{\pi_2(\pi_2(\mathrm{dec}(z, k_{as})))\}$$

$$\mathcal{D}_o \cap \overline{\mathcal{E}}_1 = \emptyset$$

$$\mathcal{M}_t^{k_{ab}} = \emptyset$$

We obtain similarly the same conclusion as for the previous protocol.