Secure composition of PKIs with public key protocols

Vincent Cheval[1], Véronique Cortier[1], and Bogdan Warinschi[2]

[1] LORIA, CNRS & INRIA, France
[2] University of Bristol, United Kingdom

Abstract. We use symbolic formal models to study the composition of public key-based protocols with public key infrastructures (PKIs). We put forth a minimal set of requirements which a PKI should satisfy and then identify several reasons why composition may fail. Our main results are positive and offer various trade-offs which align the guarantees provided by the PKI with those required by the analysis of protocol with which they are composed. We consider both the case of ideally distributed keys but also the case of more realistic PKIs. Our theorems are broadly applicable. Protocols are not limited to specific primitives and compositionality asks only for minimal requirements on shared ones. Secure composition holds with respect to arbitrary trace properties that can be specified within a reasonably powerful logic. For instance, secrecy and various forms of authentication can be expressed in this logic. Finally, our results alleviate the common yet demanding assumption that protocols are fully tagged. *Keywords:* secure composition, PKI, protocol analysis

1 Introduction

Modular analysis of cryptographic systems is an area of permanent concern in security research. Composition results are set either in the symbolic model (e.g. [19,16,17,6,27,22,14,2]) or in the computational model (e.g. [12,28,13,24,23,11,9,10]). Some of these results yield general frameworks where arbitrary components can be safely combined but, unsurprisingly, rely on particularly strong hypothesis. Other results provide narrower composition theorems tailored to specific cryptographic tasks but afford more relax and practical assumptions on the components.

This paper falls within the latter research direction. We study the composition of protocols for establishing public key infrastructures (PKIs) with arbitrary other protocols which require such keys. For two parties the question we adress is (using ad-hoc notation): when can a PKI protocol $P = P_1 \mid P_2$ that distributes public (and secret) keys be composed with a protocol $Q = Q_1 \mid Q_2$ that uses these keys. We are after a theorem which (using informal notation) guarantees that

$$P_1 \mid P_2 \models \phi_{\mathsf{PKI}} \quad \Rightarrow \quad P_1.Q_1 \mid P_2.Q_2 \models \mathsf{secrecy}(s)$$

provided that

$$Q_1(sk_A, \mathsf{pk}(sk_B)) \mid Q_2(sk_B, \mathsf{pk}(sk_A)) \models \mathsf{secrecy}(s)$$

That is, a secure PKI infrastructure P (as captured by some security property ϕ_{PKI}) can be safely used by a protocol Q provided that Q is secure (preserve the secrecy of some piece of data s) when analyzed with honestly generated keys. In the above theorem, think of P_1 as the PKI component which provides the secret key to user A and informs him of the public key of user B; protocol P_2 plays the converse role for user B.

This type of composition result is often simply assumed! For example, it is quite common for the analysis of protocols that use public keys to rely on the assumption that prior to their execution the PKI keys have been generated, distributed to all parties, and that the link between the identities of parties and their public keys is known to everyone. This convenient idealization of key distribution is often adopted by analysis via automatic tools (e.g. ProVerif[5], Scyther [18], Avispa [3], or Tamarin [26]) and reflects compelling inuition: PKI infrastructures (such as X.509) are designed to distribute and certify keys, *independently* of the protocols that will use such keys. This intuition is not supported by rigorous underpinnings and it may actually be wrong since the guarantees provided by the PKI are not always aligned with those assumed by the subsequent

protocol. For example, PKIs do not guarantee that a malicious party registers the same key with different registration authorities (so the same user may have two different public keys), do not guarantee that different users do not share the key or, more generally, that each user has followed honestly the registration process. In fact, it is not clear even what minimal guarantees for a PKI can still ensure a composition result.

There has been relatively little research on the problem of secure composition of PKIs with other protocols and, interestingly, most work is set within computational model (see related work). In this paper we approach the problem using symbolic models. As we discuss later, the higher level of abstraction yields results of broader applicability. Moreover, our results are relevant for proofs that use automated tools since they usually work on top of some symbolic model.

In a nutshell, our results are as following. We reconfirm that the mismatch between assumptions made in the analysis of Q and the guarantees offered by some PKI protocols P leads to insecure composition. Our main results are then rigorous composition theorem which carefully account for the mismatch between what is assumed and what is guaranteed. Below we highlight the main features of our work.

The perils of Idealized key distribution. At a high level the theorem we are after may fail because of implicit assumptions that underly the analysis of Q. As explained above, the assumption is usually that the keys of parties have been honestly generated and are in place before the execution of Q. For a variety of reasons, this assumption does not hold when keys are managed by a real PKI. For example, when parties generate their own secret/public keys and have them certified (e.g. the Verisign process for issuing certificates), keys are not necessarily honestly generated. Other causes include "confusion" of messages between the protocol for key registration and subsequent protocols that use these keys (which makes standalone analysis incomplete) as well as the classic message parsing errors. In Section 2 we illustrate through concrete counterexamples several obstacles which need to be carefully accounted for by any generic composition theorem.

Composition of PKIs with arbitrary protocols. The counterexamples that we identify inform our main results. We provide sufficient conditions to ensure that a protocol for distributing public keys P composes securely with a protocol Q which uses these keys, in the sense that the desired security properties of Q are guaranteed.

Our first theorem imposes only minimal requirements on P. These are formalized by formula ϕ_{PKI} (in a logic on traces which we provide) and demand that secret keys stay secret, that all parties have a consistent view of the public keys of *honest* parties, and that honest parties use distinct keys for signing and decryption. We emphasize that ϕ_{PKI} provides no guarantees on the keys held by dishonest parties. This weaker guarantees on the keys distributed by P translates into a correspondingly stronger requirement on Q. Its security needs to hold under a *permissive* key assignment (which only reflects the guarantees offered by ϕ_{PKI}). We refer to this version of Q as "permissive" Q.

In symbolic models, protocols are however never analyzed in their "permissive" form, but rather in the "ideal" form where all keys (including those of dishonest parties) are honestly generated and already predistributed. In this case the above theorem does not apply (and in fact we give counterexample protocols that shows that composition with realistic PKIs fails). Our next theorem recovers a composition result for such protocols, at the expense of stronger requirements on the PKI: we strengthen the assumption on P to require that besides ϕ_{PKI} it also satisfies ϕ_{ideal}. This additional assumption essentially asks that all honest users have a consistent view of the keys for encryption and verification that belong to other users, that keys of distinct agents are pairwise distinct and that encryption and verification keys are also distinct.

Our theorems share several features. First, they treat the properties of Q in a generic way. Composition preserves *any trace-based security property* which can be specified by a formula in a logic which we provide. In particular, (weak) secrecy and various forms of authentication properties can be specified in the logic.

Our theorems are rather *agnostic to the class of protocols* themselves. We consider arbitrary classes of protocols (possibly with else branches) which employ arbitrary cryptographic primitives (including e.g. Exclusive Or or Diffie-Hellman). While we require the minimal condition that P

and Q do not share underspecified primitives we do permit that they both use standard ones (encryption, signatures, hashes, ...).

Sharing primitives between protocols leads to well-known difficulties due to cross-protocol attacks. The traditional solution is to assume that each use of these primitives is "tagged" [17,16,2]. This convenient technique helps to easily distinguish between messages of different protocols but is not supported by current practice. Our theorems show how one may *avoid full tagging of primitives*. We propose a more general property that avoids cross-protocol attacks. This property can be enforced by tagging mechanism but also through alternative restrictions on the protocols, e.g. that P and Q employ shared functions but always under different keys or by minimal tagging assumptions (e.g. that only occurrences of public keys, and not each individual use of the primitives are tagged). For example, a PKI protocol P may use the same signature (resp. encryption) scheme as Q provided that keys shared from P to Q are either used to sign (resp. encrypt) in P or Q but not both.

A convenient specification language. Our results are set within a symbolic model similar to those that underlie existing automated tools. It turns out that existing symbolic formalisms (e.g. those close to the applied pi-calculus [1]) are not convenient to specify scenarios like those we treat in this paper. For example, in the applied-pi calculus, it is surprisingly difficult to express persistent storage e.g. of a trusted server of symmetric keys shared by unbounded number of pairs of agents. Modeling such a server requires a heavy encoding using private channels. Tools like ProVerif bypass this encoding by extending their calculus to include tables. The problem is that the notion of "agent" is captured implicitly in existing calculi and this makes it difficult to reason in a simple manner about composition.

We design a new specification language. The main feature is a notion of parameterized agents and names which allows to conveniently talk about the different sessions of protocols that share the same parameters. For example, we can elegantly express that a server shares a symmetric key K_{AS} with any agent A by writing $k[A, S]$. Then one server talking to infinitely many agents can be simply described by a process of the form

$$!^i\, R_1(k[S, A[i]]) \mid R_2(k[S, A[i]])$$

where R_1 and R_2 represent respectively the role of the server and the agent.

Related work. Our work uses and extends techniques used in other existing composition result set withing symbolic models, and is close in scope with some recent works on the composition of PKIs that rely on computational models.

Relevant composition results within symbolic models include [17] which characterizes when two protocols run in parallel may share keys and [16] which studies what is a good key establishment protocol and how it can be used. These early works hold for trace properties. More recent results establish similar results in the context of equivalence properties, useful to model privacy properties [15,2]. In [27,22,14], the authors study "vertical composition": when a protocol Q uses some secure, authenticated, or confidential channel, how such a channel can be securely realized? In contrast, our paper focuses here on PKI and studies what are the properties of a good PKI and how it can be used. Our proof techniques borrow from [2,14]. However, in addition to considering a different type of composition (PKI), we establish the first composition result that does not require an explicit tagging scheme. In other words, we can now compose actual protocols instead of composing their tagged version. To establish such a general result, we had to considerably reshape the proofs developed e.g. in [2] or [14].

In the computational model there are several generic frameworks for compositional analysis [12,28,23,11] all sharing the same underlying philosophy: components can be designed separately, yet their security is preserved when the components are used together, so composability comes somehow for free. The strength of this level of security also means that it may be difficult to achieve. Indeed, for public key infrastructures the model for PKI as introduced by Barak et al. [4] and later refined by [21] can only be achieved by registration protocols which essentially ensure that the PKI also learns the associated secret key.

The works of Boldyreva et al [7] and of Boyd et a. [8] are closest in spirit to ours in that they are exclusively concerned with the use of PKIs within other protocols and primitives. Boldyreva et al. [7] consider the security of asymmetric encryption and digital signatures in the presence of attackers that can also interfere with the registration process of long term keys. That work considers composition of PKIs with these two important primitives but leaves the study of implications to higher level protocols for future work. More recently, Boyd et al. [8] have looked at the use of PKIs within key exchange protocols. They extend standard cryptographic model for key exchange with adversarial capabilities that reflect potential PKI interference (like registering malformed keys). The models can then be used to construct key exchange protocols that protect against some weaknesses in the PKI. However, strictly speaking the results are not compositional results: there are no guarantees for when the PKI is instantiated with an actual protocol.

2 Why composing with a PKI is hard?

In this section we discuss in more details why composition with a PKI does not work so well in general, providing counter-examples and spelling out the assumptions we will consider in the rest of the paper.

2.1 Minimal assumptions on the PKI

We first state what we view as the minimal property that we believe a PKI should satisfy. Informally, we demand that:

- An honest agent has a unique public/private key pair and a unique verification/signing key pair.
- Honest agents have pairwise distinct private/signing keys.
- Keys are consistently distributed, that is, honest agents know each other public and verification keys.
- Decryption/signing keys of honest agents are private.

In this paper we explore whether these properties are actually sufficient: can a PKI that satisfies the requirements above be safely used together with any public key protocol Q?

2.2 Standard assumptions

Since composing a public-key protocol involves sharing key material, we of course face the same issues as existing composition results [17,16,15,2]. In particular, one of the protocols could act as a decryption oracle for the other one. For example, assume that the PKI includes a challenge response phase where the authority checks that A knows her private key.

$$Auth \to A : \{N\}_{\mathsf{pkA}}$$
$$A \to Auth : N$$

This challenge phase may occur during the registration of the key but also later, for example if A wishes to extend the validity of the certificate associated with her key. Such a PKI would break the security of most protocols that use public keys. Consider for example, the following simple protocol Q where B sends a secret to A using her public key.

$$B \to A : \{s\}_{\mathsf{pkA}}$$

Then Q executed in isolation with predistributed keys is secure (it does not compromise s) while Q composed with the PKI described above is insecure.

The standard way for preventing such behaviours [17,16,15,2] consists in tagging the encryption scheme which a tag t_{pki} that is specific to the protocol.

$$Auth \to A : \{\mathsf{t}_{pki}, N\}_{\mathsf{pkA}}$$
$$A \to Auth : N$$

In this paper we go one step further: we introduce a more general property which ensures that messages of different protocols are not confused. The usual tagging mechanism is only one way to enforce this property. We show that it suffices to ensure that functions shared between protocols protocols use different keys. In particular, a PKI protocol P may use the same signature (resp. encryption) scheme as Q, if keys provided by P to Q are used to sign (resp. encrypt) either by P or Q but not by both. In practice, this condition is often satisfied and allows us to compose protocols without requiring a tagging scheme. A typical exception are protocols where the PKI protocol uses the keys it provides to also carry out a challenge response as proof of possession.

2.3 Confusing public keys with other material

Analysis of public key protocols typically assumes that the keys of all parties have been honestly generated and distributed. However, this assumption is not valid in all scenarios, e.g. in the Verisign process for issuing certificates where users generate their own secret/public keys and have them certified. The following example shows that the mismatch between assumption and reality may be problematic.

Assume a setting where public keys (or verification keys) are used to identify parties. Consider a simple protocol where A sends a message M to B, signed together with the identity of B, to indicate that M is meant for B.

$$A \to B : [\mathsf{pkB}, M]_{\mathsf{skA}}$$

When B receives the message M, he is convinced that A sent it to him. Consider an attacker C who registers the string $\mathsf{pkC} = \mathsf{pkB}, \mathsf{pkC}'$ as his public key. Note that he may not be able to decrypt message encrypted by pkC (or properly sign with the corresponding key) but this still allows him to mount an attack against the simple signing protocol.

$$A \to C : [\mathsf{pkC}, M]_{\mathsf{skA}}$$
$$C(B) \to B : [\mathsf{pkB}, \mathsf{pkC}', M]_{\mathsf{skA}} \text{ since } \mathsf{pkC} = \mathsf{pkB}, \mathsf{pkC}'$$

That is, when A initiates a session with some malicious party C, C can use the message in this session to impersonate A towards user B. In practice, it could be the case that A was requesting a service to C, and the attacker uses the corresponding message to request a service to B, in the name of A. So, while the protocol is secure when long term keys of parties are honestly generated, the protocol is insecure if parties manage to register malformed keys.

One way of circumventing this issue is to tag keys that are part of messages (i.e. not used for signing/encryption).

$$A \to B : [\mathsf{t}_{\mathsf{pkey}}(\mathsf{pkB}), M]_{\mathsf{skA}}$$

Such a tagging makes sense as soon as the format of messages ensures that public keys cannot be confused with other material. However examples in the following sections show that this countermeasure is not sufficient.

2.4 Confusing public keys with other keys

Even when public keys are not sent as payload, the adversary may chose his dishonest key so that he can trigger unexpected behaviors. Consider the case where A sends out a secret encrypted with C's public keys and (immediately) decrypts the message with her private key.

$$A \to B : \mathsf{adec}(\{s\}_{\mathsf{pkC}}, \mathsf{skA})$$

Then C may simply chose his public key to be the public key of A: $\mathsf{pkC} = \mathsf{pkA}$, yielding an attack in the protocol Q described above. A similar issue occurs if A uses fixed, long term, asymmetric keys. Our example is admittedly contrived but it conveys well the composition issue. We could make it more realistic by complexifying Q.

2.5 Several public keys for the same identity

One problem which is not fixed by the use of tagging is that dishonest parties may register and use different keys to identify themselves to different users. This may yield composing issue as soon as Q contains (non trivial) else branches. Notice that a dishonest agent may register different keys for his identity. For example, A may believe C's public keys is pkC while B believes C's public keys is pkC'. This can created unexpected disequalities that undermine the security of Q, as illustrated by the following example.

$$\begin{array}{c} A \to B : [B, \mathsf{pkB}]_{\mathsf{sigA}} \\ A : [x, y_1]_{\mathsf{sigA}}, [x, y_2]_{\mathsf{sigB}} \overset{y_1 \neq y_2}{\longrightarrow} B : s \end{array}$$

A sends the public key of B as viewed by A, signed by A. Then whenever A receives two certificates (one from A and one from B), she may check that the two public keys coincide. By interacting with two sessions of the protocol (one with A and one with B), the attacker could obtain both $[C, \mathsf{pkC}]_{\mathsf{sigA}}$ and $[C, \mathsf{pkC}']_{\mathsf{sigB}}$, and send them to A to learn the secret s. While this example is again contrived, it presents well the intuition: in case two honest agents A and B do not share the same view on C, some unexpected behaviors may occur. To circumvent this issue, we have two options: either consider more demanding properties on the PKI (even dishonest keys should be consistently distributed) or we analyze a more flexible Q (see next sections). We explore both options in this paper. This issue did not surface in previous composition results since they either do not consider else branches [17,16] or do not consider dishonest keys [15,2].

2.6 Related keys

Even if a PKI guarantees that honest agents have pairwise distinct public keys, there is no guarantee that these keys are independent. Key dependencies may lead to insecurity, as exemplified by our next (pathological) example. Assume that, possibly in interaction with the PKI, A obtains k as private key ($\mathsf{skA} = k$) while B obtains $\langle k, k\rangle$ ($\mathsf{skB} = \langle k, k\rangle$). This would break the security of the following protocol Q.

$$\begin{array}{c} A \to B : \{N\}_{\mathsf{pkB}} \\ A : \mathsf{in}(x).\ \text{let } y = \mathsf{adec}(x, \langle \mathsf{skA}, \mathsf{skA}\rangle) \overset{y=N}{\longrightarrow} B : s \end{array}$$

Then A sends a fresh nonce N encrypted with B's public key and then expects a message x, decrypts it with $\langle \mathsf{skA}, \mathsf{skA}\rangle$ and leaks a secret (s) if she retrieves her nonce N. This protocol would clearly be insecure with the PKI sketched above while when keys are honestly and independently generated the protocol is clearly secure.

One way to circumvent this problem is to ensure through syntactical requirements that Q cannot break due to dependencies of keys provided by P. Interestingly, this issue is not specific to public key distribution. However, previous results discarded such behaviors by either requiring disjoint primitives [16] (the two protocols may not both use concatenation) or requiring explicitly that keys established by P are atomic or at least viewed as atomic by Q [15,2].

2.7 Permissive Q

The examples in the previous sections show that typical security assumptions on a PKI fail, in more than one way, to allow composition with arbitrary public key protocols. One option to recover

composability is to require more from the PKI, in particular w.r.t. the dishonest keys. Another option is to analyze Q under a more "permissive" assumption which makes no restrictions on how keys of dishonest parties are created. For example, instead of analyzing sessions between A, B and a dishonest C with perfectly distributed keys:

$$Q_1(sk_A, \mathsf{pk}(sk_B)) \mid Q_2(sk_B, \mathsf{pk}(sk_A)) \mid Q_2(sk_B, \mathsf{pk}(sk_C))$$

we may let agents input dishonest keys from the adversary.

$$Q_1(sk_A, \mathsf{pk}(sk_B)) \mid Q_2(sk_B, \mathsf{pk}(sk_A)) \mid \mathsf{in}(x).Q_2(sk_B, x)$$

Indeed, we show that if this permissive Q is secure then it can be safely composed with a PKI, under much lighter assumptions. Interestingly, such a permissive Q can be easily encoded in existing tools (e.g. ProVerif, Tamarin, Scyther).

2.8 Summary

In this paper, we conduct a thorough analysis on how to compose safely protocols with a PKI. Our main results are summarized in Table 1. The rest of the paper is devoted to the formalization and proof of these results. Interestingly, we do not need to prove each result separately. Instead, we can derive them from a general composition result (which will not be fully stated in the paper, due to space constraints).

<table>
<tr><th>Q secure</th><th>P secure PKI</th><th colspan="2">Additional hypotheses</th><th>Permanent hypotheses</th></tr>
<tr><td rowspan="2">Q_{perm}</td><td rowspan="2">ϕ_{PKI}</td><td colspan="2">Tagged Processes</td><td rowspan="3">• Only $\mathcal{F}^0$ as comon signature
• Tagged private keys</td></tr>
<tr><td colspan="2">Disjoint keys</td></tr>
<tr><td rowspan="2">Q_{ideal}</td><td rowspan="2">$\phi_{\mathsf{PKI}} \wedge \phi_{ideal}$</td><td>Tagged Processes</td><td>• Tagged public keys</td></tr>
<tr><td>Disjoint keys</td><td>• Only PKI keys in asym. enc.</td></tr>
</table>

Fig. 1. Summary of our composition results

3 Framework

A cryptographic protocol describes how agents exchange messages over a network. A standard framework for modelling cryptographic protocols is a process algebra, such as the applied pi-calculus [1]. It is typical for existing approaches to have an implicit notion of agents: an honest agent is modeled as a process while dishonest agents are not described – their private keys are simply passed to the attacker. This is not sufficient to describe some trust scenarios like those underlying our results. We therefore introduce novel specification framework which enhances the traditional process algebra with an explicit notion of agent. In particular, our framework provides the user directly with an intuitive notion of honest and dishonest agents, discharging him from having to hard-code which keys are known to the attacker. We also believe that it can be used to specify more complex scenario such as subnetworks, e.g. the particular protocol topology described in the introduction where a server links an unboundned number of pairs of parties.

3.1 Messages and agents

We assume a set of *names* $\mathcal{N}$ used to represent keys, nonces, etc. We consider a set of *agents* $\mathcal{A} = \mathcal{A}_D \uplus \mathcal{A}_H$ where $\mathcal{A}_D$ (resp. $\mathcal{A}_H$) represents the dishonest (resp. honest) agents, a set of *integer variables* $\mathcal{X}_{\mathbb{N}}$ and a set of *variables* $\mathcal{X} = \mathcal{X}_t \uplus \mathcal{X}_a$ where $\mathcal{X}_t$ represents term variables and $\mathcal{X}_a$ agent

variables. All these sets are infinite. Lastly, we consider a signature $\mathcal{F} = \mathcal{F}_c \uplus \mathcal{F}_d$ which consists of a finite set of function symbols and their arity. The subsets $\mathcal{F}_c$ and $\mathcal{F}_d$ represent constructor and destructor function symbols.

Many calculi (e.g. applied pi calculus [1]) rely extensively on the renaming of bounded variables and names in presence of replication. However, this renaming becomes an hindrance when one needs to refer to specific variables or names during the protocol execution. Moreover, the renaming does not allow a simple mapping between the different agents and their shared knowledge. We therefore replace part of the renaming with an alternative mechanism that relies on the notion of *parametrized agent* and *parametrized names*.

We define the set of parametrized agents $\overline{\mathcal{A}}$ as the set of elements from $\mathcal{X}_a$ or of the form $A[p_1, \ldots, p_n]$ where $A \in \mathcal{A}$, $n \in \mathbb{N}$ and $p_i \in \mathbb{N} \cup \mathcal{X}_{\mathbb{N}}$ for $i = 1 \ldots n$. We say that a parametrized agent $A[p_1, \ldots, p_n]$ is honest (resp. dishonnest) when $A \in \mathcal{A}_H$ (resp. $\mathcal{A}_D$) and we denote by $\overline{\mathcal{A}_H}$ (resp. $\overline{\mathcal{A}_D}$) their set. When there is no parameter, we write A for $A[]$. For example, for a typical protocol, we will simply consider one honest parameterized agent $H[i]$ and one dishonest parameterized agent $D[i]$ to model honest agents $a_1, a_2 \ldots$ and dishonest agents $d_1, d_2 \ldots$. A local server talking to agents inside an internal network can be be modeled as $S[i]$ with agents $A[i, j]$ where agents $A[i, 1], \ldots, A[i, n]$ only talk to $S[i]$.

Similarly, we define the set $\overline{\mathcal{N}}$ of parametrized names as the set of elements of the form $k[A_1, \ldots A_n]$ where $n \geq 1$, $k \in \mathcal{N}$ and $A_i \in \overline{\mathcal{A}}$ for $i = 1 \ldots n$. We say that a parametrized name $k[A_1, \ldots, A_n]$ is honest when $A_1, \ldots, A_n$ are all honest and is otherwise dishonest.

Terms are inductively defined as variables, names, parametrized names and agents, closed by application of function symbols (in a way that complies with arities). We say that a term t is a *constructor term* when t does not contain destructor function symbols. A term t is *ground* if it does not contain any variables and integer variables.

The destructor and constructor function symbols represent the cryptographic primitives used in the protocol. We model their behavior by means of a *rewriting system* $\mathcal{R}$ and an *equational theory* E that are standard rewriting techniques used in symbolic cryptographic models (e.g. [20]). In our model we require that the equations in E are between name-free constructor terms and that the rewrite rules in $\mathcal{R}$ are of the form $\mathsf{f}(t_1, \ldots, t_{n-1}) \to t_n$ where $t_1, \ldots, t_n$ are name-free constructor terms and $\mathsf{f} \in \mathcal{F}_d$. Moreover, we assume that $\mathcal{R}$ is convergent modulo E we denote by $u{\downarrow}$ the normal form of u modulo E. Lastly, we consider the predicate $Msg(u)$ which holds when the normal form modulo E of any subterm of u is a constructor term. In such a case, we say that u is a *message*. Thanks to our expressive modeling which considers both a rewrite system and an equational theory, we can model most primitives and in particular rather complex primitives such as Exclusive Or, associative concatenation, Diffie-Hellman, or blind signatures.

Example 1. We consider the signatures $\mathcal{F} = \mathcal{F}_c \uplus \mathcal{F}_d$ where $\mathcal{F}_d = \{\mathsf{sdec}/2, \mathsf{rsdec}/2, \mathsf{adec}/2, \mathsf{radec}/2, \mathsf{check}/2, \mathsf{proj}_1/1, \mathsf{proj}_2/1\}$ and $\mathcal{F}_c = \{\mathsf{senc}/2, \mathsf{rsenc}/2, \mathsf{aenc}/2, \mathsf{raenc}/2, \mathsf{pk}/1, \mathsf{sign}/2, \mathsf{vk}/1, \langle\,\rangle/2, \mathsf{h}/1, \oplus/2, 0/0\}$. They represent deterministic and randomized symmetric encryption as well as asymmetric encryption, signature, pairing, hash function and exclusive or. Their behavior can be modeled with the following rewriting system $\mathcal{R}$:

$$\begin{aligned}
\mathsf{sdec}(\mathsf{senc}(x, y), y) &\to x \\
\mathsf{check}(\mathsf{sign}(x, y), \mathsf{vk}(y)) &\to x \\
\mathsf{adec}(\mathsf{aenc}(x, \mathsf{pk}(y)), y) &\to x \\
\mathsf{proj}_i(\langle x_1, x_2 \rangle) &\to x_i \text{ with } i \in \{1, 2\}) \\
\mathsf{rsdec}(\mathsf{rsenc}(x, y, z), z) &\to x \\
\mathsf{radec}(\mathsf{raenc}(x, y, \mathsf{pk}(z)), z) &\to x
\end{aligned}$$

and the following equational theory E that models Exclusive Or:

$$\begin{aligned}
x \oplus x &= 0 & x \oplus (y \oplus z) &= (x \oplus y) \oplus z \\
x \oplus 0 &= x & x \oplus y &= y \oplus x
\end{aligned}$$

3.2 Processes

Processes in our framework are modeled using the grammar in Figure 2. We discuss its less standard aspects below, and we do so from the perspective of using this specification framework to formulate our results.

Before we go into the details, we introduce a useful refinement of how assignment is usually handled in processes. We are motivated by our composition scenario. A PKI infrastructure P assign secret and public keys and these keys may then be passed through variable assignment to a process Q that depends on these keys. To indicate what type of terms is expected to be assigned in a variable, we introduce a typed variable assignment $[x :=_\tau u]$. Formally, we consider a set T of types that contains $\mathbb{sk}, \mathbb{pk}, \mathbb{vk}, \mathbb{sig}$, corresponding to types for resp. private, public, verification, and signing keys. Similarly to parametrized names, we also consider the infinite sets $\mathcal{X}_{ty}$ and $\overline{T}$ of type variables and parametrized types respectively. For example, a variable assignment with type $\mathbb{pk}[A, B]$ will typically refer to the public key of B as viewed by A. As we shall see later, this is very convenient to relate variables among different agents and different sessions. Given $\tau \in T$, we denote by $\overline{\tau}_H$ the set of parametrized types $\tau[A_1, \ldots, A_n]$ where $A_1, \ldots, A_n$ are honest.

$P, Q =$	0	null
	$\mid \mathsf{in}_A(c, x).P$	input
	$\mid \mathsf{out}_A(c, u).P$	output
	$\mid \mathsf{if}\ u = v\ \mathsf{then}\ P\ \mathsf{else}\ Q$	conditional
	$\mid P \mid Q$	parallel
	$\mid !^i P$	replication
	$\mid \mathsf{new}_A\, k.P$	name restriction
	$\mid \mathsf{agent}(X, S).P$	agent selection
	$\mid [x :=_\tau u].P$	variable assignment

where $A \cup \in \overline{\mathcal{A}}$, $S \subseteq \overline{\mathcal{A}}$, $X \in \mathcal{X}_a$, $x \in \mathcal{X}_t$, $i \in \mathcal{X}_{\mathbb{N}}$, $\tau \in \overline{T}$ and c, u, v are terms.

Fig. 2. Grammar of processes

The grammar of our processes is provided in Figure 2 and explained below. Part of our grammar is classical in cryptographic process algebra. Note that we annotate inputs, outputs and name restrictions by the agent performing them. Moreover, a replication $!^i P$ is annotated by an integer i. Intuitively, P is parametrized by the variable i that will be instantiated at each replication by some (non necessarily fresh) integer $n \in \mathbb{N}$. This mechanism allows to differentiate between different replicas of P. For example, $!^i R_1(k[S, A[i]]) \mid R_2(k[S, A[i]])$ represents a server talking to infinitely many agents, each of them sharing a ket $k[S, A]$ with him. Even more interestingly, we can represent the case of an unbounded number of internal networks, where inside each network i, agents may only communicate among themselves and to a router $S[i]$, while routers may communicate between them. The corresponding process is $!^i R_1(S[i]).!^j R_2([S[i], A[i, j]])$, which denotes multiples sessions of R_1 and R_2 but where the $A[i, j]$ may only talk to the same $S[i]$. The process $\mathsf{agent}(X, S)$ selects an agent from S that instantiates X. Lastly, the process $[x :=_\tau u]$ assigns the term u to the variable x typed with τ.

Term variables are bound by input and variable assignment, agent variables are bound by agent selection and names are bound by name restriction. We say that a process P is *a role of* A if all outputs, inputs and name restrictions in P are done by A and all parametrized names and types in P contain A as agent.

Example 2. We consider a PKI where agents generate their own private/public key pair and signing/verification key pair. They send both public key and verification key to a trusted server S to be signed. When an agent A wishes to establish a connection with another agent B, he will a request to B along with his own certificate. Upon receiving the certificates of B, A will check that they are signed by the server and they correspond to the public and verification keys of B.

The role of the agent can be modeled by the following context process $P_A[\__A]$ where the hole $\__A$ corresponds to where the role of A in the composed protocol (*e.g.* Needham-Schroeder protocol) will be plugged.

$$\begin{array}{ll}
\mathsf{out}_A(pc[S,A], \langle \mathsf{pk}(sk[A]), \mathsf{vk}(sig[A])\rangle). & \textit{Register}\\
\mathsf{in}_A(pc[S,A], x_{cert}). & \\
[x_{skA} :=_{\mathbb{sk}[A]} sk[A]].[x_{sigA} :=_{\mathbb{sig}[A]} sig[A]]. & \\
\mathsf{out}_A(c, \langle\langle \mathsf{request}, B\rangle, x_{cert}\rangle).\mathsf{in}_A(c,z). & \textit{Request}\\
\mathsf{if}\ \mathsf{proj}_1(\mathsf{check}(z, \mathsf{vk}(sig[S]))) = B\ \mathsf{then} & \textit{Check}\\
\\
\mathsf{let}\ y = \mathsf{proj}_2(\mathsf{check}(z, \mathsf{vk}(sig[S])))\ \mathsf{in} & \\
[y_{pkB} :=_{\mathbb{pk}[A,B]} \mathsf{proj}_1(y)].[y_{vkB} :=_{\mathbb{vk}[A,B]} \mathsf{proj}_2(y)].__A & \textit{Assign}
\end{array}$$

We use the syntax $\mathsf{let}\ y = u\ \mathsf{in}\ P$ as a syntactic sugar for $P\{^u/_y\}$. Note that in the registration phase, $sk[A]$ and $sig[A]$ represent the private and signing keys of A. Since they are parametrized names, they will remain the same through any different sessions. Furthermore, an attacker does not have directly access to them unless A is dishonest. Also note that the agent A and the server S are communicating through a parametrised channel $pc[S,A]$ meaning that this channel is only shared between A and S. After sending its request to B, the agent A is expecting a message of the form $\mathsf{sign}(\langle B, \langle t_1, t_2\rangle\rangle, sig[S])$ where t_1 and t_2 respectively correspond to the public and verification key of B. Once the agent A verifies the signature and the ownership of the certificate, he assigns the variables accordingly.

The role of the receiver B is very similar to the one of A and can be modeled by the following context process $P_B[\__B]$. The process modeling the role of the server registering the key of an agent A, denoted $R(A)$, is described as follows:

$$\mathsf{in}_S(pc[S,A], x).\mathsf{out}_S(pc[S,A], \mathsf{sign}(\langle A, x\rangle, sig[S]))$$

A complete session of the PKI with a server S between two agents A and B can thus be modeled by the following context process $P[\__A, \__B] = P_A[\__A] \mid P_B[\__B] \mid R(A) \mid R(B)$. Furthermore, if we want to model unbounded number of sessions between honest and dishonest agents, with a unique trusted server S. It corresponds to the following context process

$$!^i\ \mathsf{agent}(A, \{H[i], D[i]\}).!^j\ \mathsf{agent}(B, \{H[j], D[j]\}).P[\__A, \__B]$$

where $S, H \in \mathcal{A}_H$ and $D \in \mathcal{A}_D$.

The following example models the well-known Needham-Schroeder-Lowe protocol [25].

Example 3. Needham-Schroeder-Lowe protocol can be informally described as follows.

$$\begin{array}{l}
A \to B : \{\mathsf{pkA}, N_a\}_{\mathsf{pkB}}\\
B \to A : \{\mathsf{pkB}, N_a, N_b\}_{\mathsf{pkA}}\\
A \to B : \{N_b\}_{\mathsf{pkB}}
\end{array}$$

The following process Q_A represents the role of the initiator A in the Needham-Schroeder protocol:

$$\begin{array}{l}
\mathsf{new}_A\, n_a.\mathsf{out}_A(c, \mathsf{aenc}(\langle \mathsf{pk}(x_{skA}), n_a\rangle, x_{pkB})).\mathsf{in}_A(c,y).\\
\quad \mathsf{if}\ n_a = \mathsf{proj}_1(\mathsf{proj}_2(\mathsf{adec}(y, x_{skA})))\ \mathsf{then}\\
\quad \mathsf{if}\ x_{pkB} = \mathsf{proj}_1(\mathsf{adec}(y, x_{skA}))\ \mathsf{then}\\
\quad \mathsf{out}_A(c, \mathsf{aenc}(\mathsf{proj}_2(\mathsf{proj}_2(\mathsf{adec}(y, x_{skA}))), x_{pkB}))
\end{array}$$

Note that x_{skA}, x_{pkB} are free in Q_A. Intuitively, these variables should be bound by a PKI infrastructure process P that assigns variables x_{skA} and x_{pkB} respectively with type $sk[A]$ and $pk[A,B]$ where B is the agent contacted by A.

Definition 1. *A configuration is a tuple $(\mathcal{E}; P; \Phi; \sigma; \mu)$ where:*

– *$\mathcal{E}$ is a set of names that corresponds intuitively to the private names of the process.*

– *P is a process where names and variables are bound only once.*
– *Φ and σ are both substitutions of term variables to ground terms. The variables of* $\mathrm{dom}(\Phi)$ *do not appear anywhere else in the configuration.*
– *μ is a mapping from $\overline{T}$ to sets of term variables.*

The set $\mathcal{E}$ represents the set of names that have been generated by honest agents. The substitution Φ, also called *frame*, represents the messages that have been sent on channels controlled by the attacker (and which the adversary therefore knows). The substitution σ represents the variables instantiated so far. Lastly, $\mu(\tau)$ for some τ is the set of variables that have been assigned with type τ. We sometimes write P instead of the initial configuration $(\emptyset; P; \emptyset; \emptyset; \emptyset)$.

The attacker can forge new messages by applying *recipes* to his knowledge that is by applying function symbols. He may also use names, except the names generated by honest agents. Formally, given a frame Φ and a set $\mathcal{E}$, we define $\mathsf{Recipe}(\Phi, \mathcal{E})$ as the set of terms M whose variables are of the domain of Φ, whose names are not in $\mathcal{E} \cup \overline{\mathcal{N}}_H$ and that satisfies $Msg(M\Phi)$.

3.3 Semantics

We define the operational semantics of configurations through a transition relation $\mathcal{K} \to \mathcal{K}'$ between configurations. The transition relation is defined by the rules given in Figure 3. We denote by $\to^*$ the transitive closure of $\to$.

$$(\mathcal{E}; P \mid \mathsf{out}_A(c,u).Q; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid Q; \Phi \cdot \{w \to u\sigma\}; \sigma; \mu) \quad \text{(Out)}$$
$$\text{if } w \text{ is fresh, } Msg(c\sigma), Msg(u\sigma) \text{ and } \exists M \in \mathsf{Recipe}(\mathcal{E}, \Phi).M\Phi{\downarrow} = c\sigma{\downarrow}$$

$$(\mathcal{E}; P \mid \mathsf{in}_A(c,x).Q; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid Q; \Phi; \sigma \cdot \{x \to N\Phi\sigma\}; \mu) \quad \text{(In)}$$
$$\text{if } \exists M, N \in \mathsf{Recipe}(\mathcal{E}, \Phi) \text{ s.t. } M\Phi{\downarrow} = c\sigma{\downarrow}, Msg(c\sigma)$$

$$(\mathcal{E}; P \mid \mathsf{in}_A(c,x).Q \mid \mathsf{out}_B(d,u).R; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid Q \mid R; \Phi; \sigma \cdot \{x \to u\sigma\}; \mu) \quad \text{(Comm)}$$
$$\text{if } Msg(c\sigma), Msg(d\sigma), Msg(u\sigma) \text{ and } c\sigma{\downarrow} = d\sigma{\downarrow}$$

$$(\mathcal{E}; P \mid \mathsf{if}\ u = v\ \mathsf{then}\ Q\ \mathsf{else}\ R; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid Q; \Phi; \sigma; \mu) \quad \text{if } u\sigma{\downarrow} = v\sigma{\downarrow}, Msg(u\sigma), Msg(v\sigma) \quad \text{(Then)}$$

$$(\mathcal{E}; P \mid \mathsf{if}\ u = v\ \mathsf{then}\ Q\ \mathsf{else}\ R; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid R; \Phi; \sigma; \mu) \quad \text{if } u\sigma{\downarrow} \neq v\sigma{\downarrow} \text{ or } \neg Msg(u\sigma) \text{ or } \neg Msg(v\sigma) \quad \text{(Else)}$$

$$(\mathcal{E}; P \mid !^i\, Q; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid !^i\, Q\{i \to n\}\rho; \Phi; \sigma; \mu) \quad \text{(Repl)}$$
$$\text{if } n \in \mathbb{N} \text{ and } \rho \text{ is a fresh renaming of bound names and variables of } Q$$

$$(\mathcal{E}; P \mid \mathsf{new}_A\, k.Q; \Phi; \sigma; \mu) \to (\mathcal{E}'; P \mid Q; \Phi; \sigma; \mu) \quad \text{where } \mathcal{E}' = \mathcal{E} \cup \{k\} \text{ if } A \in \overline{\mathcal{A}}_H \text{ else } \mathcal{E}' = \mathcal{E} \quad \text{(New)}$$

$$(\mathcal{E}; P \mid \mathsf{agent}(X,S).Q; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid Q\{X \to A\}; \Phi; \sigma; \mu) \quad \text{if } A \in S \quad \text{(Agent)}$$

$$(\mathcal{E}; P \mid [x :=_\tau u].Q; \Phi; \sigma; \mu) \to (\mathcal{E}; P \mid Q; \Phi; \sigma \cdot \{x \to u\sigma\}; \mu') \quad \text{(Assign)}$$
$$\text{if } Msg(u\sigma),\ \mu'(\tau') = \mu(\tau') \text{ for } \tau' \neq \tau \text{ and } \mu'(\tau) = \mu(\tau) \cup \{x\}$$

Fig. 3. Semantics of configuration

The rules follow the intuition we gave when describing the grammar of of processes. Note that the rule New adds a name k restricted in $\mathsf{new}_A\, k.P$ to the set $\mathcal{E}$ only if A is honest. If A is dishonest, k becomes available to the attacker (since $k \notin \mathcal{E}$, it can be freely used in recipes by the attacker). Also note that the rule Assign augments μ by adding x to the set $\mu(\tau)$ of variables of type τ.

Example 4. Consider the process Q_A of Example 3 representing the role of the initiator in the Needham-Shroeder protocol. Recall that x_{skA} and x_{pkB} where free in Q_A. Assume that Q_B is a process representing the role of the receiver with x_{skB} and x_{pkA} as free variables. The following process models an unbounded number of sessions of the Needham-Schoeder protocol between honest or dishonest agents where the public keys and private keys are ideally distributed.

$$!^i\, \mathsf{agent}(A, \{H[i], D[i]\}).!^j\, \mathsf{agent}(B, \{H[j], D[j]\}).(\\ Q_A\{^{sk[A]}/_{x_{skA}}, ^{\mathsf{pk}(sk[B])}/_{x_{pkB}}\} \mid Q_B\{^{sk[B]}/_{x_{skB}}, ^{\mathsf{pk}(sk[A])}/_{x_{pkA}}\})$$

where $H \in \mathcal{A}_H$ and $D \in \mathcal{A}_D$.

3.4 Logical formulas

To express security property, we introduce a first order logic on configurations. It will be particularly convenient to specify the properties expected from a "good" PKI. We consider the following atomic formula.

- $u = v$ and $u \neq v$ where u, v are terms
- $x \mathrel{\mathring{=}} y$ and $x \mathrel{\mathring{\neq}} y$ where x, y are term variables
- $\tau_1 = \tau_2$ where τ_1, τ_2 are parametrized types
- $\not\vdash x$ where x is a term variable

A valuation is a configuration $\mathcal{K} = (\mathcal{E}; P; \Phi; \sigma; \mu)$. The satisfaction relation $\models_c$ of atomic formulas is defined as

$$\begin{array}{ll}
\mathcal{K} \models_c x \mathrel{\mathring{=}} y & \text{iff } x = y \\
\mathcal{K} \models_c u = v & \text{iff } u\sigma\downarrow = v\sigma\downarrow \\
\mathcal{K} \models_c \not\vdash x & \text{iff } \forall M \in \mathsf{Recipe}(\mathcal{E}, \Phi).\, Msg(M\Phi) \\
 & \qquad \text{implies } M\Phi\downarrow \neq x\sigma\downarrow \\
\mathcal{K} \models_c \tau_1 =_{\mathcal{A}} \tau_2 & \text{iff } \exists \gamma_1, \gamma_2 \in T. \exists A_1, \ldots, A_n \in \overline{\mathcal{A}}. \\
 & \qquad \tau_1 = \gamma_1[A_1, \ldots, A_n] \wedge \tau_2 = \gamma_2[A_1, \ldots, A_n]
\end{array}$$

and is lifted as usual to logic formulas with boolean connectors $\wedge, \vee$ and universal and existential quantification of parametrized agent and type variables. Moreover, we consider universal quantification of term variables over parametrized type: $\forall x \in \tau.\phi$ with $x \in \mathcal{X}_t$, $\tau \in \overline{T}$. Its satisfaction relation is defined as: $\mathcal{K} \models_c \forall x \in \tau.\phi$ iff $\forall x \in \mu(\tau), \mathcal{K} \models_c \phi$. Similarly, we also consider existential quantification of term variables.

We say that a process P satisfies a formula ϕ, denoted $P \models \phi$, if ϕ holds in an accessible configuration, that is, $\mathcal{K} \models_c \phi$ for any configuration $\mathcal{K}$ such that $P \rightarrow^* \mathcal{K}$.

Example 5. Consider a type $\mathtt{sk}$ and a process $!^i\, \mathsf{agent}(X, \{H[i], D[i]\}).P$ where P contains a single assignment variable $[x :=_{\mathtt{sk}(X)} u]$. The formula

$$\forall A \in \overline{\mathcal{A}}_H. \forall y, z \in \mathtt{sk}(A). y = z$$

expresses that any two sessions of some honest agent always assign x to the same term. Note that the formula does not say anything about sessions of dishonest agents.

Secrecy. To model secrecy preservation, we consider an additional type $\mathtt{secret}$, yielding a set of types T that contains at least $\{\mathtt{sk}, \mathtt{pk}, \mathtt{sig}, \mathtt{vk}, \mathtt{secret}\}$. We assume that variables that should remain confidential are assigned the type $\mathtt{secret}$. Then secrecy can be generically defined by the following formula ϕ_{sec}.

$$\forall \tau \in \overline{\mathtt{secret}}_H. \forall x \in \tau. \not\vdash x$$

This formula states that any variable of type $\mathtt{secret}_A$ for A honest should not be deducible (for any of its instantiations).

Example 6. Continuing Example 3, we can require secrecy of the nonce n_a generated by A and the nonce n_b as received by A by simply modifying process Q_A as follows.

$$\begin{array}{l}
\mathsf{new}_A\, n_a.[z :=_{\mathtt{secret}[A,B]} n_a]. \\
\quad \mathsf{out}_A(c, \mathsf{aenc}(\langle \mathsf{pk}(x_{skA}), n_a \rangle, y_{pkB})).\mathsf{in}_(c, y) \\
\quad \mathsf{if}\ n_a = \mathsf{proj}_1(\mathsf{proj}_2(\mathsf{adec}(y, x_{skA})))\ \mathsf{then} \\
\quad \mathsf{if}\ y_{pkB} = \mathsf{proj}_1(\mathsf{adec}(y, x_{skA}))\ \mathsf{then} \\
\quad [z' :=_{\mathtt{secret}[A,B]} \mathsf{proj}_2(\mathsf{proj}_2(\mathsf{adec}(y, x_{skA})))]. \\
\quad \mathsf{out}_A(c, \mathsf{aenc}(\mathsf{proj}_2(\mathsf{proj}_2(\mathsf{adec}(y, x_{skA}))), y_{pkB}))
\end{array}$$

Authentication. In the literature, authentication properties are usually modeled using events. In our formalism, variables assignments can play such a role. Consider for example two types $\mathbb{ev}_{\mathbb{1}}$ and $\mathbb{ev}_{\mathbb{2}}$ contained in T. The authentication property modeling a correspondence between the two types can be defined by the following formula ϕ_{auth}.

$$\forall \tau \in \overline{\mathbb{ev}_{\mathbb{1}}}_H . \forall x \in \tau . \exists \tau' \in \overline{\mathbb{ev}_{\mathbb{2}}}_H . \exists y \in \tau' . \tau =_{\mathcal{A}} \tau' \wedge x = y$$

Informally, the formula indicates that whenever a variable x of type $\mathbb{ev}_{\mathbb{1}}[A_1, \ldots, A_n]$ is assigned a term with honest agents $A_1, \ldots, A_n$ then there exists a variable y of type $\mathbb{ev}_{\mathbb{2}}[A_1, \ldots, A_n]$ must have been assigned previously with the same term. We could also consider injective authentication by further requiring the variable y to be unique, which can be expressed by $\forall z \in \tau' . y \neq z \vee y \mathrel{\mathring{=}} z$.

Example 7. Continuing Example 3, authentication can be expressed through ϕ_{auth} and adding in Q_A the assignment $[x :=_{\mathbb{ev}_{\mathbb{2}}[A,B]} \langle n_A, \mathsf{proj}_2(\mathsf{proj}_2(\mathsf{adec}(y, x_{skA})))\rangle]$ and similarly in Q_B but with the type $\mathbb{ev}_{\mathbb{1}}$.

Composable properties. In this paper, we will show that our composition result preserves any *composable property*, that is, a closed formula from our logic where quantification of agents are over honest agents, i.e. of the form $\forall A \in S$ and $\exists A \in S$ with $S \subseteq \overline{\mathcal{A}}_H$, and where any atomic formula $u = v$ and $u \neq v$ involves only variables $(u, v \in \mathcal{X})$.

4 Composition hypotheses

In this section we formalize the hypothesis that underlie our composition theorem. Since the development is rather technical we include here a small roadmap for this section. We begin (Section 4.1) with formalizing the guarantees that we view as minimal for any PKI as skecthed in Section 2.1. Next, in Section 4.2, we formalize the composition of an arbitrary PKI protocol P with an arbitrary other protocol Q. Most of the development here consists of syntactical restrictions which essentially force that the composition between protocol P and Q.

The rest of the section deals with more subtle interactions between P and Q. In Section 4.3 we explain how to deal with private keys: they should be only be used as key material in cryptographic algorithms and, if sent as payload, they should be tagged. We discuss in Sections 4.3 and 4.4 two distinct approaches to ensure that the use of common primitives does not lead to unwanted interference between the two composed components. Our theorem can employ either of the two approaches.

We discuss each of the more subtle hypothesis that we require through the prism of an example that motivates it. For simplicity, both the discussions and the formalism that we develop in this paper consider the case of two party protocols; our results can be lifted to n-party protocols.

4.1 PKI properties

We consider PKIs that establish keys both for encryption and signatures. We model these types of keys through a set T of types for assignment variables that includes the types $\mathbb{sk}, \mathbb{pk}, \mathbb{sig}$ and $\mathbb{vk}$ respectively for asymmetric private keys, asymmetric public keys, signing keys, and verification keys. Agents do not necessarily share the same values for keys, in particular, an agent A may think that C's public key is pkC while B believes that C's public key is pkC'. We do not want to discard this possibility (since as discussed in Section 2.5, this is a possible attack against a PKI). We model this possibility using our notion of parametrized types. Specifically, we consider types of the form $\mathbb{sk}[A]$, $\mathbb{pk}[A, B]$, $\mathbb{sig}[A]$ and $\mathbb{vk}[A, B]$ where $\mathbb{pk}[A, B]$ (resp. $\mathbb{vk}[A, B]$) represents the asymmetric public (resp. verification) key of B as viewed by A.

As stated in Section 2.1, we informally demand that a PKI satisfies the following properties.

- An honest agent has a unique public/private key pair and a unique verification/signing key pair.

– Honest agents of course have pairwise distinct private/signing keys.
– Keys are consistently distributed, that is, honest agents know each other public and verification keys.
– Private/signing keys of honest agents are indeed private.

For asymmetric encryption keys, these properties are captured through the formula ϕ_{asy} below. Each line corresponds to a bullet above.

$$\begin{aligned}\phi_{asy} \mathrel{\hat{=}} \forall A, B \in \overline{\mathcal{A}}_H.\forall x, y \in \mathbb{sk}[A].x = y \\ \wedge \forall x \in \mathbb{sk}[A].\forall y \in \mathbb{sk}[B].A = B \vee x \neq y) \\ \wedge \forall x \in \mathbb{sk}[A].\forall y \in \mathbb{pk}[B, A].\mathsf{pk}(x) = y) \\ \wedge \forall x \in \mathbb{sk}[A].\not\vdash x)\end{aligned}$$

We model the analogous property of a good PKI w.r.t. signing/verification keys with a formula ϕ_{sig} obtained from ϕ_{asy} by replacing $\mathbb{sk}$, $\mathbb{pk}$ and pk respectively by $\mathbb{sig}$, $\mathbb{vk}$ and vk.

Finally, the overall guarantee that a PKI should offer are the two properties above together with the requirement that the keys used for signing/verification are different from those used for encryption/decryption:

$$\phi_{\mathsf{PKI}} \mathrel{\hat{=}} \phi_{asy} \wedge \phi_{sig} \wedge \forall A, B \in \overline{\mathcal{A}}_H.\forall x \in \mathbb{sk}[A].\forall y \in \mathbb{sig}[B].x \neq y$$

The last part of ϕ_{PKI} indicates that signing keys and private asymmetric keys should be pairwise distinct.

Example 8. Consider the PKI protocol modeled by the process P in Example 2. The protocol satisfies our security requirement: $C[P[0,0]] \models \phi_{\mathsf{PKI}}$ where $C[\_]$ is the context $!^i\ \mathsf{agent}(A, \{H[i], D[i]\}).!^j\ \mathsf{agent}(B, \{H[j], D[j]$ that declares the agents.

4.2 Composition Setup

In the previous section we introduced the security guarantee which we require from protocol P (when analyzed in isolation). From this point onwards we consider the interaction between P and Q. We start by defining the composition between a PKI protocol P and an arbitrary protocol Q. Formally, we first consider a process $P[\__A, \__B]$ representing a PKI protocol that establishes long term keys for two agents A and B. Second, we consider two processes Q_A and Q_B modeling the roles of a two-agents protocol Q in which keys are assumed to be already distributed. Our goal is to identify on which conditions on P and Q their combination remains secure. Formally, the combination of Q using the PKI P is expressed by the following process.

$$!^i\ \mathsf{agent}(A, \{H[i], D[i]\}).!^j\ \mathsf{agent}(B, \{H[j], D[j]\}).P[Q_A, Q_B]$$

This process models an unbounded number of sessions between honest and dishonest agents.

Since we consider two-agent protocols, we assume w.l.o.g. the following properties on P and Q.

H$_1$. $x_{skA}, y_{pkB}, x_{sigA}, y_{vkB}$ are the only possible free variables of Q_A, Q_A is a role of A and the hole $\__A$ in P is in the scope of $[x_{skA} :=_{\mathbb{sk}[A]} u]$, $[y_{pkB} :=_{\mathbb{pk}[A,B]} v]$, $[x_{sigA} :=_{\mathbb{sig}[A]} w]$, $[y_{vkB} :=_{vk[A,B]} r]$ for some u, v, w, r. We require the analogous hypothesis for Q_B and $\__B$. Moreover, the sets of bound names and free names in P and Q are distinct.

This hypothesis simply formalises the setting and ensures that the process $P[Q_A, Q_B]$ avoids name clashes and is closed, meaning that the free variables of Q_A and Q_B will be instantiated.

Moreover, we demand that the only shared keys are those that the PKI protocol P generates and passes to Q. Both protocols may generate other keys, but these cannot be shared. In particular, P and Q may not share long term keys.

H$_2$. for all $n[A_1, \ldots, A_p] \in pn(P[\__A, \__B])$, for all $m[B_1, \ldots, B_q] \in pn(Q_1, Q_2)$, $n \neq m$.

4.3 Tagging

As discussed in Section 2, a PKI infrastructure and a protocol Q do not immediately yield a secure composition. We first need to get rid of the behaviors explained in Section 2.2 where the PKI infrastructure P intereferes with a protocol Q as they use the same primitives and the same keys.

Similarly to the approach of Arapinis, Cheval, and Delaune [2] we consider a setting where P and Q may use arbitrary primitives, except for the shared ones, that should be the standard primitives. Formally, we consider the following common signature $\mathcal{F}^0 = \mathcal{F}^0_c \uplus \mathcal{F}^0_d$ where $\mathcal{F}^0_d = \{\mathsf{sdec}/2, \mathsf{rsdec}/2, \mathsf{adec}/2, \mathsf{radec}/3, \mathsf{check}/2, \mathsf{proj}_1/1, \mathsf{proj}_2/1\}$ and $\mathcal{F}^0_c = \{\mathsf{senc}/2, \mathsf{rsenc}/3, \mathsf{aenc}/2, \mathsf{raenc}/3, \mathsf{pk}/1, \mathsf{sign}/2, \mathsf{vk}/1, \langle\,\rangle/2, \mathsf{h}/1\}$. The associated rewriting system $\mathcal{R}^0$ has been defined in Example 1.

We also consider two disjoints signatures for P and Q, namely $\mathcal{F}^P, \mathcal{F}^Q$, as well as their associated rewriting systems $\mathcal{R}^P, \mathcal{R}^Q$ and equational theories $\mathrm{E}^P, \mathrm{E}^Q$.

Tagging of private keys We first need to guarantee that Q does not manipulare the structure of private keys, to avoid the "related keys" example of Section 2.6. Such related keys will be tolerated under the condition that Q never "opens" a private keys nor sends them as payload unless they are tagged (in principle, private keys should not be sent in payload anyway). Formally, assume that $\mathcal{F}^Q$ contains two function symbols tagk and untagk such that $\mathsf{untagk}(\mathsf{tagk}(x)) \to x \in \mathcal{R}^Q$ and $\mathsf{tagk}, \mathsf{untagk}$ do not appear in any other rewrite rules in $\mathcal{R}^Q$ or in E^Q. The next hypothesis states how private keys are tagged when used as payload:

H_3. Process $P[\_{A}, \_{B}]$ is built over $\mathcal{F}^P \cup \mathcal{F}^0$, process Q_A, Q_B are built over $\mathcal{F}^Q \cup \mathcal{F}^0 \setminus \{\mathsf{untagk}\}$ and in Q_A and Q_B, the private and signing keys provided by the PKI can only be used in key position with $\mathsf{adec}, \mathsf{radec}, \mathsf{sign}$ respectively or as the argument of tagk.

Tagging processes As illustrated in Section 2.2, primitives shared between P and Q should be tagged. For instance, tagging an encryption $\mathsf{senc}(u, k)$ may be done by encrypting u alongside some constant t, *i.e.* $\mathsf{senc}(\langle \mathsf{t}, u\rangle, k)$. As for the tags on private keys, we do not wish to specify exactly how tags are implemented. Therefore, for all $i \in \{P, Q\}$, we assume the existence of two function symbols tag_i and untag_i such that $\mathsf{untag}_i(\mathsf{tag}_i(x)) \to x \in \mathcal{R}^Q$ and $\mathsf{tag}_i, \mathsf{untag}_i$ do not appear in any other rewrite rules in $\mathcal{R}^i$ or in E^i.

Definition 2 (Tagged terms and processes). *Let $i \in \{P, Q\}$. We define the set of i-*tagged terms*, denoted $\textsc{Tagt}(i)$, as the smallest set of term built on $\mathcal{F}^i \cup \mathcal{F}^0$ such that for all $u_1, \ldots, u_n \in \textsc{Tagt}(i)$, for all $\mathsf{f}/n \in \mathcal{F}^i \cup \mathcal{F}^0$,*

- $u \in \textsc{Tagt}(i)$ *if* $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \mathcal{X}_t$
- $\mathsf{untag}_i(\mathsf{f}(u_1, \ldots, u_n)) \in \textsc{Tagt}(i)$ *if* $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{adec}, \mathsf{rsdec}, \mathsf{radec}, \mathsf{check}\}$
- $\mathsf{f}(\mathsf{tag}_i(u_1), u_2, \ldots, u_n) \in \textsc{Tagt}(i)$ *if* $\mathsf{f} \in \{\mathsf{senc}, \mathsf{aenc}, \mathsf{rsenc}, \mathsf{raenc}, \mathsf{sign}\}$
- $\mathsf{f}(u_1, \ldots, u_n) \in \textsc{Tagt}(i)$ *when* $\mathsf{f} \in \{\mathsf{h}, \langle\,\rangle, \mathsf{proj}_1, \mathsf{proj}_2, \mathsf{vk}, \mathsf{pk}\} \cup \mathcal{F}^i \setminus \{\mathsf{untag}_i\}$

*A process is said to be i-tagged if for all terms u contained in an action of the process (*i.e. *input, output, conditional and variable assignment), $u \in \textsc{Tagt}(i)$.*

We can now state our condition for tagged processes:

C_1. $P[\_{A}, \_{B}]$ is P-tagged and Q_A, Q_B are Q-tagged

4.4 Disjoint public keys

Considering tagged protocols P and Q is an efficient way to ensure that honest agents do not confuse messages from P with messages from Q. While simple, such a tagging assumption is rarely met in practice. Even simple protocols such as the Needham-Schroeder-Love protocol would not be covered by our composition result. We propose here an alternative assumption that is best explained going back to the example described in Section 2.2 where the executions of P and Q

may interfere with each other. To avoid such interferences, we need to make sure that the set of keys that are used for encryption and signatures in P is disjoint from the set of keys used in Q. Such a condition may however be difficult to check. We therefore formulate a stronger assumption, usually met in practice.

Specifically, we assume that the only public/private keys *dynamically* generated by P and Q are those passed from P to Q. This assumption is often met in practice, e.g. for our NSL example. This is informally stated as follows.

C_2. All terms in $P[\_A, \_B]$ used in key positions w.r.t. $\mathcal{F}^0$ are ground, that is, P only uses keys known in advance.

C_3. All terms in Q_A, Q_B used in key positions w.r.t. $\mathcal{F}^0$ are either ground and disjoint from the terms in $P[\_A, \_B]$ used in key positions w.r.t. $\mathcal{F}^0$ or in $\{x_{skA}, y_{pkB}, x_{sigA}, y_{vkB}, x_{skB}, y_{pkA}, x_{sigB}, y_{vkA}\}$. Similarly, Q uses only known keys or keys from P.

Note that these assumptions only restrict keys used in the common signatures. P and Q may of course freely create keys provided they use a different encryption/signing scheme.

It then remains to ensure that the keys established by P (and therefore shared with Q) are distinct from the other keys used by P. This property can be expressed in our logic by considering a special type $\mathtt{test} \in T$, and a process P' obtained from P by adding assignments of the form $[x :=_{\mathtt{test}} t]$ where x a fresh variable, for any t appearing in P as key position w.r.t. the common signature $\mathcal{F}^0$. None of these shared terms should collide with the PKI keys established by P.

C_4. $P' \models \forall x \in \mathtt{test}. \forall y \in \overline{\mathtt{sk}}_H. \forall z \in \overline{\mathtt{sig}}_H. x \neq y \wedge x \neq z \wedge x \neq \mathsf{pk}(y) \wedge x \neq \mathsf{vk}(z)$.

Example 9. Continuing Example 2, the only keys used in key position are $sig[S]$ (in the role of the server) and $\mathsf{vk}(sig[S])$ (when A and B check the certificates). Since none of these keys is freshly bound, the process $P'[\_A, \_B]$ can simply be the process $P[\_A, \_B] \mid [z_1 :=_{\mathtt{test}} sig[S]] \mid [z_2 :=_{\mathtt{test}} \mathsf{vk}(sig[S])]$. Moreover, it is easy to show that no honest agent can be assigned the public key nor the verification key of the server, meaning that $P[\_A, \_B]$ satisfies the condition C_4.

As previously mentioned, to ensure secure composition, we need either our protocols to verify the disjoint-keys hypotheses or the tagging hypotheses. Therefore, we can state the following hypothesis that gathers both cases:

H_4. either condition C_1 holds or conditions C_2, C_3 and C_4 hold.

5 Composition results

The previous section lists necessary assumptions to avoid interferences between a PKI protocol P and a subsequent protocol Q. We are therefore ready to state our result: if Q is secure and if P is a good PKI then Q may securely use P for the establishment of its keys. In fact, we note that such a composition result (still) does not hold in general since a good PKI provides weaker guarantees than an ideal distribution of the keys as usually assumed in the analysis of Q as exemplified in Section 2 We therefore need to introduce a more *permissive* Q which is the final ingredient to our main composition result.

5.1 Permissive Q

Our "confusing material" example in Section 2.3 shows that Q should be analysed without assuming dishonest keys to be honestly generated and distributed. Instead, a *permissive* Q should be considered, where dishonest keys are simply provided by the attacker. The goal of this section is to formally define permissive Q. We assume $d \in \mathcal{N}$ to be a fresh public channel (that is, a name not used elsewhere) and that the names sk and sig do not occur in Q_A and Q_B.

Recall that $Q = Q_A \mid Q_B$ and $x_{skA}, y_{pkB}, \ldots$ are the only possible free variables of Q (cf H_1). The ideal instantiation of the private variables and public variables of an agent A are

$\sigma_A^{\mathsf{priv}} = \{^{sk[A]}/_{x_{skA}}, ^{sig[A]}/_{x_{sigA}}\}$ and $\sigma_B^{\mathsf{pub}} = \{^{\mathsf{pk}(sk[B])}/_{y_{pkB}}, ^{\mathsf{vk}(sig[B])}/_{y_{vkB}}\}$ respectively. Similarly, we define σ_B^{priv} and σ_A^{pub}. However, if A is dishonest, he should be able to chose his public and verification keys freely, i.e., they are under the control of the attacker. Formally, we define

- $I_A^{\mathsf{pub}}[\_] = \mathsf{in}_B(d, y_{pkA}).\mathsf{in}_B(d, y_{vkA}).\_$
- $I_B^{\mathsf{pub}}[\_] = \mathsf{in}_A(d, y_{pkB}).\mathsf{in}_A(d, y_{vkB}).\_$

In the previous section, we stated all the hypotheses that we rely on to ensure a secure composition between the PKI P and the protocol Q. For our first main result, we consider that a *permissive* Q satisfies the secrecy property.

Permissive Q is the protocol Q where honest keys are ideally distributed (and private keys remain private) while dishonest ones are under the control of the attacker.

Definition 3 (Permissive Q). *Let $Q = Q_A \mid Q_B$ be a process satisfying assumptions H_1 and H_2. We define* permissive Q*, denoted Q_{perm}, as the following process:*

$$\begin{array}{l} !^i\,\mathsf{agent}(A, \{H[i]\}).!^j\,\mathsf{agent}(B, \{H[j]\}). \\ \qquad\qquad (O_A[Q_A]\sigma_A^{\mathsf{priv}}\sigma_B^{\mathsf{pub}} \mid O_B[Q_B]\sigma_B^{\mathsf{priv}}\sigma_A^{\mathsf{pub}}) \\ |!^i\,\mathsf{agent}(A, \{D[i]\}).!^j\,\mathsf{agent}(B, \{H[j]\}).I_A^{\mathsf{pub}}[O_B[Q_B]]\sigma_B^{\mathsf{priv}} \\ |!^i\,\mathsf{agent}(A, \{H[i]\}).!^j\,\mathsf{agent}(B, \{D[j]\}).I_B^{\mathsf{pub}}[O_A[Q_A]]\sigma_A^{\mathsf{priv}} \end{array}$$

where $O_A[\_] = \mathsf{out}_A(d, \langle \mathsf{pk}(x_{skA}), y_{pkB}, \mathsf{vk}(x_{sigA}), y_{vkB}\rangle).[z_1 :=_{\mathtt{secret}[A]} x_{skA}].[z_2 :=_{\mathtt{secret}[A]} x_{sigA}].\_$ *with z_1, z_2 fresh and similarly for $O_B[\_]$.*

The process $O_A[\_]$ simply outputs the public keys of A and B as viewed by A and indicates that the private keys of A should stay secret, and similarly for $O_B[\_]$. The first part of Q_{perm} corresponds to sessions between honest agents, where all keys are ideally distributed while the second (resp. third) part of Q_{perm} corresponds to sessions between an honest B (resp. A) and a dishonest A (resp. B).

If permissive Q is secure, then Q can safely be composed with a good PKI.

Theorem 1. *Let $P[\__A, \__B]$ be a context process and $Q = Q_A \mid Q_B$ be a process such that P and Q satisfy hypotheses H_1 to H_4. Let ϕ be a composable property.*

If the following conditions are satisfied

- $!^i\,\mathsf{agent}(A, \{H[i], D[i]\}).!^j\,\mathsf{agent}(B, \{H[j], D[j]\}).$
  $P[O_A, O_B] \models \phi_{\mathsf{PKI}}$ *(that is, P is a secure PKI)*
- $Q_{perm} \models \phi_{sec} \wedge \phi$ *(that is, Q is a secure protocol)*

then $P[Q_A, Q_B]$ is secure, that is

$$!^i\,\mathsf{agent}(A, \{H[i], D[i]\}).!^j\,\mathsf{agent}(B, \{H[j], D[j]\}).P[Q_A, Q_B] \models \phi$$

where $\phi_{sec} \hat{=} \forall \tau \in \overline{\mathtt{secret}}_H.\forall x \in \tau.\not\vdash x.$

Note that we require $P[O_A, O_B]$ to satisfy ϕ_{PKI} and not just P. This is because we need to make sure that P remains a secure PKI even when the public keys are indeed public.

Interestingly, the permissive version of a protocol can easily be encoded and analysed in ProVerif. This is the first lesson learned from our work: if you wish to analyze a protocol Q independently of the underlying PKI, you should analyze permissive Q instead of the ideal (standard) Q. As we shall see in the next section, it may be sufficient to analyse the ideal version of Q, at the price of additional assumptions on either P or Q.

5.2 Composition with an "ideal Q"

As far as we know, in symbolic models protocols are never analyzed in their "permissive" version. Instead, all existing libraries consider all keys to be properly generated and distributed, including those of dishonest parties. We will say that libraries consider *ideal* protocols. As illustrated by our "confusing material" example in Section 2.3, such ideal protocols *are* indeed too abstract and may be flawed when used in conjunction with a true PKI. So a natural question arrises: what about the hundreds of protocols that have already been analyzed? Should all these analysis start over? In this section, we study under which conditions it is sufficient to analyze an ideal protocol Q. Clearly, secure composition requires to a corresponding strenghtening of the guarantees of the PKI.

We first define formally "ideal Q". It consists of the protocol Q where all keys are ideally distributed.

Definition 4 (Ideal Q). *Let $Q = Q_A \mid Q_B$ be a process satisfying assumptions H_1 and H_2. We define* ideal Q*, denoted Q_{ideal}, as the following process:*

$$!^i\,\mathsf{agent}(A, \{H[i], D[i]\}).!^j\,\mathsf{agent}(B, \{H[j], D[j]\}).\\ (O_A[Q_A]\sigma_A^{\mathsf{priv}}\sigma_B^{\mathsf{pub}} \mid O_B[Q_B]\sigma_B^{\mathsf{priv}}\sigma_A^{\mathsf{pub}})$$

where $O_A[\_], O_B[\_], \sigma_A^{\mathsf{priv}}, \sigma_B^{\mathsf{priv}}\sigma_A^{\mathsf{pub}}\sigma_B^{\mathsf{pub}}$ have been defined in Section 5.1.

Process Q_A is instantiated by the expected private keys σ_A^{priv} and public keys σ_B^{pub} of B and similarly for Q_B.

Tagged public keys As illustrated by our "confusing material" example in Section 2.3, when public keys are used as payload, they may interfere with other parts of the protocol. To avoid such intereferences, we need public keys to be "isolated". So, similarly to the case of private keys (Assumption H_9), we now require that public keys used as payload are isolated within a tag. We further require that only PKI keys may be used for asymmetric encryption/decryption in Q. This is more formally stated as follows.

H_5. In the processes Q_A and Q_B, the public and verification keys provided by the PKI can only be used in key position with $\mathsf{aenc}, \mathsf{raenc}, \mathsf{check}$ respectively or below a tag tagk. Moreover, only the private, public, signing, verification keys provided by the PKI can be used in key position with the common signature or below a tag tagk.

Such an assumption is trivially satisfied when public keys are not used as payload but only for encryption. However, a lesson learned from our analysis is that for protocols that use public key as payloads then either permissive Q should be analyzed or tagging public keys is necessary.

Ideal PKI Even if public keys are properly used in Q, the attacker can control dishonest public keys and interferes with Q's behavior, as exemplified in Section 2.5 where we show unexpected behaviors if honest agents do not share the same view of dishonest keys. Therefore, we consider an additional property which ensures that public and verification keys of dishonest agents are consistently distributed among honest agents. This is formally captured by formula ϕ_{ideal} as follows.

$$\begin{aligned}\phi_{ideal} \mathrel{\hat{=}} \forall A, B \in \overline{\mathcal{A}}_H.\forall C, D \in \overline{\mathcal{A}}.\\ \forall x \in \mathbb{pk}[A, C].\forall y \in \mathbb{pk}[B, D].C = D \Leftrightarrow x = y\\ \wedge\ \forall x \in \mathbb{vk}[A, C].\forall y \in \mathbb{vk}[B, D].C = D \Leftrightarrow x = y\\ \wedge\ \forall x \in \mathbb{pk}[A, C].\forall y \in \mathbb{vk}[A, C].x \neq y\end{aligned}$$

The first line ensures that all agents share the same public key for a given agent C and that conversely, public keys of distinct agents are pairwise distinct. The second lines states the same property for verification keys. Finally, public and verification keys should of course be distinct.

Such strong guarantees are typically met when public keys are issued by a (trusted) authority, for example a governmental agency that issues electronic IDs.

The next theorem establishes that analysis of the ideal version of a protocol Q still enables secure composition with a PKI protocol P, provided that P satisfies ϕ_{PKI} and ϕ_{ideal}.

Theorem 2. *Let $P[\_{A}, \_{B}]$ be a context process and $Q = Q_A \mid Q_B$ be a process such that P and Q satisfy hypotheses H_1 to H_5. Let ϕ be a composable property.*

If the following conditions are satisfied

- *$C[P[O_A, O_B]] \models \phi_{\mathsf{PKI}} \wedge \phi_{ideal}$ (that is, P is an ideal PKI)*
- *$Q_{ideal} \models \phi_{sec} \wedge \phi$ (that is, Q is an ideal secure protocol)*

then $P[Q_A, Q_B]$ is secure, that is $C[P[Q_A, Q_B]] \models \phi$ where $C[\_] = !^i\, \mathsf{agent}(A, \{H[i], D[i]\}).!^j\, \mathsf{agent}(B, \{H[j], D[j]\}).\_$.

6 Conclusion

Standalone analysis of protocols that rely on long term asymmetric keys typically assumes idealized key distribution through some PKI. Yet, this property is not naturally guaranteed by standard PKIs. We have therefore initiated a study of the conditions under which the composition of PKIs (for both asymmetric encryption and digital signatures) with arbitrary protocols that require such keys yields a secure system.

We have shown that this is possible through modular analysis which considers the two protocols separately and requires minimal, easy to implement and verify conditions on how the two components of the composition interact. In short, we have identified several useful recommendations. To deal with the weaker guarantees offered by PKIs, the *permissive* version of the protocol that uses PKI keys should be analyzed rather than its *ideal* version. In addition, to eliminate unwanted interference between the two components of the composition the protocols should not share any keys (beyond those that the PKI distributes). In fact, standards already suggest that this should be the case – our analysis confirms that this guarantee helps guarantee the desired composability between protocols. Finally, we have shown that under some conditions, security analysis of protocols that assumes idealized key distribution is sound if the PKI also guarantees a consistent distribution of dishonest keys.

In our study, we also identified several cases where composition is not secure, and provided examples. Some of these examples are contrived. As future work, we plan to explore whether real case protocols cannot indeed be composed, or alternatively, identify why "realistic" examples do not run into the same issues and formalize the corresponding theorems.

References

1. M. Abadi and C. Fournet. Mobile values, new names, and secure communication. In *Proc. of the 28th ACM Symposium on Principles of Programming Languages (POPL'01)*, pages 104–115, January 2001.
2. M. Arapinis, V. Cheval, and S. Delaune. Composing security protocols: from confidentiality to privacy. In R. Focardi and A. Myers, editors, *Proceedings of the 4th International Conference on Principles of Security and Trust (POST'15)*, Lecture Notes in Computer Science, London, UK, Apr. 2015. Springer Berlin Heidelberg.
3. A. Armando, D. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuellar, P. Hankes Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron. The AVISPA Tool for the automated validation of internet security protocols and applications. In K. Etessami and S. Rajamani, editors, *17th International Conference on Computer Aided Verification, CAV'2005*, volume 3576 of *Lecture Notes in Computer Science*, pages 281–285, Edinburgh, Scotland, 2005. Springer.
4. B. Barak, R. Canetti, J. B. Nielsen, and R. Pass. Universally composable protocols with relaxed set-up assumptions. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science*, FOCS '04, pages 186–195, Washington, DC, USA, 2004. IEEE Computer Society.

5. B. Blanchet. An efficient cryptographic protocol verifier based on prolog rules. In *Proc. CSFW'01*, 2001.
6. F. Bohl and D. Unruh. Symbolic universal composability. In *Proceedings of the 2013 IEEE 26th Computer Security Foundations Symposium*, CSF '13, pages 257–271, Washington, DC, USA, 2013. IEEE Computer Society.
7. A. Boldyreva, M. Fischlin, A. Palacio, and B. Warinschi. A closer look at PKI: security and efficiency. In T. Okamoto and X. Wang, editors, *Public Key Cryptography - PKC 2007, 10th International Conference on Practice and Theory in Public-Key Cryptography, Beijing, China, April 16-20, 2007, Proceedings*, volume 4450 of *Lecture Notes in Computer Science*, pages 458–475. Springer, 2007.
8. C. Boyd, C. Cremers, M. Feltz, K. G. Paterson, B. Poettering, and D. Stebila. ASICS: authenticated key exchange security incorporating certification systems. In J. Crampton, S. Jajodia, and K. Mayes, editors, *Computer Security - ESORICS 2013 - 18th European Symposium on Research in Computer Security, Egham, UK, September 9-13, 2013. Proceedings*, volume 8134 of *Lecture Notes in Computer Science*, pages 381–399. Springer, 2013.
9. C. Brzuska, M. Fischlin, N. P. Smart, B. Warinschi, and S. C. Williams. Less is more: relaxed yet composable security notions for key exchange. *Int. J. Inf. Sec.*, 12(4):267–297, 2013.
10. C. Brzuska, M. Fischlin, B. Warinschi, and S. C. Williams. Composability of bellare-rogaway key exchange protocols. In Y. Chen, G. Danezis, and V. Shmatikov, editors, *Proceedings of the 18th ACM Conference on Computer and Communications Security, CCS 2011, Chicago, Illinois, USA, October 17-21, 2011*, pages 51–62. ACM, 2011.
11. J. Camenisch, R. R. Enderlein, S. Krenn, R. Küsters, and D. Rausch. Universal composition with responsive environments. In J. H. Cheon and T. Takagi, editors, *Advances in Cryptology - ASIACRYPT 2016 - 22nd International Conference on the Theory and Application of Cryptology and Information Security, Hanoi, Vietnam, December 4-8, 2016, Proceedings, Part II*, volume 10032 of *Lecture Notes in Computer Science*, pages 807–840, 2016.
12. R. Canetti. Universally composable security: A new paradigm for cryptographic protocols. In *42nd Annual Symposium on Foundations of Computer Science, FOCS 2001, 14-17 October 2001, Las Vegas, Nevada, USA*, pages 136–145. IEEE Computer Society, 2001.
13. R. Canetti, L. Cheung, D. K. Kaynar, M. Liskov, N. A. Lynch, O. Pereira, and R. Segala. Time-bounded task-pioas: A framework for analyzing security protocols. In S. Dolev, editor, *DISC*, volume 4167 of *Lecture Notes in Computer Science*, pages 238–253. Springer, 2006.
14. V. Cheval, V. Cortier, and E. le Morvan. Secure Refinements of Communication Channels. In P. Harsha and G. Ramalingam, editors, *35th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2015)*, volume 45 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 575–589, Dagstuhl, Germany, 2015. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.
15. C. Chevalier, S. Delaune, S. Kremer, and M. D. Ryan. Composition of password-based protocols. *Formal Methods in System Design*, 43(3):369–413, 2013.
16. Ş. Ciobâcă and V. Cortier. Protocol composition for arbitrary primitives. In *Proceedings of the 23rd IEEE Computer Security Foundations Symposium (CSF'10)*, pages 322–336. IEEE Computer Society Press, July 2010.
17. V. Cortier and S. Delaune. Safely composing security protocols. *Formal Methods in System Design*, 34(1):1–36, Feb. 2009.
18. C. Cremers. The Scyther Tool: Verification, falsification, and analysis of security protocols. In *Computer Aided Verification, 20th International Conference, CAV 2008, Princeton, USA, Proc.*, volume 5123/2008 of *Lecture Notes in Computer Science*, pages 414–418. Springer, 2008.
19. S. Delaune, S. Kremer, and O. Pereira. Simulation based security in the applied pi calculus. In R. Kannan and K. N. Kumar, editors, *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2009, December 15-17, 2009, IIT Kanpur, India*, volume 4 of *LIPIcs*, pages 169–180. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2009.
20. N. Dershowitz and J.-P. Jouannaud. Rewrite systems. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume B, chapter 6, pages 243–320. Elsevier,, 1990.
21. Y. Dodis, J. Katz, A. Smith, and S. Walfish. Composability and on-line deniability of authentication. In *Proceedings of the 6th Theory of Cryptography Conference on Theory of Cryptography*, TCC '09, pages 146–162, Berlin, Heidelberg, 2009. Springer-Verlag.
22. T. Gibson-Robinson, A. Kamil, and G. Lowe. Verifying layered security protocols. *Journal of Computer Security*, 23(3), 2015.
23. D. Hofheinz, E. Kiltz, and V. Shoup. Practical chosen ciphertext secure encryption from factoring. *J. Cryptology*, 26(1):102–118, 2013.

24. R. Kusters. Simulation-based security with inexhaustible interactive turing machines. In *Proceedings of the 19th IEEE Workshop on Computer Security Foundations*, CSFW '06, pages 309–320, Washington, DC, USA, 2006. IEEE Computer Society.
25. G. Lowe. Breaking and fixing the Needham-Schroeder public-key protocol using FDR. In T. Margaria and B. Steffen, editors, *Tools and Algorithms for the Construction and Analysis of Systems (TACAS'96)*, volume 1055 of *LNCS*, pages 147–166. Springer-Verlag, march 1996.
26. S. Meier, B. Schmidt, C. Cremers, and D. Basin. The TAMARIN Prover for the Symbolic Analysis of Security Protocols. In N. Sharygina and H. Veith, editors, *Computer Aided Verification, 25th International Conference, CAV 2013, Princeton, USA, Proc.*, volume 8044 of *Lecture Notes in Computer Science*, pages 696–701. Springer, 2013.
27. S. Moedersheim and L. Viganò. Sufficient conditions for vertical composition of security protocols. In *ASIACCS*, pages 435–446, 2014.
28. B. Pfitzmann and M. Waidner. Composition and integrity preservation of secure reactive systems. In D. Gritzalis, S. Jajodia, and P. Samarati, editors, *CCS 2000, Proceedings of the 7th ACM Conference on Computer and Communications Security, Athens, Greece, November 1-4, 2000.*, pages 245–254. ACM, 2000.

A Tagging

We extend in this section the tagging scheme presented in [2]. In these paper, a tag is systematically added in all encryptions and signatures of the common signature. It allows us to ensure that a message coming from the protocol Q is not assimilated as a message of the protocol P, and vice versa.

Example 10. Consider two simple process $P = \mathsf{out}_A(c, \mathsf{senc}(s,k))$ and $Q = \mathsf{in}_A(c,x).\mathsf{out}_A(c, \mathsf{sdec}(x,k))$. Individually, P and Q both preserve the secrecy of s however $P \mid Q$ and $P \cdot Q$ do not preserves the secrecy s.

Similarly [2], we consider that protocols can only share a fix set of primitives that we denote by Σ_0 as defined as follows:

$$\Sigma_0 = \{\mathsf{sdec}, \mathsf{senc}, \mathsf{adec}, \mathsf{aenc}, \mathsf{pk}, \langle,\rangle, \mathsf{proj}_1, \mathsf{proj}_2, \mathsf{sign}, \mathsf{check}, \mathsf{vk}, \mathsf{h}\}$$

We associate to Σ_0 a rewrite system $\mathcal{R}_0$ defined as follows:

$$\begin{array}{rr} \mathsf{sdec}(\mathsf{senc}(x,y),y) \to x & \mathsf{check}(\mathsf{sign}(x,y),\mathsf{vk}(y)) \to x \\ \mathsf{adec}(\mathsf{aenc}(x,\mathsf{pk}(y)),y) \to x & \mathsf{proj}_i(\langle x_1,x_2\rangle) \to x_i \text{ with } i \in \{1,2\}) \\ \mathsf{rsdec}(\mathsf{rsenc}(x,y,z),z) \to x & \mathsf{radec}(\mathsf{raenc}(x,y,\mathsf{pk}(z)),z) \to x \end{array}$$

We also consider a family of signatures $\Sigma_1, \ldots, \Sigma_{N_{sig}}$ disjoint from each other and disjoint from Σ_0. In order to tag a process, we introduce a new family of signatures $\Sigma_1^{\mathsf{tag}}, \ldots, \Sigma_{N_{sig}}^{\mathsf{tag}}$. For each $\eta \in \{1, \ldots, N_{sig}\}$, we have that $\Sigma_\eta^{\mathsf{tag}} = \{\mathsf{tag}_\eta, \mathsf{untag}_\eta\}$ where tag_η and untag_η are two function symbols of arity 1 that we will use for tagging. The role of the tag_η function is to tag its argument with the tag η. The role of the untag_η function is to remove the tag. To model this interaction between tag_η and untag_η, we consider the rewrite system: $\mathcal{R}_\eta^{\mathsf{tag}} = \{\mathsf{untag}_\eta(\mathsf{tag}_\eta(x)) \to x\}$.

Note that even though we consider the composition of only two protocols, say P and Q, we still consider N_{sig} disjoint signatures. In fact, we will assume that P relies on some of the signatures $\Sigma_1, \ldots, \Sigma_{N_{sig}}$ while Q relies on the remaining signature. In term of signature, it would have been similar to consider a unique signature for P and a unique signature for Q, in addition to the common signature. However, the resulting tagged process would have been different. Indeed, tagging a process is syntactical transformation that depends on the signature we consider. Hence, if P (or Q) already correspond to the composition of tagged processes then P is in fact uniformly tagged. What matters is that the tags used in P differs from the one used in Q. As such, we split the set $\{1, \ldots, N_{sig}\}$ into two disjoint sets α and β. Given a set $\gamma \subseteq \{1, \ldots, N_{sig}\}$, we will denote

$$\begin{array}{lll} \Sigma_\gamma \mathrel{\hat{=}} \bigcup_{\eta\in\gamma} \Sigma_\eta & \Sigma_\gamma^{\mathsf{tag}} \mathrel{\hat{=}} \bigcup_{\eta\in\gamma} \Sigma_\eta^{\mathsf{tag}} & \Sigma_\gamma^+ \mathrel{\hat{=}} \Sigma_\gamma \cup \Sigma_\gamma^{\mathsf{tag}} \\ \mathrm{E}_\gamma \mathrel{\hat{=}} \bigcup_{\eta\in\gamma} \mathrm{E}_\eta & \mathrm{E}_\gamma^{\mathsf{tag}} \mathrel{\hat{=}} \bigcup_{\eta\in\gamma} \mathrm{E}_\eta^{\mathsf{tag}} & \mathrm{E}_\gamma^+ \mathrel{\hat{=}} \mathrm{E}_\gamma \cup \mathrm{E}_\gamma^{\mathsf{tag}} \end{array}$$

Definition 5. *Let $\eta \in \{1, \ldots, N_{sig}\}$. We define the* set of tagged terms w.r.t. η, *denoted* $\textsc{Tag}\mathrm{T}(\eta)$, *as a set of elements of the form (u, K_s, K_a) where u is term built on $\Sigma_\eta^+ \cup \Sigma_0$ and K_s, K_a are sets of terms built on $\Sigma_\eta^+ \cup \Sigma_0$. Moreover, $\textsc{Tag}\mathrm{T}(\eta)$ is the smallest set such that for all $(u_1, K_s^1, K_a^1), \ldots, (u_n, K_s^n, K_a^n) \in \textsc{Tag}\mathrm{T}(\eta)$, for all $\mathsf{f}/n \in \Sigma$, for all $v \in \mathcal{N} \cup \mathcal{X}$, if we denote $K_s = K_s^1 \cup \ldots \cup K_s^n$ and $K_a = K_a^1 \cup \ldots \cup K_a^n$ then*

1. $(v, \emptyset, \emptyset) \in \textsc{Tag}\mathrm{T}(\eta)$
2. $(\mathsf{f}(u_1, \ldots, u_n), K_s \cup \{u_n\}, K_a)$ *if* $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{sdec}, \mathsf{rsdec}\}$
3. $(\mathsf{f}(u_1, \ldots, u_n), K_s, K_a \cup \{u_n\})$ *if* $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}, \mathsf{check}\}$
4. $(\mathsf{f}(u_1, \ldots, u_n), K_s, K_a \cup \{\mathsf{pk}(u_n)\}) \in \textsc{Tag}\mathrm{T}(\eta)$ *if* $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}\}$
5. $(\mathsf{f}(u_1, \ldots, u_n), K_s, K_a \cup \{\mathsf{vk}(u_n)\}) \in \textsc{Tag}\mathrm{T}(\eta)$ *if* $\mathsf{f} = \mathsf{sign}$
6. $(\mathsf{untag}_\eta(\mathsf{f}(u_1, \ldots, u_n)), K_s, K_a) \in \textsc{Tag}\mathrm{T}(\eta)$ *if* $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{adec}, \mathsf{rsdec}, \mathsf{radec}, \mathsf{check}\}$
7. $(\mathsf{f}(\mathsf{tag}_\eta(u_1), u_2, \ldots, u_n), K_s, K_a) \in \textsc{Tag}\mathrm{T}(\eta)$ *if* $\mathsf{f} \in \{\mathsf{senc}, \mathsf{aenc}, \mathsf{rsenc}, \mathsf{raenc}, \mathsf{sign}\}$
8. $(\mathsf{f}(u_1, \ldots, u_n), K_s, K_a) \in \textsc{Tag}\mathrm{T}(\eta)$ *when* $\mathsf{f} \in \{\mathsf{h}, \langle\,\rangle, \mathsf{proj}_1, \mathsf{proj}_2, \mathsf{vk}, \mathsf{pk}, \mathsf{tag}_\eta, \mathsf{tagk}_\eta\} \cup \Sigma_\eta$

Definition 6. *Let $\eta \in \{1,\ldots,N_{sig}\}$. We define the* set of fully tagged terms w.r.t. η, *denoted* $\text{FTAGT}(\eta)$, *as* $\{u \mid (u,\emptyset,\emptyset) \in \text{TAGT}(\eta)\}$.

From a process representing a composition of two protocols, it is not necessary clear which part of the process comes from one of the protocol or from the other. However, in order to correctly tag the complete process, we need to know which tag to use for each individual actions. In [**?**,2], the authors consider that a process is colored by the indices from $\{1,\ldots,p\}$. Typically, they augment the syntax of process with index from $\{1,\ldots,p\}$ representing the tag we should use in order to tag the process.

Definition 7 (Colored plain process). *A colored plain process is a plain process where all outputs, input, conditionals, events and assignments are annotated by an element of* $\{1,\ldots,N_{sig}\}$. *Moreover, we require that all actions colored by* $\eta \in \{1,\ldots,N_{sig}\}$ *can only contain terms in the signature* $\Sigma_\eta^+ \cup \Sigma_0$. *Given a set* $\gamma \subseteq \{1,\ldots,N_{sig}\}$, *we say than an action is colored with* γ *if this action is colored by* $\eta \in \{1,\ldots,N_{sig}\}$.

Definition 8 (Fully tagged process). *Consider a set* $\eta \subseteq \{1,\ldots,N_{sig}\}$. *We say that* P *is fully tagged w.r.t.* η *if all actions of* P *are colored by* η *and all terms contained in an action of* P *are in* $\text{FTAGT}(\eta)$.

B Material for combination

To handle the different signatures and equational theories, we consider the notion of *ordered rewriting*. It has been shown that by applying the *unfailing completion procedure* to E where $\text{E} = \mathcal{R}_1 \uplus \text{E}_1 \uplus \mathcal{R}_2 \uplus \text{E}_2 \uplus \ldots \uplus \mathcal{R}_{N_{sig}} \uplus \text{E}_{N_{sig}}$ is the union of disjoint rewriting systems and equational theories $(\mathcal{F}_i, \mathcal{R}_i, \text{E}_i)$ where $\mathcal{F}_i = \mathcal{F}_c^i \uplus \mathcal{F}_d^i$ (for all i,j, we have that $\mathcal{F}_i \cap \mathcal{F}_j = \emptyset$), we can derive a (possibly infinite) set of equations $\mathcal{O}$ such that on ground terms:

1. the relations $=_{\mathcal{O}}$ and $=_{\mathcal{R},\text{E}}$ are equal,
2. the rewriting system $\rightarrow_{\mathcal{O}}$ is convergent.

Since the relation $\rightarrow_{\mathcal{O}}$ is convergent on ground terms, we define $M{\downarrow_{\mathcal{R},\text{E}}}$ (or briefly $M{\downarrow}$) as the unique normal form of the ground term M for $\rightarrow_{\mathcal{O}}$. These notations are extended as expected to sets of terms.

We now introduce our notion of *factors* and state some properties on them w.r.t. the different equational theories. A similar notion is also used in [**?**].

Definition 9 (factors). *Let* $M \in \mathcal{T}(\Sigma, \mathcal{N} \cup \mathcal{X})$. *The* factors *of* M, *denoted* $Fct(M)$, *are the maximal syntactic subterms of* M *that are alien to* M

Lemma 1. *Let* M *be a ground term such that all its factors are in normal form and* $\mathsf{root}(M) \in \Sigma_i$. *Then*

- *either* $M{\downarrow} \in Fct(M) \cup \{n_{min}\}$,
- *or* $\mathsf{root}(M{\downarrow}) \in \Sigma_i$ *and* $Fct(M{\downarrow}) \subseteq Fct(M) \cup \{n_{min}\}$.

Lemma 2. *Let* t *be a ground term with* $t = C_1[u_1,\ldots,u_n]$ *where* C_1 *is a context built on* Σ_i, $i \in \{1,\ldots,p\}$ *and the terms* $u_1,\ldots,u_n$ *are the factors of* t *in normal form. Let* C_2 *be a context built on* Σ_i *(possibly a hole) such that* $t{\downarrow} = C_2[u_{j_1},\ldots,u_{j_k}]$ *with* $j_1,\ldots,j_k \in \{0\ldots n\}$ *and* $u_0 = n_{min}$ *(the existence is given by Lemma 1). We have that for all ground terms* $v_1,\ldots,v_n$ *in normal form and alien to* t, *if*

$$\textit{for every } q,q' \in \{1\ldots n\} \textit{ we have } u_q = u_{q'} \Leftrightarrow v_q = v_{q'}$$

then $C_1[v_1,\ldots,v_n]{\downarrow} = C_2[v_{j_1},\ldots,v_{j_k}]$ *with* $v_0 = n_{min}$.

A proof of these lemmas can be found in [**?**,**?**].

C Name replacement

Now that we have fixed some notations, we have to explain how the replacement will be applied on the shared process to extract the disjoint case. Actually a same term will be abstracted differently depending on the context which is just above it.

In this section given $\gamma \subseteq \{1, \ldots, N_{sig}\}$, and given $S_1, \ldots, S_{N_{sig}}$ sets, we will denote S_γ the set $\bigcup_{i \in \gamma} S_i$. Let us consider α and β two sets such that $\alpha \cup \beta = \{1, \ldots, p\}$ and $\alpha \cap \beta = \emptyset$. Moreover, we consider the predicate $\mathcal{P}_{keys}(\mathsf{Ks}, \mathsf{Ka})$ to hold if and only if

- $\mathsf{Ks} = [\mathsf{Ks}_i]_{i=1}^{N_{sig}}$, $\mathsf{Ka} = [\mathsf{Ka}_i]_{i=1}^{N_{sig}}$, and
- for all $i, j \in \{1, \ldots, p\}$, if $i \neq j$ then $\mathsf{Ks}_i \cap \mathsf{Ks}_j = \emptyset$ and $\mathsf{Ka}_i \cap \mathsf{Ka}_j = \emptyset$, and
- for all $i \in \{1, \ldots, p\}$, for all $u \in \mathsf{Ka}_i$, $\mathsf{root}(u) \in \{\mathsf{vk}, \mathsf{pk}\}$

for some sets $\mathsf{Ks}_1, \ldots, \mathsf{Ks}_{N_{sig}}, \mathsf{Ka}_1, \ldots, \mathsf{Ka}_{N_{sig}}$ of ground messages in normal form. We will also sometimes assimilate Ks and Ka respectively for the sets $\bigcup_{i=1}^{N_{sig}} \mathsf{Ks}_i$ and $\bigcup_{i=1}^{N_{sig}} \mathsf{Ka}_i$.

Definition 10. *Let u be a ground message in normal form. Let $\mathsf{Ks} = [\mathsf{Ks}_i]_{i=1}^{N_{sig}}$ and $\mathsf{Ka} = [\mathsf{Ka}_i]_{i=1}^{N_{sig}}$ two sequences of of sets of messages in normal form. We define $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u)$, namely the tag of the root of u w.r.t. Ks and Ka as follows:*

- $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = \bot$ *when* $u \in \mathcal{N} \cup \mathcal{X}$*;*
- $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = i$ *if* $u = \mathsf{f}(u_1, \ldots, u_n)$ *and either*
  - $\mathsf{f} \in \Sigma_i^+$*; or*
  - $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}\}$ *and either* $u_n \in \mathsf{Ks}_i$ *or* $\mathsf{root}(u_1) = \mathsf{tag}_i$ *and* $u_n \notin \mathsf{Ks}$ *; or*
  - $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$ *and either* $u_n \in \mathsf{Ka}_i$ *or* $\mathsf{root}(u_1) = \mathsf{tag}_i$ *and* $u_n \notin \mathsf{Ka}$*; or*
  - $\mathsf{f} \in \mathsf{sign}$ *and either* $\mathsf{vk}(u_2) \in \mathsf{Ka}_i$ *or* $\mathsf{root}(u_1) = \mathsf{tag}_i$ *and* $\mathsf{vk}(u_2) \notin \mathsf{Ka}$
- $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = 0$ *otherwise.*

Definition 11 (Compatibility). *Let ρ_α, ρ_β be two mappings from $\mathcal{X}$ to $\mathcal{N}$. We define the set* Compatible$(\rho_\alpha, \rho_\beta)$ *as the smallest set such that for all substitutions σ of ground messages in normal form, if for all $\gamma \in \{\alpha, \beta\}$, for all $x, y \in \mathrm{dom}(\sigma) \cap \mathrm{dom}(\rho_\gamma)$, $x\sigma =_{\mathrm{E}} y\sigma \Leftrightarrow x\rho_\gamma = y\rho_\gamma$ then $\sigma \in$* Compatible$(\rho_\alpha, \rho_\beta)$*.*

For all $\sigma \in$ Compatible$(\rho_\alpha, \rho_\beta)$*, for all $\gamma \in \{\alpha, \beta\}$, we define the* extension *of ρ_γ w.r.t. σ, denoted ρ_γ^σ, as follows:*

- $\mathrm{dom}(\rho_\gamma^\sigma) = \{x\sigma \mid x \in \mathrm{dom}(\rho_\gamma) \cap \mathrm{dom}(\sigma)\}$*, and*
- *for any $x \in \mathrm{dom}(\rho_\gamma) \cap \mathrm{dom}(\sigma)$, $\rho_\gamma^\sigma(x\sigma) \mathrel{\hat{=}} \rho_\gamma(x)$.*

Note that ρ_γ^σ and ρ_β^σ are injective.

Similarly to [2], we introduce a function that will transform a message in normal form into its abstraction. However, in this paper, we relax some hypothesis on the management of public keys. In particular, in [2], they only allow names as argument for the function symbol pk and vk. Furthermore, they also consider some restriction on the shape of the keys that can be passed down from one protocol to the other, *e.g.* it cannot be a pair or a hash. For the rest of this paper, we consider an infinite set $\mathcal{N}_{abs} \subseteq \mathcal{N}$ such that $n_{min} \notin \mathcal{N}_{abs}$.

Definition 12 (Setup). *A* setup *is a tuple $(\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ where:*

- *ρ_α, ρ_β are two mappings from $\mathcal{X}$ to $\mathcal{N}_{abs}$; and*
- *μ_α, μ_β are two injective mappings from ground terms to $\mathcal{N}_{abs}$; and*
- *Ks, Ka are two sequences of sets of ground terms in normal form; and*
- *$\mathsf{H}_\alpha, \mathsf{H}_\beta$ are two sets of ground terms in normal form; and*
- *σ is a substitution of ground messages in normal form.*

Moreover, the following properties are satisfied:

1. *$\mathcal{P}_{keys}(\mathsf{Ks}, \mathsf{Ka})$ and $\sigma \in$* Compatible$(\rho_\alpha, \rho_\beta)$

2. $\mathrm{dom}(\rho^\sigma_\alpha)$, $\mathrm{dom}(\rho^\sigma_\beta)$, $\mathrm{dom}(\mu_\alpha)$, $\mathrm{dom}(\mu_\beta)$, H_α *and* H_β *are pairwise disjoint except the pairs* $(\mathrm{dom}(\rho^\sigma_\alpha), \mathrm{dom}(\mu_\alpha))$, $(\mathrm{dom}(\rho^\sigma_\beta), \mathrm{dom}(\mu_\beta))$, $(\mathrm{dom}(\rho^\sigma_\alpha), \mathsf{H}_\alpha)$ *and* $(\mathrm{dom}(\rho^\sigma_\beta), \mathsf{H}_\beta)$
3. $\mathrm{img}(\rho^\sigma_\alpha)$, $\mathrm{img}(\rho^\sigma_\beta)$, $\mathrm{img}(\mu_\alpha)$, $\mathrm{img}(\mu_\beta)$ *are pairwise disjoint*
4. $\mathrm{img}(\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta) \subseteq \mathcal{N}_{abs}$ *and* $names(\mathrm{img}(\sigma), \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta, \mu_\alpha, \mu_\beta), \mathsf{Ks}, \mathsf{Ka}, \mathsf{H}_\alpha, \mathsf{H}_\beta) \cap \mathcal{N}_{abs} = \emptyset$
5. $n_{min} \notin \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta, \mu_\alpha, \mu_\beta) \cup \mathsf{Ks}$
6. $\forall \gamma \in \{\alpha, \beta\}$, $\forall t \in \mathrm{dom}(\mu_\gamma)$, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t) \notin \gamma \cup \{0\}$
7. $\forall \gamma \in \{\alpha, \beta\}$, $\forall t \in \mathrm{dom}(\rho^\sigma_\gamma)$, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t) \notin \gamma$ *and if* $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t) = 0$ *then* $\mathsf{root}(t) \in \{\mathsf{pk}, \mathsf{vk}, \langle\,\rangle, \mathsf{h}\}$
8. $\forall t \in \mathsf{H}_\alpha \cup \mathsf{H}_\beta$, $\mathsf{root}(t) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$
9. $\mathsf{Ka} \cap \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta) = \emptyset$, $\mathsf{Ka}_\alpha \cap \mathsf{H}_\alpha = \emptyset$ *and* $\mathsf{Ka}_\beta \cap \mathsf{H}_\beta = \emptyset$

Definition 13 (Transformation). *Let $\mathcal{S}$ be a setup. The* transformation functions of $\mathcal{S}$ *are two mappings* tr *and* trH *from $\{\alpha, \beta\}$ and terms to terms, and defined as follows: For all $\gamma \in \{\alpha, \beta\}$, for all terms u,*

1. $\mathsf{tr}(\gamma, u) = u\rho^\sigma_\gamma$ *when* $u \in \mathrm{dom}(\rho^\sigma_\gamma)$
2. *otherwise* $\mathsf{tr}(\gamma, u) = \mathsf{trH}(\gamma, u)$ *when* $u \in \mathsf{H}_\gamma$
3. *otherwise* $\mathsf{tr}(\gamma, u) = u\mu_\gamma$ *when* $u \in \mathrm{dom}(\mu_\gamma)$
4. *otherwise* $\mathsf{tr}(\gamma, u) = u$ *when u is a name*
5. *otherwise* $\mathsf{tr}(\gamma, u) = \mathsf{f}(\mathsf{tr}_\omega(u_1), \ldots, \mathsf{tr}_\omega(u_n))$ *when* $u = \mathsf{f}(u_1, \ldots, u_n)$, $\omega = \gamma$ *(resp. α, β) and* $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = 0$ *(resp. $\in \alpha$, $\in \beta$).*

For all $\gamma \in \{\alpha, \beta\}$, for all terms u,

6. $\mathsf{trH}(\gamma, u) = u\mu_\gamma$ *when* $u \in \mathrm{dom}(\mu_\gamma)$
7. *otherwise* $\mathsf{trH}(\gamma, u) = \mathsf{f}(\mathsf{trH}(\gamma, u_1), \ldots, \mathsf{trH}(\gamma, u_n))$ *when* $u = \mathsf{f}(u_1, \ldots, u_n)$ *and either* $\mathsf{f} = \langle\,\rangle$ *or* $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ *and* $u \in \mathsf{H}_\gamma$
8. *otherwise* $\mathsf{trH}(\gamma, u) = \mathsf{tr}(\gamma, u)$.

In the rest of this paper, we will also denote $\mathsf{trH}(\gamma, u)$ and $\mathsf{trH}(\gamma, u)$ by $\mathsf{trH}_\gamma(u)$ and $\mathsf{trH}_\gamma(u)$ respectively.

Lemma 3. *Let $\mathcal{S}$ be a setup and let* tr *and* trH *the transformation functions of $\mathcal{S}$. Let t_1 and t_2 be ground messages in normal form such that $names(t_1, t_2) \cap \mathcal{N}_{abs} = \emptyset$. We have that for all $\gamma, \omega \in \{\alpha, \beta\}$, for all $\delta, \delta' \in \{\mathsf{tr}, \mathsf{trH}\}$, $\delta(\gamma, t_1) = \delta'(\omega, t_2)$ implies $t_1 = t_2$.*

Proof. We prove the result by induction on $\max(|t_1|, |t_2|)$.

Base case $\max(|t_1|, |t_2|) = 1$*:* Let $\gamma, \omega \in \{\alpha, \beta\}$. Let $\delta, \delta' \in \{\mathsf{tr}, \mathsf{trH}\}$. In such a case, we have that $t_1, t_2 \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$. Note that by Property 8 of Definition 12, $t_1, t_2 \notin \mathsf{H}_\gamma \cup \mathsf{H}_\omega$.

We do a small case analysis:

- Case $\delta(\gamma, t_1) \in \mathrm{img}(\rho^\sigma_\gamma)$: In such a case, $\delta'(\omega, t_2) \in \mathrm{img}(\rho^\sigma_\gamma)$. By Properties 4 and 3 of Definition 12 and since $names(t_1, t_2) \cap \mathcal{N}_{abs} = \emptyset$, we deduce that $\delta = \delta' = \mathsf{tr}$ and $\gamma = \omega'$. Thus, $\delta(\gamma, t_1) = t_1\rho^\sigma_\gamma = t_2\rho^\sigma_\gamma = \delta'(\omega, t_2)$. But ρ^σ_γ is injective. Therefore, we conclude that $t_1 = t_2$.
- Case $\delta'(\omega, t_2) \in \mathrm{img}(\rho^\sigma_\omega)$: Similar to previous case.
- Case $\delta(\gamma, t_1) \in \mathrm{img}(\mu_\gamma)$: In such a case, $\delta'(\omega, t_2) \in \mathrm{img}(\mu_\gamma)$. By Properties 4 and 3 of Definition 12 and since $names(t_1, t_2) \cap \mathcal{N}_{abs} = \emptyset$, we deduce that $\gamma = \omega'$. Moreover, by Definition 13, we deduce that $\delta(\gamma, t_1) = t_1\mu_\gamma = t_2\mu_\gamma = \delta'(\omega, t_2)$. But μ_γ is injective. Therefore, we conclude that $t_1 = t_2$.
- Case $\delta(\omega, t_2) \in \mathrm{img}(\mu_\omega)$: Similar to previous case.
- Otherwise, by Definition 13, we deduce that $\delta(\gamma, t_1) = t_1$ and $\delta'(\omega, t_2) = t_2$ meaning that $t_1 = t_2$.

Inductive step $\max(|t_1|, |t_2|) > 1$*:* Assume w.l.o.g. that $|t_1| > 1$. Thus, there exists a symbol function f and terms $u_1, \ldots u_n$ such that $t_1 = \mathsf{f}(u_1, \ldots u_n)$. Let $\gamma, \omega \in \{\alpha, \beta\}$. Let us first assume that $\delta = \mathsf{tr}$. We do a case analysis on t_1 which is in normal form.

– Case $t_1 \in \mathrm{dom}(\rho^{\sigma}_{\gamma})$: In such a case $\delta(\gamma, t_1) \in \mathrm{img}(\rho^{\sigma}_{\gamma})$ and we can apply the same reasoning as in the base case.
– Case $t_1 \in \mathsf{H}_\gamma$: By Property 8 of Definition 12, we deduce that $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$. Moreover, by Property 6 of Definition 12, we also deduce that $t_1 \notin \mathrm{dom}(\mu_\gamma)$. Hence $\mathsf{trH}_\gamma(t_1) = \mathsf{f}(\mathsf{trH}_\gamma(u_1), \ldots, \mathsf{trH}_\gamma(u_n))$. Thus, $\mathsf{root}(\mathsf{trH}_\omega(t_2)) \in \mathsf{f}$. If $\delta' = \mathsf{tr}$ then we deduce from Definition 13 that there exist $v_1, \ldots, v_n$ such that $\mathsf{f}(v_1, \ldots, v_n) = t_2$. Moreover, we also know that either $t_2 \in \mathsf{H}_\omega$ and so $\delta'(t_2, \omega) = \mathsf{f}(\mathsf{trH}_\omega(v_1), \ldots, \mathsf{trH}_\omega(v_n))$ or else there exists $\omega' \in \{\alpha, \beta\}$ such that $\delta'(t_2, \omega) = \mathsf{f}(\mathsf{tr}_{\omega'}(v_1), \ldots, \mathsf{tr}_{\omega'}(v_n))$. Therefore, in all cases, we obtain that there exists $\delta'' \in \{\mathsf{tr}, \mathsf{trH}\}$, $\omega' \in \{\alpha, \beta\}$ such that $\delta'(t_2, \omega') = \mathsf{f}(\delta''(v_1, \omega'), \ldots, \delta''(v_n, \omega'))$. Hence for all $i \in \{1, \ldots, n\}$, $\mathsf{trH}_\gamma(u_i) = \delta''(v_i, \omega')$. By our inductive hypothesis, we obtain that for all $i \in \{1, \ldots, n\}$, $u_i = v_i$ which allows us to conclude that $t_1 = t_2$.
– Case $t_1 \in \mathrm{dom}(\mu_\gamma)$: In such a case, $\delta(\gamma, t_1) \in \mathrm{img}(\mu_\gamma)$ and we can apply the same reasoning as in the base case.
– Otherwise there exists $\gamma' \in \{\alpha, \beta\}$ such that $\delta(\gamma, t_1) = \mathsf{f}(\mathsf{tr}_{\gamma'}(u_1), \ldots, \mathsf{tr}_{\gamma'}(u_n))$. Therefore, we deduce that $\mathsf{root}(\delta'(\omega, t_2)) = \mathsf{f}$. If $\delta' = \mathsf{tr}$ then we deduce from Definition 13 that there exists $v_1, \ldots, v_n$ such that $\mathsf{f}(v_1, \ldots, v_n) = t_2$. Moreover, we also know that either $t_2 \in \mathsf{H}_\omega$ and so $\delta'(t_2, \omega) = \mathsf{f}(\mathsf{trH}_\omega(v_1), \ldots, \mathsf{trH}_\omega(v_n))$ or else there exists $\omega' \in \{\alpha, \beta\}$ such that $\delta'(t_2, \omega) = \mathsf{f}(\mathsf{tr}_{\omega'}(v_1), \ldots, \mathsf{tr}_{\omega'}(v_n))$. Therefore, in all cases, we obtain that there exists $\delta'' \in \{\mathsf{tr}, \mathsf{trH}\}$, $\omega' \in \{\alpha, \beta\}$ such that $\delta'(t_2, \omega') = \mathsf{f}(\delta''(v_1, \omega'), \ldots, \delta''(v_n, \omega'))$. Hence for all $i \in \{1, \ldots, n\}$, $\mathsf{tr}_{\gamma'}(u_i) = \delta''(v_i, \omega')$. By our inductive hypothesis, we obtain that for all $i \in \{1, \ldots, n\}$, $u_i = v_i$ which allows us to conclude that $t_1 = t_2$.

Assume now that $\delta = \mathsf{trH}$. Once again we do a case analysis on t_1.

– Case $t_1 \in \mathrm{dom}(\mu_\gamma)$: In such a case $\delta(\gamma, t_1) \in \mathrm{img}(\mu_\gamma)$ and we can apply the same reasoning as in the base case.
– Case $\mathsf{f} = \langle\,\rangle$ or $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ and $t_1 \in \mathsf{H}_\gamma$: In such a case, $\delta(\gamma, t_1) = \mathsf{f}(\mathsf{trH}_\gamma(u_1), \ldots, \mathsf{trH}_\gamma(u_n))$. Hence, $\mathsf{root}(\delta'(\omega, t_2)) = \mathsf{f}$. If $\delta' = \mathsf{tr}$ then we deduce from Definition 13 that there exists $v_1, \ldots, v_n$ such that $\mathsf{f}(v_1, \ldots, v_n) = t_2$. Moreover, $t_2 \in \mathsf{H}_\omega$ and so $\delta'(t_2, \omega) = \mathsf{f}(\mathsf{trH}_\omega(v_1), \ldots, \mathsf{trH}_\omega(v_n))$ or else there exists $\omega' \in \{\alpha, \beta\}$ such that $\delta'(t_2, \omega) = \mathsf{f}(\mathsf{tr}_{\omega'}(v_1), \ldots, \mathsf{tr}_{\omega'}(v_n))$. Therefore, in all cases, we obtain that there exists $\delta'' \in \{\mathsf{tr}, \mathsf{trH}\}$, $\omega' \in \{\alpha, \beta\}$ such that $\delta'(t_2, \omega') = \mathsf{f}(\delta''(v_1, \omega'), \ldots, \delta''(v_n, \omega'))$. Hence for all $i \in \{1, \ldots, n\}$, $\mathsf{trH}_\gamma(u_i) = \delta''(v_i, \omega')$. By our inductive hypothesis, we obtain that for all $i \in \{1, \ldots, n\}$, $u_i = v_i$ which allows us to conclude that $t_1 = t_2$.
– Otherwise $\delta(\gamma, t_1) = \mathsf{tr}_\gamma(t_1)$: We already covered that case. □

Consider a setup $(\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ and its tranformation functions tr and trH. We will denote by $\mathsf{tr}(\mathsf{Ks})$ and $\mathsf{tr}(\mathsf{Ka})$ respectively the sequences $[\mathsf{tr}_\gamma(\mathsf{Ks}_i) \mid \gamma \in \{\alpha, \beta\} \wedge i \in \gamma]_{i=1}^{p}$ and $[\mathsf{tr}_\gamma(\mathsf{Ka}_i) \mid \gamma \in \{\alpha, \beta\} \wedge i \in \gamma]_{i=1}^{p}$.

Lemma 4. *Let $\mathcal{S}$ be a setup and let tr and trH the transformation functions of $\mathcal{S}$. Let u be a ground message in normal form such that $\mathit{names}(u) \cap \mathcal{N}_{abs} = \emptyset$. Let $\gamma \in \{\alpha, \beta\}$. We have that:*

– *$\mathsf{tr}_\gamma(u)$ and $\mathsf{trH}_\gamma(u)$ are in normal form; and*
– *$\mathsf{root}(\mathsf{tr}_\gamma(u)) \neq \mathsf{root}(u)$ implies $\mathsf{root}(\mathsf{tr}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\rho^{\sigma}_{\gamma}, \mu_\gamma)$; and*
– *$\mathsf{root}(\mathsf{trH}_\gamma(u)) \neq \mathsf{root}(u)$ implies $\mathsf{root}(\mathsf{trH}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\mu_\gamma)$; and*
– *$\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{tr}_\gamma(u)) \neq \mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u)$ implies $\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{tr}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\rho^{\sigma}_{\gamma}, \mu_\gamma)$; and*
– *$\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{trH}_\gamma(u)) \neq \mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u)$ implies $\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{trH}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\mu_\gamma)$.*

Proof. We prove this result by induction on $|u|$.

Base case $|u| = 1$: In such a case, we have that $u \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$ meaning that $\mathsf{root}(u) = \bot$ and $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u)$. By Definition 13, we also have that $\mathsf{tr}_\gamma(u), \mathsf{trH}_\gamma(u) \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$. Therefore, $\mathsf{tr}_\gamma(u)$ and $\mathsf{trH}_\gamma(u)$ are in normal form, $\mathsf{root}(\mathsf{tr}_\gamma(u)) = \mathsf{root}(\mathsf{trH}_\gamma(u)) = \bot$ and $\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{tr}_\gamma(u)) = \mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{trH}_\gamma(u)) = \bot$. Hence the result holds.

Inductive $|u| > 1$*:* In such a case, $u = \mathsf{f}(u_1, \ldots, u_n)$. Let us first consider $\mathsf{tr}_\gamma(u)$. We do a case analysis on u.

Case $u \in \mathrm{dom}(\rho^\sigma_\gamma)$: In such case, by Definition 13, we have that $\mathsf{tr}_\gamma(u) \in \mathrm{img}(\rho^\sigma_\gamma) \subseteq \mathcal{N}_{abs}$. Thus, $\mathsf{tr}_\gamma(u)$ is in normal form. Moreover, $\mathsf{root}(\mathsf{tr}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\rho^\sigma_\gamma)$. Similarly, we have that $\mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\rho^\sigma_\gamma)$. Therefore the result holds.

Otherwise case $u \in \mathsf{H}_\gamma$: In such a case, by Properties 8 and 6, we deduce that $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ and $u \notin \mathrm{dom}(\mu_\gamma)$. Thus, $\mathsf{tr}_\gamma(u) = \mathsf{f}(\mathsf{trH}_\gamma(u_1), \ldots, \mathsf{trH}_\gamma(u_n))$. By inductive hypothesis, we deduce that for all $i \in \{1, \ldots, n\}$, $\mathsf{trH}_\gamma(u_i)$ is in normal form and so $\mathsf{tr}_\gamma(u)$ is in normal form. Moreover, $\mathsf{root}(\mathsf{tr}_\gamma(u)) = \mathsf{root}(u)$ and $\mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u)) = \mathsf{tagroot}_{\mathsf{Ks,Ka}}(u) = 0$. Therefore, the result holds.

Otherwise case $u \in \mathrm{dom}(\mu_\gamma)$: In such case, by Definition 13, we have that $\mathsf{tr}_\gamma(u) \in \mathrm{img}(\mu_\gamma) \subseteq \mathcal{N}_{abs}$. Thus, $\mathsf{tr}_\gamma(u)$ is in normal form. Moreover, $\mathsf{root}(\mathsf{tr}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\mu_\gamma)$. Similarly, $\mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\mu_\gamma)$. Therefore the result holds.

Otherwise case $u = C[v_1, \ldots, v_m]$ where C is built on Σ_j^+ with $j \in \{1, \ldots, p\}$, C is different from a hole and for all $k \in \{1, \ldots, m\}$, v_k are factors in normal form of u: Let $\omega \in \{\alpha, \beta\}$ such that $j \in \omega$. We deduce that $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u) \in \omega$. Let p a position of C different from a hole. Since $\mathsf{root}(u|_p) \in \Sigma_j^+$, we obtain that $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u|_p) \in \omega$. Note that by Properties 8 and 7 of Definition 12, we deduce that for all positions p of C different from a hole, $u|_p \notin \mathrm{dom}(\rho^\sigma_\omega) \cup \mathsf{H}_\omega$. Therefore, by Definition 13, we obtain that $\mathsf{tr}_\gamma(u) = C[\mathsf{tr}_\omega(v_1), \ldots, \mathsf{tr}_\omega(v_m)]$. Since C is not a hole, we know that $|v_1| < |u|, \ldots, |v_m| < |u|$. Thanks to our inductive hypothesis on $v_1, \ldots, v_m$, we have that $\mathsf{tr}_\omega(v_1), \ldots, \mathsf{tr}_\omega(v_m)$ are in normal form and $\mathsf{tr}_\omega(v_1), \ldots, \mathsf{tr}_\omega(v_m)$ are factors of $\mathsf{tr}_\gamma(u)$. Recall that u is in normal form, meaning that $C[v_1, \ldots, v_m]{\downarrow} = C[v_1, \ldots, v_m]$. By Lemmas 2 and 3, we deduce that

$$C[\mathsf{tr}_\omega(v_1), \ldots, \mathsf{tr}_\omega(v_m)]{\downarrow} = C[\mathsf{tr}_\omega(v_1), \ldots, \mathsf{tr}_\omega(v_m)]$$

i.e. $\mathsf{tr}_\gamma(u){\downarrow} = \mathsf{tr}_\gamma(u)$. Furthermore, we have $\mathsf{root}(\mathsf{tr}_\gamma(u)) = \mathsf{root}(u)$ and $\mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u)) = \mathsf{tagroot}_{\mathsf{Ks,Ka}}(u)$.

Otherwise case $\mathsf{f} \in \Sigma_0$: By Definition 13, there exists $\omega \in \{\alpha, \beta\}$ such that $\mathsf{tr}_\gamma(u) = \mathsf{f}(\mathsf{tr}_\omega(u_1), \ldots, \mathsf{tr}_\omega(u_n))$. Note that since u is a message, $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{pk}, \mathsf{sign}, \mathsf{vk}, \mathsf{h}, \langle\ \rangle\}$. In this case, we have that $\mathsf{tr}_\gamma(u){\downarrow} = \mathsf{f}(\mathsf{tr}_\omega(u_1){\downarrow}, \ldots, \mathsf{tr}_\omega(u_n){\downarrow})$. Since by inductive hypothesis, $\mathsf{tr}_\omega(u_k)$ is in normal form, for all $k \in \{1, \ldots, n\}$, we can deduce that $\mathsf{tr}_\gamma(u)$ is also in normal form and $\mathsf{root}(\mathsf{tr}_\gamma(u)) = \mathsf{f} = \mathsf{root}(u)$. We do a case analysis on f to determine $\mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u))$:

Case 1, $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\ \rangle\}$*:* In such a case, by Definition 10, we obtain that $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u) = \mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u)) = 0$.

Case 2, $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}\}$*,* $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u) \in \varepsilon$*,* $\varepsilon \in \{\alpha, \beta\}$*:* Let $i \in \varepsilon$ such that $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u) = i$. First of all, by Definition 13, we know that $\mathsf{tr}_\gamma(u) = \mathsf{f}(\mathsf{tr}_\varepsilon(u_1), \ldots, \mathsf{tr}_\varepsilon(u_n))$. Moreover, by Definition 10, we know that either (a) $u_n \in \mathsf{Ks}_i$ or (b) $\mathsf{root}(u_1) = \mathsf{tag}_i$ and $u_n \notin \mathsf{Ks}$. In case (a), by definition of $\mathsf{tr}(\mathsf{Ks})$, we have $\mathsf{tr}_\varepsilon(\mathsf{Ks}_i) = \mathsf{tr}(\mathsf{Ks})_i$. Therefore, $\mathsf{tr}_\varepsilon(u_m) \in \mathsf{tr}(\mathsf{Ks})_i$ meaning that $\mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u)) = i$. In case (b), $\mathsf{root}(u_1) = \mathsf{tag}_i$ implies $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u_1) = i$. Therefore, by Properties 7 and 6 of Definition 12, we deduce that $u_1 \notin \mathrm{dom}(\rho^\sigma_\varepsilon, \mu_\varepsilon)$. Hence, by applying our inductive hypothesis on u_1, we deduce that $\mathsf{root}(\mathsf{tr}_\varepsilon(u_1)) = \mathsf{tag}_i$. Hence it remains to prove that $\mathsf{tr}_\varepsilon(u_m) \notin \mathsf{tr}(\mathsf{Ks})$. We prove this by contradiction. If $\mathsf{tr}_\varepsilon(u_n) \in \mathsf{tr}(\mathsf{Ks})$ then there exist $\varepsilon' \in \{\alpha, \beta\}$ and $w \in \mathsf{Ks}$ such that $\mathsf{tr}_{\varepsilon'}(w) = \mathsf{tr}_\varepsilon(u_n)$. Note that by Property 4 of Definition 12, $\mathit{names}(\mathsf{Ks}) \cap \mathcal{N}_{abs} = \emptyset$. Hence by Lemma 3, we deduce that $w = u_n$ and so $u_n \in \mathsf{Ks}$ which is a contradiction with our hypothesis $u_n \notin \mathsf{Ks}$. Hence, we conclude that $\mathsf{tagroot}_{\mathsf{tr(Ks)},\mathsf{tr(Ka)}}(\mathsf{tr}_\gamma(u)) = i$.

Case 3, $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}\}$*,* $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u) = 0$*:* In such a case, $\mathsf{tr}_\gamma(u) = \mathsf{f}(\mathsf{tr}_\gamma(u_1), \ldots, \mathsf{tr}_\gamma(u_n))$. Moreover, by Definition 10, we know that $u_n \notin \mathsf{Ks}$ and $\mathsf{root}(u_1) \notin \{\mathsf{tag}_1, \ldots, \mathsf{tag}_p\}$. By our inductive hypothesis on u_1, we deduce that $\mathsf{root}(\mathsf{tr}_\gamma(u_1)) \notin \{\mathsf{tag}_1, \ldots, \mathsf{tag}_p\}$. Assume by contradiction that $\mathsf{tr}_\gamma(u_n) \in \mathsf{Ks}$. In such a case, there exist $\varepsilon \in \{\alpha, \beta\}$ and $w \in \mathsf{Ks}$ such that $\mathsf{tr}_\gamma(u_n) = \mathsf{tr}_\varepsilon(w)$. Note that by Property 4 of Definition 12, $\mathit{names}(\mathsf{Ks}) \cap \mathcal{N}_{abs} = \emptyset$. Hence by Lemma 3, we deduce

that $w = u_n$ and so $u_n \in \mathsf{Ks}$ which is a contradiction with $u_n \notin \mathsf{Ks}$. Hence, $\mathsf{tr}_\gamma(u_n) \notin \mathsf{tr}(\mathsf{Ks})$ and so $\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{tr}_\gamma(u)) = 0$.

Case 4, $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) \in \varepsilon$, $\varepsilon \in \{\alpha, \beta\}$*:* Similar to the case 2.2 (by replacing Ks by Ka in the proof).

Case 5, $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = 0$*:* Similar to the case 2.3 (by replacing Ks by Ka in the proof).

Case 6, $\mathsf{f} = \mathsf{sign}$, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) \in \varepsilon$, $\varepsilon \in \{\alpha, \beta\}$*:* Let $i \in \varepsilon$ such that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = i$. In such a case, $\mathsf{tr}_\gamma(u) = \mathsf{sign}(\mathsf{tr}_\varepsilon(u_1), \mathsf{tr}_\varepsilon(u_2))$. By Definition 10, we know that either (a) $\mathsf{vk}(u_2) \in \mathsf{Ka}_i$ or (b) $\mathsf{root}(u_1) = \mathsf{tag}_i$ and $\mathsf{vk}(u_2) \notin \mathsf{Ka}$. In case (a), we have $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(\mathsf{vk}(u_2)) = 0$. Note that by Property 9 of Definition 12, $\mathsf{vk}(u_2) \notin \mathsf{H}_\varepsilon$ and $\mathsf{vk}(u_2) \notin \mathrm{dom}(\rho^\sigma_\varepsilon)$. Also note that by Property 6 of Definition 12, $\mathsf{vk}(u_2) \notin \mathrm{dom}(\mu_\varepsilon)$. Therefore, by Definition 13, we deduce that $\mathsf{tr}_\varepsilon(\mathsf{vk}(u_2)) = \mathsf{vk}(\mathsf{tr}_\varepsilon(u_2))$. Since $\mathsf{tr}_\varepsilon(\mathsf{vk}(u_2)) \in \mathsf{tr}(\mathsf{Ka})_\varepsilon$ by definition, we obtain that $\mathsf{vk}(\mathsf{tr}_\varepsilon(u_2)) \in \mathsf{tr}(\mathsf{Ka})_\varepsilon$ and so $\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{tr}_\gamma(u)) = i$. In case (b), $\mathsf{root}(u_1) = \mathsf{tag}_i$ implies $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u_1) = i$. Therefore, by Property 7 of Definition 12, we deduce that $u_1 \notin \mathrm{dom}(\rho^\sigma_\varepsilon)$. Hence, by applying our inductive hypothesis on u_1, we deduce that $\mathsf{root}(\mathsf{tr}_\varepsilon(v_1)) = \mathsf{tag}_i$. Hence it remains to prove that $\mathsf{vk}(\mathsf{tr}_\varepsilon(u_2)) \notin \mathsf{tr}(\mathsf{Ka})$. We prove this by contradiction. If $\mathsf{vk}(\mathsf{tr}_\varepsilon(u_2)) \in \mathsf{tr}(\mathsf{Ka})$ then there exist $\varepsilon' \in \{\alpha, \beta\}$ and $\mathsf{vk}(w) \in \mathsf{Ka}$ such that $\mathsf{tr}_{\varepsilon'}(\mathsf{vk}(w)) = \mathsf{vk}(\mathsf{tr}_\varepsilon(u_2))$. Since $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(\mathsf{vk}(w)) = 0$ and $\mathsf{root}(\mathsf{tr}_{\varepsilon'}(\mathsf{vk}(w))) = \mathsf{vk}$, we deduce from Definition 13 that either $\mathsf{tr}_{\varepsilon'}(\mathsf{vk}(w)) = \mathsf{vk}(\mathsf{tr}_{\varepsilon'}(w))$ or $\mathsf{tr}_{\varepsilon'}(\mathsf{vk}(w)) = \mathsf{vk}(\mathsf{trH}_{\varepsilon'}(w))$. By Property 4 of Definition 12, we know that $\mathit{names}(w) \cap \mathcal{N}_{abs} = \emptyset$. Moreover, we already know that $\mathit{names}(u) \cap \mathcal{N}_{abs} = \emptyset$. Hence, by Lemma 3, we obtain that $u_2 = w$ which would imply that $\mathsf{vk}(u_2) \in \mathsf{Ka}$. Hence a contradiction with our hypothesis $\mathsf{vk}(u_2) \notin \mathsf{Ka}$. Thus, we conclude that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(\mathsf{tr}_\gamma(u)) = i$.

Case 7, $\mathsf{f} = \mathsf{sign}$, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = 0$*:* In such a case, by Definition 10, we know that $\mathsf{vk}(u_2) \notin \mathsf{Ka}$ and $\mathsf{root}(u_1) \notin \{\mathsf{tag}_1, \ldots, \mathsf{tag}_p\}$. By our inductive hypothesis on u_1, we deduce that $\mathsf{root}(\mathsf{tr}_\gamma(u_1)) \notin \{\mathsf{tag}_1, \ldots, \mathsf{tag}_p\}$. We show that $\mathsf{vk}(\mathsf{tr}_\gamma(u_2)) \notin \delta(\mathsf{Ka})$. Assume by contradiction that $\mathsf{vk}(\mathsf{tr}_\gamma(u_2)) \in \delta(\mathsf{Ka})$. Thus, there exist $\varepsilon \in \{\alpha, \beta\}$ and $\mathsf{vk}(w) \in \mathsf{Ka}$ such that $\mathsf{tr}_\varepsilon(\mathsf{vk}(w)) = \mathsf{vk}(\mathsf{tr}_\gamma(u_2))$. Since $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(\mathsf{vk}(w)) = 0$ and $\mathsf{root}(\mathsf{tr}_\varepsilon(\mathsf{vk}(w))) = \mathsf{vk}$, we deduce from Definition 13 that either $\mathsf{tr}_\varepsilon(\mathsf{vk}(w)) = \mathsf{vk}(\mathsf{tr}_\varepsilon(w))$ or $\mathsf{tr}_\varepsilon(\mathsf{vk}(w)) = \mathsf{vk}(\mathsf{trH}_{\varepsilon'}(w))$. By Property 4 of Definition 12, we know that $\mathit{names}(w) \cap \mathcal{N}_{abs} = \emptyset$. Moreover, we already know that $\mathit{names}(u) \cap \mathcal{N}_{abs} = \emptyset$. Hence, by Lemma 3, we obtain that $u_2 = w$ which would imply that $\mathsf{vk}(u_2) \in \mathsf{Ka}$. Hence a contradiction with our hypothesis $\mathsf{vk}(u_2) \notin \mathsf{Ka}$. Thus, we conclude that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(\mathsf{tr}_\gamma(u)) = 0$.

This conclude the proof for the different properties on $\mathsf{tr}_\gamma(u)$. It remains to show the properties on $\mathsf{trH}_\gamma(u)$. We do a case analysis on u.

Case $u \in \mathrm{dom}(\mu_\gamma)$: In such case, by Definition 13, we have that $\mathsf{trH}_\gamma(u) \in \mathrm{img}(\mu_\gamma) \subseteq \mathcal{N}_{abs}$. Thus, $\mathsf{trH}_\gamma(u)$ is in normal form. Moreover, $\mathsf{root}(\mathsf{trH}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\mu_\gamma)$. Similarly, $\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{trH}_\gamma(u)) = \bot$ and $u \in \mathrm{dom}(\mu_\gamma)$. Therefore the result holds.

Otherwise case $\mathsf{f} = \langle\,\rangle$ or $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ and $u \in \mathsf{H}_\gamma$: In such a case, $\mathsf{trH}_\gamma(u) = \mathsf{f}(\mathsf{trH}_\gamma(u_1), \ldots, \mathsf{trH}_\gamma(u_n))$. Hence $\mathsf{root}(\mathsf{trH}_\gamma(u)) = \mathsf{root}(u)$ and $\mathsf{tagroot}_{\mathsf{tr}(\mathsf{Ks}),\mathsf{tr}(\mathsf{Ka})}(\mathsf{trH}_\gamma(u)) = \mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = 0$. Moreover, by our inductive hypothesis, we obtain that for all $i \in \{1, \ldots, n\}$, $\mathsf{trH}_\gamma(u_i)$ is in normal form hence, we conclude that $\mathsf{trH}_\gamma(u)$ is in normal form. Therefore, the result holds.

Otherwise $\mathsf{trH}_\gamma(u) = \mathsf{tr}_\gamma(u)$: Case already covered. □

Lemma 5. *Let $\mathcal{S}$ be a setup and let tr and trH the transformation functions of $\mathcal{S}$. Let t_1 and t_2 be ground messages in normal form such that $\mathit{names}(t_1, t_2) \cap \mathcal{N}_{abs} = \emptyset$. We have that for all $\delta, \delta' \in \{\mathsf{tr}, \mathsf{trH}\}$, for all $\gamma, \omega \in \{\alpha, \beta\}$, $\delta(\gamma, t_1) \in st(\delta'(\omega, t_2))$ implies $t_1 \in st(t_2)$.*

Proof. We prove the result by induction on $|t_2|$.

Base case $|t_2| = 1$*:* In such a case, $t_2 \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ and so $\delta(\gamma, t_1) = \delta'(\omega, t_2)$. By Lemma 3, we obtain that $t_1 = t_2$.

Inductive step $|t_2| > 1$*:* There exists a symbol function f and terms $u_1, \ldots u_n$ such that $t_2 = \mathsf{f}(u_1, \ldots u_n)$. By Lemma 4, we know that either $\mathsf{root}(\delta'(\omega, t_2)) = \bot$ or $\mathsf{root}(\delta'(\omega, t_2)) = \mathsf{f}$. In the

former case, we obtain that $\delta(\gamma, t_1) = \delta'(\omega, t_2)$ and so we conclude with Lemma 3. In the latter case, by Definition 13, we deduce that there exist $\omega' \in \{\alpha, \beta\}$ and $\delta'' \in \{\mathsf{tr}, \mathsf{trH}\}$ such that $\delta'(\omega, t_2) = \mathsf{f}(\delta''(\omega', u_1), \ldots, \delta''(\omega', u_n))$. Thus, $\delta(\gamma, t_1) \in st(\delta'(\omega, t_2))$ implies either $\delta(\gamma, t_1) = \delta'(\omega, t_2)$ or there exists $k \in \{1, \ldots, n\}$ such that $\delta(\gamma, t_1) \in st(\delta''(\omega', u_k))$. In the former case, we can once again conclude with Lemma 3. In the latter case, we conclude by inductive hypothesis on u_k. □

D Executed terms

For all substitution σ of ground terms in normal form, for all $\gamma \in \{\alpha, \beta\}$, we denote by $\mathsf{tr}_\gamma(\sigma)$ the substitution such that $\mathrm{dom}(\sigma) = \mathrm{dom}(\mathsf{tr}_\gamma(\sigma))$ and for all $x \in \mathrm{dom}(\mathsf{tr}_\gamma(\sigma))$, $x\mathsf{tr}_\gamma(\sigma) = \mathsf{tr}_\gamma(x\sigma)$.

Definition 14. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. Let u be a ground term. We define the two predicates $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u, \gamma)$ and $\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(u, i)$ as follows:*

- *$\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u, \gamma)$ iff for all $p \in \mathcal{P}os(u)$, $u|_p \in \mathrm{dom}(\rho^\sigma_\gamma)$ implies there exists p' strict prefix of p such that $\mathsf{root}(u|_{p'}) \neq \langle\rangle$.*
- *$\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(u, i)$ iff $u \notin \mathrm{dom}(\rho^\sigma_\gamma) \cup (\mathsf{Ka} \setminus \mathsf{Ka}_i)$ and if $\mathsf{root}(u) \in \{\mathsf{pk}, \mathsf{vk}\}$ then*
  - *$u|_1 \in \mathrm{dom}(\rho^\sigma_\gamma) \Rightarrow u \notin \mathsf{H}_\gamma$*
  - *$u|_1 \notin \mathrm{dom}(\rho^\sigma_\gamma) \Rightarrow \mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u|_1, \gamma)$*

Lemma 6. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $\gamma \in \{\alpha, \beta\}$. For all ground term u, if $names(u) \cap \mathcal{N}_{abs} = \emptyset$ and $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u, \gamma)$ then $\mathsf{tr}_\gamma(u) = \mathsf{trH}_\gamma(u)$.*

Proof. We prove this result by induction on $|u|$.

Base case $|u| = 1$: In such a case, $u \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$. Note that by our hypothesis, we know that $u \notin \mathrm{dom}(\rho^\sigma_\gamma)$. If $u \in \mathsf{H}_\gamma$ then we directly have by Definition 13 that $\mathsf{tr}_\gamma(u) = \mathsf{trH}_\gamma(u)$. Else if $u \in \mathrm{dom}(\mu_\gamma)$ then we know by Definition 13 that $\mathsf{trH}_\gamma(u) = u\mu_\gamma$. Moreover, since $u \notin \mathrm{dom}(\rho^\sigma_\gamma)$, we also obtain that $\mathsf{tr}_\gamma(u) = u\mu_\gamma$ and so the result holds. Else, by Definition 13 (Case 8), we directly obtain that $\mathsf{tr}_\gamma(u) = \mathsf{trH}_\gamma(u)$.

Inductive step $|u| > 1$: In such a case, we deduce that $u = \mathsf{f}(u_1, \ldots, u_n)$ for some function symbol f and ground terms $u_1, \ldots, u_n$. Let us do a case analysis on u.

- $u \in \mathrm{dom}(\rho^\sigma_\gamma)$: This case is impossible by our hypothesis.
- $u \in \mathsf{H}_\gamma$: Once again the result directly holds by Definition 13.
- $u \in \mathrm{dom}(\mu_\gamma)$: We obtain directly by Definition 13 that $\mathsf{tr}_\gamma(u) = \mathsf{trH}_\gamma(u)$
- Otherwise: By Definition 13, we know that either $\mathsf{f} = \langle\rangle$ and $\mathsf{trH}_\gamma(u) = \mathsf{f}(\mathsf{trH}_\gamma(u_1), \ldots, \mathsf{trH}_\gamma(u_n))$ or else $\mathsf{trH}_\gamma(u) = \mathsf{tr}_\gamma(u)$. In the latter case, the result directly holds. In the former case, we also know by Definition 13 that $\mathsf{tr}_\gamma(u) = \mathsf{f}(\mathsf{tr}_\gamma(u_1), \ldots, \mathsf{tr}_\gamma(u_n))$. Let us now show that we can apply our inductive hypothesis on $u_1, \ldots, u_n$. We already know that for all $i \in \{1, \ldots, n\}$, $|u_i| < |u|$. Moreover, since $u_i \in st(u)$, we directly have that $names(u_i) \cap \mathcal{N}_{abs} = \emptyset$. Lastly, let $p \in \mathcal{P}os(u_i)$ such that $u_i|_p \in \mathrm{dom}(\rho^\sigma_\gamma)$. Hence, $i \cdot p \in \mathcal{P}os(u)$. Hence by our hypothesis on u, we obtain that there exists p' strict prefix of $i \cdot p$ such that $\mathsf{root}(u|_{p'}) \neq \langle\rangle$. But $\mathsf{f} = \langle\rangle$. Hence, we deduce that there exist q strict prefix of p such that $\mathsf{root}(u|_{i \cdot q}) \neq \langle\rangle$. Lastly, $\mathsf{root}(u|_{i \cdot q}) \neq \langle\rangle$ implies $\mathsf{root}(u_i|_q) \neq \langle\rangle$. Therefore, we can apply our inductive hypothesis $u_1, \ldots, u_n$ meaning that for all $i \in \{1, \ldots, n\}$, $\mathsf{trH}_\gamma(u_i) = \mathsf{tr}_\gamma(u_i)$ and so $\mathsf{tr}_\gamma(u) = \mathsf{trH}_\gamma(u)$. □

Lemma 7. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. For all ground term u, for all $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}\}$, if $names(u) \cap \mathcal{N}_{abs} = \emptyset$ and $\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(\mathsf{f}(u), i)$ then $\mathsf{tr}_\gamma(\mathsf{f}(u)) = \mathsf{trH}_\gamma(\mathsf{f}(u)) = \mathsf{f}(\mathsf{tr}_\gamma(u))$.*

Proof. Let us do a case analysis on $\mathsf{f}(u)$.

- Case $\mathsf{f}(u) \in \mathrm{dom}(\rho^\sigma_\gamma)$: Such a case is impossible since we know from $\mathcal{P}^{\mathcal{S}}_{\text{e-keys}}(\mathsf{f}(u), i)$ that $\mathsf{f}(u) \notin \mathrm{dom}(\rho^\sigma_\gamma)$.

– Otherwise case $\mathsf{f}(u) \in \mathsf{H}_\gamma$: In such a case, we know by definition that $\mathsf{tr}_\gamma(\mathsf{f}(u)) = \mathsf{trH}_\gamma(\mathsf{f}(u))$. Note that by Property 6 of Definition 12, we deduce that $\mathsf{f}(u) \notin \mathrm{dom}(\mu_\gamma)$. Hence, $\mathsf{tr}_\gamma(\mathsf{f}(u)) = \mathsf{f}(\mathsf{trH}_\gamma(u))$. However, since $\mathcal{P}^{\mathcal{S}}_{\text{e-keys}}(\mathsf{f}(u), i)$ and $\mathsf{f}(u) \in \mathsf{H}_\gamma$, we deduce that $u \notin \mathrm{dom}(\rho^\sigma_\gamma)$ and so $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u, \gamma)$. By Lemma 6, we obtain that $\mathsf{trH}_\gamma(u) = \mathsf{tr}_\gamma(u)$ which allows us to conclude.
– Otherwise case $\mathsf{f}(u) \in \mathrm{dom}(\mu_\gamma)$: Such a case is impossible by Property 6 of Definition 12.
– Otherwise: We deduce that $\mathsf{tr}_\gamma(\mathsf{f}(u)) = \mathsf{f}(\mathsf{tr}_\gamma(u))$. Moreover, since $\mathsf{f}(u) \notin \mathsf{H}_\gamma \cup \mathrm{dom}(\mu_\gamma)$, we also know by definition that $\mathsf{trH}_\gamma(\mathsf{f}(u)) = \mathsf{tr}_\gamma(\mathsf{f}(u))$. This allow us to conclude. □

Definition 15. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let u be a message in normal form. We define the predicate $\mathcal{P}^{\mathcal{S}}_{gen}(u)$ to hold iff for all $\gamma \in \{\alpha, \beta\}$, for all $i \in \gamma$, for all $p \in \mathcal{P}os(u)$,*

– *if $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u|_p) = i$ and $\mathsf{root}(u|_p) = \mathsf{f}/n$ then $\exists j \in \{1, \ldots, n\}.\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u|_{p\cdot j}, \gamma)$ implies $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{sign}, \mathsf{tagk}_i\}$, $j = n$ and $u|_{p\cdot n} \in \mathrm{dom}(\rho^\sigma_\gamma)$*
– *if $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u|_p) = 0$ and $\mathsf{root}(u|_p) = \mathsf{f}/n \notin \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\rangle\}$ then for all $j \in \{1, \ldots, n\}$, $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u|_{p\cdot j}, \gamma)$.*

Definition 16 (e-terms). *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. We define the set of* executed terms w.r.t. $\mathcal{S}$ and i, *denoted* $\text{E-TERMS}_i(\mathcal{S})$, *as the smallest set such that $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$ when the following properties hold:*

1. *$(u, K_s, K_a) \in \text{TAGT}(i)$ and $u \notin \mathrm{dom}(\rho_\gamma)$*
2. *$K_s\sigma\!\downarrow \subseteq \mathsf{Ks}_i$ and $K_a\sigma\!\downarrow \subseteq \mathsf{Ka}_i$*
3. *$names(u) \cap \mathcal{N}_{abs} = \emptyset$, $names(u) \cap \mathrm{dom}(\rho^\sigma_\gamma, \mu_\gamma) = \emptyset$ and $n_{min} \notin names(u)$*
4. *$fv(u) \subseteq \mathrm{dom}(\sigma)$ and $\forall x \in fv(u)$, $\mathcal{P}^{\mathcal{S}}_{gen}(u)$ and either $x \in \mathrm{dom}(\rho_\gamma)$ or $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(x\sigma, \gamma)$*
5. *for all $p \in \mathcal{P}os(u)$, if $u|_p \in \mathrm{dom}(\rho_\gamma)$ then either there exists p' such that $p = p' \cdot 1$ and $\mathsf{root}(u|_{p'}) \in \{\mathsf{vk}, \mathsf{pk}, \mathsf{tagk}_i\}$ or there exist $\mathsf{f}/n \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}, \mathsf{sign}\}$ and p' such that $p = p' \cdot n$ and $\mathsf{root}(u|_{p'}) = \mathsf{f}$*
6. *for all $p \in \mathcal{P}os(u)$, if $\mathsf{root}(u|_p) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\rangle\}$ then $\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(u|_p\sigma\!\downarrow, i)$*
7. *for all $p \in \mathcal{P}os(u)$, if $\mathsf{root}(u|_p) \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$ then $\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(u|_{p\cdot 1}\sigma\!\downarrow, i)$*
8. *for all $p \in \mathcal{P}os(u)$, if $\mathsf{root}(u|_p) = \mathsf{sign}$ then $\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(\mathsf{vk}(u|_{p\cdot 2})\sigma\!\downarrow, i)$*
9. *for all $p \in \mathcal{P}os(u)$, if $\mathsf{root}(u|_p) \in \{\mathsf{adec}, \mathsf{radec}\}$ then $\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(\mathsf{pk}(u|_{p\cdot 2})\sigma\!\downarrow, i)$*
10. *for all $p \in \mathcal{P}os(u)$, for all $\mathsf{f}/n \in \{\mathsf{aenc}, \mathsf{raenc}, \mathsf{check}\}$, if $\mathsf{root}(u|_p) = \mathsf{f}$ then $\mathcal{P}^{\mathcal{S}}_{e\text{-}keys}(u|_{p\cdot n}\sigma\!\downarrow, i)$*
11. *for all $p \in \mathcal{P}os(u)$, for all $\mathsf{f}/n \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{sdec}, \mathsf{rsdec}\}$, if $\mathsf{root}(u|_p) = \mathsf{f}$ then $u|_{p\cdot n}\sigma\!\downarrow \notin \mathsf{Ks}\backslash\mathsf{Ks}_i$*

Lemma 8. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. For all $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$, for all $(v, K'_s, K'_a) \in \text{TAGT}(i)$, if $v \in st(u)$, $v \notin \mathrm{dom}(\rho_\gamma)$, $K'_s \subseteq K_s$ and $K'_a \subseteq K_a$ then $(v, K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$.*

Proof. Direct from Definition 16. □

Lemma 9. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. For all $(u, K_s, K_a), (u', K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$, for all $p \in \mathcal{P}os(u)$, if $u|_p \in \mathcal{X}\backslash\mathrm{dom}(\rho_\gamma)$ and $u|_p\sigma = u'\sigma\!\downarrow$ then there exists $(v, K''_s, K''_a) \in \text{E-TERMS}_i(\mathcal{S})$ such that:*

– *$u\sigma$ and $u'\sigma$ being messages implies $v\sigma$ is a message*
– *$v = u[u']_p$ and $v\sigma\!\downarrow = u\sigma\!\downarrow$*

Proof. Direct from Definitions 5 and 16. □

D.1 Link between σ and $\mathsf{tr}_\gamma(\sigma)$ in an executed term

Lemma 10. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup and let tr and trH be the transformation functions of $\mathcal{S}$. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. Let $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$. If $u\sigma$ is a message then $u\mathsf{tr}_\gamma(\sigma)\!\downarrow = \mathsf{trH}_\gamma(u\sigma\!\downarrow) = \mathsf{tr}_\gamma(u\sigma\!\downarrow)$, $\mathcal{P}^{\mathcal{S}}_{gen}(u\sigma\!\downarrow)$, $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\!\downarrow, \gamma)$ and $u\mathsf{tr}_\gamma(\sigma)$ is a message.*

Proof. By Property 1 of Definition 16, we know that there exists K_s and K_a such that $(u, K_s, K_a) \in \text{TAGT}(i)$. We prove the result by induction on $|u|$.

Base case $|u| = 1$: In such a case, $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}} \cup \mathcal{X}$. If $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$, we know from Definition 13 that $\mathsf{tr}_\gamma(u), \mathsf{trH}_\gamma(u) \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ and so $\mathsf{tr}_\gamma(u)\downarrow = \mathsf{tr}_\gamma(u)$ and $\mathsf{trH}_\gamma(u)\downarrow = \mathsf{trH}_\gamma(u)$. Note that we also have that $u\sigma\downarrow = u$. Thanks to Property 3 of Definition 16, we know that $u \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$. Lastly, thanks to Property 8 of Definition 12, we also know that $u \notin \mathsf{H}_\gamma$. Hence $\mathsf{tr}_\gamma(u) = \mathsf{trH}_\gamma(u) = u$. This allows us to deduce that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{trH}_\gamma(u\sigma\downarrow) = u = u\mathsf{tr}_\gamma(\sigma)\downarrow$. Note that since $u \notin \text{dom}(\rho^\sigma_\gamma)$ and $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}} \cup \mathcal{X}$, we directly obtain that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow, \gamma)$. Hence the result holds.

Otherwise, we have $u \in \mathcal{X}$. By Definition 12, we know that σ is a substitution of ground messages in normal form meaning that $u\sigma\downarrow = u\sigma$. Hence, by Lemma 4, we obtain that $\mathsf{tr}_\gamma(u\sigma)$ and $\mathsf{trH}_\gamma(u\sigma)$ are in normal form. Moreover, by Properties 4 and 1 of Definition 16, we know that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow, \gamma)$. Hence, by Property 4 of Definition 12 and by Lemma 6, we obtain that $\mathsf{trH}_\gamma(u\sigma) = \mathsf{tr}_\gamma(u\sigma)$. Lastly, by definition of $\mathsf{tr}_\gamma(\sigma)$, we have $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(u\sigma)\downarrow = \mathsf{tr}_\gamma(u\sigma)$. With $u\sigma\downarrow = u\sigma$, the result holds.

Inductive case $|u| > 1$: In such a case, we have $u = \mathsf{f}(u_1, \ldots, u_n)$ for some terms $u_1, \ldots, u_n$ and function symbol f. We do a case analysis on f following Definition 5.

Case 2 of Definition 5: In such a case, we know that $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{sdec}, \mathsf{rsdec}\}$, for all $j \in \{1, \ldots, n\}$, $(u_j, K^j_s, K^j_a) \in \text{TAGT}(i)$ for some K^j_s, K^j_a and $K_s = \{u_n\} \cup \bigcup_{j=1}^n K^j_s$ and $K_a = \bigcup_{j=1}^n K^j_a$. By Property 5 of Definition 16, we know that for all $j \in \{1, \ldots, n-1\}$, $u_j \notin \text{dom}(\rho_\gamma)$. If $u_n \in \text{dom}(\rho_\gamma)$ then $u_n\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(u_n\sigma)\downarrow$. But thanks to Property 2 of Definition 12, we deduce that $\mathsf{tr}_\gamma(u_n\sigma) = u_n\sigma\rho^\sigma_\gamma \in \mathcal{N}_{abs}$. Hence $\mathsf{tr}_\gamma(u_n\sigma)\downarrow = \mathsf{tr}_\gamma(u_n\sigma)$ and $u_n\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, by Property 4 of Definition 16, we know that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_n\sigma)$.

Moreover, by Lemma 8, we deduce that for all $j \in \{1, \ldots, n-1\}$, $(u_j, K^j_s, K^j_a) \in \text{E-TERMS}_i(\mathcal{S})$ and if $u_n \notin \text{dom}(\rho_\gamma)$ then $(u_n, K^n_s, K^n_a) \in \text{E-TERMS}_i(\mathcal{S})$. Hence, we can apply our inductive hypothesis on $u_1, \ldots, u_{n-1}$ and on u_n when $u_n \notin \text{dom}(\rho_\gamma)$ meaning that for all $j \in \{1, \ldots, n\}$, $\mathsf{tr}_\gamma(u_j\sigma\downarrow) = u_j\mathsf{tr}_\gamma(\sigma)\downarrow$, $u_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow, \gamma)$ then $j = n$ and $u_n \in \text{dom}(\rho_\gamma)$.

If $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}\}$ then we deduce that $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Note that by Properties 8 and 6 of Definition 12, we know that $u\sigma\downarrow \notin \mathsf{H}_\gamma$ and $u\sigma\downarrow \notin \text{dom}(\mu_\gamma)$. Hence by Definition 13, we obtain that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{trH}_\gamma(u\sigma\downarrow)$. Moreover, we know that $u_n\sigma\downarrow \in \mathsf{Ks}_i$ thanks to Property 2 of Definition 16. Therefore, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u\sigma\downarrow) = i$. By Properties 8, 7 and 6 of Definition 12, we deduce that $u\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $u\sigma\downarrow \notin \mathsf{H}_\gamma$. Therefore, we obtain $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{f}(\mathsf{tr}_\gamma(u_1\sigma\downarrow), \ldots, \mathsf{tr}_\gamma(u_n\sigma\downarrow))$. By our inductive hypothesis, we obtain $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{f}(u_1\mathsf{tr}_\gamma(\sigma)\downarrow, \ldots, u_n\mathsf{tr}_\gamma(\sigma)\downarrow)$. Since $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}\}$, we conclude that $\mathsf{trH}_\gamma(u\sigma\downarrow) = \mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{f}(u_1\mathsf{tr}_\gamma(\sigma), \ldots, u_n\mathsf{tr}_\gamma(\sigma))\downarrow = u\mathsf{tr}_\gamma(\sigma)\downarrow$ and $u\mathsf{tr}_\gamma(\sigma)$ is a message. Since $\mathsf{root}(u\sigma\downarrow) = \mathsf{f}$ and $u\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma)$, we directly obtain that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow, \gamma)$. Lastly, we know that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u\sigma\downarrow) = i$ and for all $j \in \{1, \ldots, n\}$, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow, \gamma)$ then $j = n$ and $u_n \in \text{dom}(\rho_\gamma)$. Thus, we directly obtain that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$ holds.

If $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}\}$ then $n = 2$ and $u\sigma$ being a message implies that there exist $\mathsf{g}/m \in \{\mathsf{senc}, \mathsf{rsenc}\}$, $v_1, \ldots, v_m$ such that $u_1\sigma\downarrow = \mathsf{g}(v_1, \ldots, v_m)$, $u_2\sigma\downarrow = v_m$ and $u\sigma\downarrow = v_1$. Note that $u_2\sigma\downarrow \in \mathsf{Ks}_i$ thanks to Property 2 of Definition 16. Hence, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u_1\sigma\downarrow) = i$. By Properties 7, 8 and 6 of Definition 12, we deduce that $u_1\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $u_1\sigma\downarrow \notin \mathsf{H}_\gamma$. Therefore, we obtain that $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{g}(\mathsf{tr}_\gamma(v_1), \ldots, \mathsf{tr}_\gamma(v_m))$. However, $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{f}(u_1\mathsf{tr}_\gamma(\sigma)\downarrow, u_2\mathsf{tr}_\gamma(\sigma)\downarrow)\downarrow$. By our inductive hypothesis, we deduce that $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{f}(\mathsf{tr}_\gamma(u_1\sigma\downarrow), \mathsf{tr}_\gamma(u_2\sigma\downarrow))\downarrow = \mathsf{f}(\mathsf{g}(\mathsf{tr}_\gamma(v_1), \ldots, \mathsf{tr}_\gamma(v_m)), \mathsf{tr}_\gamma(v_m))\downarrow$. Hence, $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(v_1) = \mathsf{tr}_\gamma(u\sigma\downarrow)$. Note that we already proved that for all $j \in \{1, 2\}$, $u_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow, \gamma)$ then $j = 2$ and $u_2 \in \text{dom}(\rho_\gamma)$. Therefore for $u\mathsf{tr}_\gamma(\sigma)$ to be a message, we only need to show that $u\mathsf{tr}_\gamma(\sigma)\downarrow$ is a constructor term. But we proved that $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(v_1) \in st(\mathsf{tr}_\gamma(u_1\sigma\downarrow))$. Hence, $u\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, $u\sigma\downarrow \in st(u_1\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_1\sigma\downarrow)$ implies by Definition 15 that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$. Lastly, we know that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u_1\sigma\downarrow) = i$, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_1\sigma\downarrow)$, $u\sigma\downarrow = v_1$ and $u_1\sigma\downarrow = \mathsf{g}(v_1, \ldots, v_m)$. Thus by Defini-

tion 15, we deduce that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(v_1,\gamma)$ and so $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow,\gamma)$. Moreover, by Lemma 6, we obtain that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{trH}_\gamma(u\sigma\downarrow)$. Hence the result holds.

Case 3 of Definition 5: In such a case, we know that $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}, \mathsf{check}\}$, for all $j \in \{1,\ldots,n\}$, $(u_j, K_s^j, K_a^j) \in \text{TAGT}(i)$ for some K_s^j, K_a^j and $K_s = \bigcup_{j=1}^n K_s^j$ and $K_a = \{u_n\} \cup \bigcup_{j=1}^n K_a^j$. By Property 5 of Definition 16, we deduce that for all $j \in \{1,\ldots,n\}$, $u_j \notin \text{dom}(\rho_\gamma)$. Hence by Lemma 8, we deduce that for all $j \in \{1,\ldots,n\}$, $(u_j, K_s^j, K_a^j) \in \text{E-TERMS}_i(\mathcal{S})$. Hence, we can apply our inductive hypothesis on u_j meaning that $\mathsf{trH}_\gamma(u_j\sigma\downarrow) = \mathsf{tr}_\gamma(u_j\sigma\downarrow) = u_j\mathsf{tr}_\gamma(\sigma)\downarrow$, $u_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow,\gamma)$.

If $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$ then we deduce that $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow,\ldots,u_n\sigma\downarrow)$. We know that $u_n\sigma\downarrow \in \mathsf{Ka}_i$ thanks to Property 2 of Definition 16. Therefore, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u\sigma\downarrow) = i$. By Properties 6, 7 and 8 of Definition 12, we deduce that $u\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $u\sigma\downarrow \notin \mathsf{H}_\gamma$. Therefore, we obtain $\mathsf{trH}_\gamma(u\sigma\downarrow) = \mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{f}(\mathsf{tr}_\gamma(u_1\sigma\downarrow),\ldots,\mathsf{tr}_\gamma(u_n\sigma\downarrow))$. By our inductive hypothesis, we obtain $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{f}(u_1\mathsf{tr}_\gamma(\sigma)\downarrow,\ldots,u_n\mathsf{tr}_\gamma(\sigma)\downarrow)$. Since $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$, we conclude that $\mathsf{trH}_\gamma(u\sigma\downarrow) = \mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{f}(u_1\mathsf{tr}_\gamma(\sigma),\ldots,u_n\mathsf{tr}_\gamma(\sigma))\downarrow = u\mathsf{tr}_\gamma(\sigma)\downarrow$ and $u\mathsf{tr}_\gamma(\sigma)$ is a message. Since $\mathsf{root}(u\sigma\downarrow) = \mathsf{f}$ and $u\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma)$, we also obtain that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow,\gamma)$. Lastly, since for all $j \in \{1,\ldots,n\}$, $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow,\gamma)$ and $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$, we deduce that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$. Hence the result holds.

If $\mathsf{f} = \mathsf{check}$ then $n = 2$ and $u\sigma$ being a message implies that there exist v_1, v_2 such that $u_1\sigma\downarrow = \mathsf{sign}(v_1, v_2)$, $u_2\sigma\downarrow = \mathsf{vk}(v_2)$ and $u\sigma\downarrow = v_1$. Note that $u_2\sigma\downarrow \in \mathsf{Ka}_i$ thanks to Property 2 of Definition 16. Hence, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u_1\sigma\downarrow) = i$. By Properties 7, 8 and 6 of Definition 12, we deduce that $u_1\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $u_1\sigma\downarrow \notin \mathsf{H}_\gamma$. Therefore, we obtain that $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{sign}(\mathsf{tr}_\gamma(v_1), \mathsf{tr}_\gamma(v_2))$. Note that by Property 10 of Definition 16, we know that $\mathcal{P}^{\mathcal{S}}_{\text{e-keys}}(\mathsf{vk}(v_2), i)$. Hence by Lemma 7, $\mathsf{tr}_\gamma(\mathsf{vk}(v_2)) = \mathsf{vk}(\mathsf{tr}_\gamma(v_2))$. However, $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{f}(u_1\mathsf{tr}_\gamma(\sigma)\downarrow, u_2\mathsf{tr}_\gamma(\sigma)\downarrow)\downarrow$. By our inductive hypothesis, we deduce that $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{f}(\mathsf{tr}_\gamma(u_1\sigma\downarrow), \mathsf{tr}_\gamma(u_2\sigma\downarrow))\downarrow = \mathsf{f}(\mathsf{sign}(\mathsf{tr}_\gamma(v_1), \mathsf{tr}_\gamma(v_2)), \mathsf{vk}(\mathsf{tr}_\gamma(v_2)))\downarrow$. Thus $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(v_1) = \mathsf{tr}_\gamma(u\sigma\downarrow)$. Note that we already proved that for all $j \in \{1,2\}$, $u_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow,\gamma)$. Therefore for $u\mathsf{tr}_\gamma(\sigma)$ to be a message, we only need to show that $u\mathsf{tr}_\gamma(\sigma)\downarrow$ is a constructor term. But we proved that $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(v_1) \in st(\mathsf{tr}_\gamma(u_1\sigma\downarrow))$. Hence, $u\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, $u\sigma\downarrow \in st(u_1\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_1\sigma\downarrow)$ implies by Definition 15 that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$. Lastly, we know that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u_1\sigma\downarrow) = i$, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_1\sigma\downarrow)$, $u\sigma\downarrow = v_1$ and $u_1\sigma\downarrow = \mathsf{sign}(v_1, v_2)$. Thus by Definition 15, we deduce that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(v_1,\gamma)$ and so $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow,\gamma)$. Moreover, by Lemma 6, we obtain that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{trH}_\gamma(u\sigma\downarrow)$. Hence the result holds.

Case 4 of Definition 5: In such a case, we know that $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}\}$ and $n = 2$, for all $j \in \{1,2\}$, $(u_j, K_s^j, K_a^j) \in \text{TAGT}(i)$ for some K_s^j, K_a^j and $K_s = \bigcup_{j=1}^n K_s^j$ and $K_a = \{\mathsf{pk}(u_n)\} \cup \bigcup_{j=1}^n K_a^j$. By Property 5 of Definition 16, we deduce that $u_1 \notin \text{dom}(\rho_\gamma)$. If $u_2 \in \text{dom}(\rho_\gamma)$ then $u_2\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(u_2\sigma)\downarrow$. But thanks to Property 2 of Definition 12, we deduce that $\mathsf{tr}_\gamma(u_2\sigma) = u_2\sigma\rho^\sigma_\gamma \in \mathcal{N}_{abs}$. Hence $\mathsf{tr}_\gamma(u_2\sigma)\downarrow = \mathsf{tr}_\gamma(u_2\sigma)$ and $u_2\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, by Property 4 of Definition 16, we know that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_2\sigma)$.

Moreover, by Lemma 8, we deduce that $(u_1, K_s^1, K_a^1) \in \text{E-TERMS}_i(\mathcal{S})$ and if $u_2 \notin \text{dom}(\rho_\gamma)$ then $(u_2, K_s^2, K_a^2) \in \text{E-TERMS}_i(\mathcal{S})$. Hence, we can apply our inductive hypothesis on u_1 and on u_2 when $u_2 \notin \text{dom}(\rho_\gamma)$ meaning that for all $j \in \{1,2\}$, $\mathsf{tr}_\gamma(u_j\sigma\downarrow) = u_j\mathsf{tr}_\gamma(\sigma)\downarrow$, $u_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow,\gamma)$ then $j = 2$ and $u_2 \in \text{dom}(\rho_\gamma)$.

Since $u\sigma$ is a message then there exist $\mathsf{g}/m \in \{\mathsf{aenc}, \mathsf{raenc}\}$ ($\mathsf{g} = \mathsf{aenc}$ when $\mathsf{f} = \mathsf{adec}$ else $\mathsf{g} = \mathsf{raenc}$) and $v_1,\ldots,v_m$ such that $u_1\sigma\downarrow = \mathsf{g}(v_1,\ldots,v_m)$, $\mathsf{pk}(u_2\sigma\downarrow) = v_m$ and $u\sigma\downarrow = v_1$. Note that $\mathsf{pk}(u_2\sigma\downarrow) \in \mathsf{Ka}_i$ thanks to Property 2 of Definition 16. Hence, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u_1\sigma\downarrow) = i$. By Properties 7, 8 and 6 of Definition 12, we deduce that $u_1\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $u_1\sigma\downarrow \notin \mathsf{H}_\gamma$. Therefore, we obtain that $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{g}(\mathsf{tr}_\gamma(v_1),\ldots,\mathsf{tr}_\gamma(v_m))$. Note that by Property 9 of Definition 16, we know that $\mathcal{P}^{\mathcal{S}}_{\text{e-keys}}(\mathsf{pk}(u_2\sigma\downarrow), i)$. Hence by Lemma 7, $\mathsf{tr}_\gamma(\mathsf{pk}(u_2\sigma\downarrow)) = \mathsf{pk}(\mathsf{tr}_\gamma(u_2\sigma\downarrow))$.

However, $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{f}(u_1\mathsf{tr}_\gamma(\sigma)\downarrow, u_2\mathsf{tr}_\gamma(\sigma)\downarrow)\downarrow$. Hence $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{f}(\mathsf{tr}_\gamma(u_1\sigma\downarrow), \mathsf{tr}_\gamma(u_2\sigma\downarrow))\downarrow = \mathsf{f}(\mathsf{g}(\mathsf{tr}_\gamma(v_1),\ldots,\mathsf{tr}_\gamma(v_m)), \mathsf{tr}_\gamma(u_2\sigma\downarrow))\downarrow$ with $\mathsf{tr}_\gamma(v_m) = \mathsf{pk}(\mathsf{tr}_\gamma(u_2\sigma\downarrow))$. Thus $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(v_1) = \mathsf{tr}_\gamma(u\sigma\downarrow)$. Note that we already proved that for all $j \in \{1,2\}$, $u_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow,\gamma)$ then $j = 2$ and $u_2 \in \text{dom}(\rho_\gamma)$. Therefore for $u\mathsf{tr}_\gamma(\sigma)$ to be a message, we only need to show that $u\mathsf{tr}_\gamma(\sigma)\downarrow$ is a constructor term. But we proved that $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(v_1) \in st(\mathsf{tr}_\gamma(u_1\sigma\downarrow))$.

Hence, $u\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, $u\sigma\downarrow \in st(u_1\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_1\sigma\downarrow)$ implies by Definition 15 that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$. Lastly, we know that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u_1\sigma\downarrow) = i$, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_1\sigma\downarrow)$, $u\sigma\downarrow = v_1$ and $u_1\sigma\downarrow = \mathsf{g}(v_1, v_2)$. Thus by Definition 15, we deduce that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(v_1, \gamma)$ and so $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow, \gamma)$. Moreover, by Lemma 6, we obtain that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{trH}_\gamma(u\sigma\downarrow)$. Hence the result holds.

Case 5 of Definition 5: In such a case, we know that $\mathsf{f} = \mathsf{sign}$, $n = 2$ and for all $j \in \{1, 2\}$, $(u_j, K^j_s, K^j_a) \in \text{TAGT}(i)$ for some K^j_s, K^j_a and $K_s = \bigcup_{j=1}^{2} K^j_s$ and $K_a = \{\mathsf{vk}(u_2)\} \cup \bigcup_{j=1}^{n} K^j_a$. By Property 5 of Definition 16, we deduce that $u_1 \notin \text{dom}(\rho_\gamma)$. If $u_2 \in \text{dom}(\rho_\gamma)$ then $u_2\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(u_2\sigma)\downarrow$. But thanks to Property 2 of Definition 12, we deduce that $\mathsf{tr}_\gamma(u_2\sigma) = u_2\sigma\rho^\sigma_\gamma \in \mathcal{N}_{abs}$. Hence $\mathsf{tr}_\gamma(u_2\sigma)\downarrow = \mathsf{tr}_\gamma(u_2\sigma)$ and $u_2\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, by Property 4 of Definition 16, we know that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_2\sigma)$.

Moreover, by Lemma 8, we deduce that for all $(u_1, K^1_s, K^1_a) \in \text{E-TERMS}_i(\mathcal{S})$ and if $u_2 \notin \text{dom}(\rho_\gamma)$ then $(u_2, K^2_s, K^2_a) \in \text{E-TERMS}_i(\mathcal{S})$. Hence, we can apply our inductive hypothesis on u_1 and on u_2 when $u_2 \notin \text{dom}(\rho_\gamma)$ meaning that for all $j \in \{1, 2\}$, $\mathsf{tr}_\gamma(u_j\sigma\downarrow) = u_j\mathsf{tr}_\gamma(\sigma)\downarrow$, $u_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow, \gamma)$ then $j = 2$ and $u_2 \in \text{dom}(\rho_\gamma)$.

Since $\mathsf{f} = \mathsf{sign}$, we deduce that $u\sigma\downarrow = \mathsf{sign}(u_1\sigma\downarrow, u_2\sigma\downarrow)$. Moreover, we know that $\mathsf{vk}(u_n\sigma\downarrow) \in \mathsf{Ka}_i$ thanks to Property 2 of Definition 16. Therefore, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u\sigma\downarrow) = i$. By Properties 8, 7 and 6 of Definition 12, we deduce that $u\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $u\sigma\downarrow \notin \mathsf{H}_\gamma$. Therefore, we obtain $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{sign}(\mathsf{tr}_\gamma(u_1\sigma\downarrow), \mathsf{tr}_\gamma(u_2\sigma\downarrow))$. By our inductive hypothesis, we obtain $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{sign}(u_1\mathsf{tr}_\gamma(\sigma)\downarrow, u_2\mathsf{tr}_\gamma(\sigma)\downarrow)$. We conclude that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{sign}(u_1\mathsf{tr}_\gamma(\sigma), u_2\mathsf{tr}_\gamma(\sigma))\downarrow = u\mathsf{tr}_\gamma(\sigma)\downarrow$ and $u\mathsf{tr}_\gamma(\sigma)$ is a message. Since $\mathsf{root}(u\sigma\downarrow) = \mathsf{sign}$ and $u\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma)$, we directly obtain that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow, \gamma)$. Lastly, we know that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u\sigma\downarrow) = i$ and for all $j \in \{1, 2\}$, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u_j\sigma\downarrow, \gamma)$ then $j = 2$ and $u_2 \in \text{dom}(\rho_\gamma)$. Thus, we directly obtain that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$ holds. Lastly, by Lemma 6, we obtain that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{trH}_\gamma(u\sigma\downarrow)$. Hence the result holds.

Case 6 of Definition 5: In such a case, we know that $n = 1$, $\mathsf{f} = \mathsf{untag}_i$ and there exist $\mathsf{g} \in \{\mathsf{sdec}, \mathsf{adec}, \mathsf{rsdec}, \mathsf{radec}, \mathsf{check}\}$ and $(v_1, K^1_s, K^1_a), (v_2, K^2_s, K^2_a) \in \text{TAGT}(i)$ such that $u_1 = \mathsf{g}(v_1, v_2)$, $K_s = K^1_s \cup K^2_s$ and $K_a = K^1_a \cup K^2_a$. By Property 5 of Definition 16, we deduce that $v_1 \notin \text{dom}(\rho_\gamma)$ and if $v_2 \in \text{dom}(\rho_\gamma)$ then $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}\}$. Furthermore, if $v_2 \in \text{dom}(\rho_\gamma)$ then $v_2\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(v_2\sigma)\downarrow$. But thanks to Property 2 of Definition 12, we deduce that $\mathsf{tr}_\gamma(v_2\sigma) = v_2\sigma\rho^\sigma_\gamma \in \mathcal{N}_{abs}$. Hence $\mathsf{tr}_\gamma(v_2\sigma)\downarrow = \mathsf{tr}_\gamma(v_2\sigma)$ and $v_2\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, by Property 4 of Definition 16, we know that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(v_2\sigma)$.

Moreover, by Lemma 8, we deduce that $(v_1, K^1_s, K^1_a) \in \text{E-TERMS}_i(\mathcal{S})$ and if $v_2 \notin \text{dom}(\rho_\gamma)$ then $(v_2, K^2_s, K^2_a) \in \text{E-TERMS}_i(\mathcal{S})$. Hence, we can apply our inductive hypothesis on v_1 and on v_2 when $v_2 \notin \text{dom}(\rho_\gamma)$ meaning that for all $j \in \{1, 2\}$, $\mathsf{tr}_\gamma(v_j\sigma\downarrow) = v_j\mathsf{tr}_\gamma(\sigma)\downarrow$, $v_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(v_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(v_j\sigma\downarrow, \gamma)$ then $j = 2$, $\mathsf{g} \in \{\mathsf{sdec}, \mathsf{rsdec}\}$ and $v_2 \in \text{dom}(\rho_\gamma)$.

We know that $u\sigma\downarrow$ is a message. Hence, there exist a function symbol g'/m and $w_1, \ldots, w_m$ such that $\mathsf{g}' = \mathsf{senc}$ (resp. $\mathsf{aenc}, \mathsf{rsenc}, \mathsf{raenc}$ and sign) and $u\sigma\downarrow = w_1$, $v_1\sigma\downarrow = \mathsf{g}'(\mathsf{tag}_i(w_1), w_2, \ldots, w_m)$ and $v_2\sigma\downarrow = w_m$ (resp. $\mathsf{pk}(v_2\sigma\downarrow) = w_m$, $v_2\sigma\downarrow = w_m$, $\mathsf{pk}(v_2\sigma\downarrow) = v_m$ and $v_2\sigma\downarrow = \mathsf{vk}(w_m)$) when $\mathsf{g} = \mathsf{sdec}$ (resp. $\mathsf{adec}, \mathsf{rsdec}, \mathsf{radec}$ and check). Note that by Property 11 (resp. 9, 11, 9 and 10) of Definition 16, we deduce that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(\mathsf{g}'(\mathsf{tag}_i(w_1), w_2, \ldots, w_n)) = i$. By Properties 8, 7 and 6 of Definition 12, we deduce that $v_1\sigma\downarrow, \mathsf{tag}_i(w_1) \notin \text{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $v_1\sigma\downarrow \notin \mathsf{H}_\gamma$. Therefore, we obtain that $\mathsf{tr}_\gamma(v_1\sigma\downarrow) = \mathsf{g}'(\mathsf{tag}_i(\mathsf{tr}_\gamma(w_1)), \ldots, \mathsf{tr}_\gamma(w_m))$. Moreover, Lemma 7, we also deduce that $\mathsf{tr}_\gamma(\mathsf{pk}(v_2\sigma\downarrow)) = \mathsf{pk}(\mathsf{tr}_\gamma(v_2\sigma\downarrow))$ when $\mathsf{g} \in \{\mathsf{adec}, \mathsf{radec}\}$ and $\mathsf{tr}_\gamma(\mathsf{vk}(w_m)) = \mathsf{vk}(\mathsf{tr}_\gamma(w_m))$ when $\mathsf{g} = \mathsf{check}$.

However, $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{untag}_i(\mathsf{g}(v_1\mathsf{tr}_\gamma(\sigma)\downarrow, v_2\mathsf{tr}_\gamma(\sigma)\downarrow))\downarrow$. Hence $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{untag}_i(\mathsf{g}(\mathsf{tr}_\gamma(v_1\sigma\downarrow), \mathsf{tr}_\gamma(v_2\sigma\downarrow)))\downarrow = \mathsf{untag}_i(\mathsf{g}(\mathsf{g}'(\mathsf{tag}_i(\mathsf{tr}_\gamma(w_1)), \ldots, \mathsf{tr}_\gamma(w_m)), \mathsf{tr}_\gamma(v_2\sigma\downarrow)))\downarrow$ with $\mathsf{tr}_\gamma(w_m) = \mathsf{tr}_\gamma(v_2\sigma\downarrow)$ when $\mathsf{g} \in \{\mathsf{sdec}, \mathsf{rsdec}\}$, with $\mathsf{tr}_\gamma(w_m) = \mathsf{pk}(\mathsf{tr}_\gamma(v_2\sigma\downarrow))$ when $\mathsf{g} \in \{\mathsf{adec}, \mathsf{radec}\}$ and $\mathsf{tr}_\gamma(v_2\sigma\downarrow) = \mathsf{vk}(\mathsf{tr}_\gamma(w_m))$ when $\mathsf{g} = \mathsf{check}$. Thus $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(w_1) = \mathsf{tr}_\gamma(u\sigma\downarrow)$. Note that we already proved that for all $j \in \{1, 2\}$, $v_j\mathsf{tr}_\gamma(\sigma)$ is a message, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(v_j\sigma\downarrow)$ and if $\neg\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(v_j\sigma\downarrow, \gamma)$ then $j = 2$, $\mathsf{g} \in \{\mathsf{sdec}, \mathsf{rsdec}\}$ and $v_2 \in \text{dom}(\rho_\gamma)$. Therefore for $u\mathsf{tr}_\gamma(\sigma)$ to be a message, we only need to show that $u\mathsf{tr}_\gamma(\sigma)\downarrow$ is a constructor term. But we proved that $u\mathsf{tr}_\gamma(\sigma)\downarrow = \mathsf{tr}_\gamma(w_1) \in st(\mathsf{tr}_\gamma(v_1\sigma\downarrow))$. Hence, $u\mathsf{tr}_\gamma(\sigma)$ is a message. Moreover, $u\sigma\downarrow \in st(v_1\sigma\downarrow)$ and $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(v_1\sigma\downarrow)$ implies by Definition 15

that $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(u\sigma\downarrow)$. Lastly, we know that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(v_1\sigma\downarrow) = i$, $\mathcal{P}^{\mathcal{S}}_{\text{gen}}(v_1\sigma\downarrow)$, $u\sigma\downarrow = w_1$ and $v_1\sigma\downarrow = \mathsf{g}'(\mathsf{tag}_i(w_1), w_2, \ldots, w_m)$. Thus by Definition 15, we deduce that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(w_1, \gamma)$ and so $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(u\sigma\downarrow, \gamma)$. Moreover, by Lemma 6, we obtain that $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{trH}_\gamma(u\sigma\downarrow)$. Hence the result holds.

Lemma 11. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup and let tr and trH be the transformation functions of $\mathcal{S}$. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. Let $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$. If $u\mathsf{tr}_\gamma(\sigma)$ is a message then $u\sigma$ is message.*

Proof. We prove this result by induction on $|u|$.

Base case $|u| = 1$: In such a case, by Lemma 4, we know that either $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ or $u \in \mathcal{X}$. Since $\text{img}(\sigma)$ is a set of ground messages in normal form, we deduce that $u\sigma$ is a message.

Inductive step $|u| > 1$: There exists f/n and $u_1, \ldots, u_n$ such that $u = \mathsf{f}(u_1, \ldots, u_n)$. By Property 1 of Definition 16, we know that $(u, K_s, K_a) \in \text{TAGT}(i)$. We do a case analysis on the different cases of Definition 5.

Cases 2,3,4,5,8 of Definition 5 with $\mathsf{f} \notin \Sigma_i$: In such a case, $(u_1, K_s^1, K_a^1), \ldots, (u_n, K_s^n, K_a^n) \in \text{TAGT}(i)$ for some $K_s^1, K_a^1, \ldots, K_s^n, K_a^n$. Moreover, by Lemma 8 and Property 5 of Definition 16, we deduce that for all $j \in \{1, \ldots, n\}$, $(u_j, K_s^j, K_a^j) \notin \text{E-TERMS}_i(\mathcal{S})$ implies $u_j \in \text{dom}(\rho_\gamma)$. If $u_j \in \text{dom}(\rho_\gamma)$ then we have that $u_j\sigma$ is a message since $\text{img}(\sigma)$ is a set of ground messages in normal form. Otherwise, by inductive hypothesis and since $u\mathsf{tr}_\gamma(\sigma)$ being a message implies $u_j\mathsf{tr}_\gamma(\sigma)$ being a message, we obtain that $u_j\sigma$ is a message. Therefore, we deduce that for all $j \in \{1, \ldots, n\}$, $u_j\sigma$ is a message. Hence, we only need to prove that $u\sigma\downarrow$ does not contain destructor function symbol. If $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}, \mathsf{h}, \langle\,\rangle, \mathsf{vk}, \mathsf{pk}, \mathsf{tag}_i\}$ then the result directly holds. Else $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}, \mathsf{check}, \mathsf{adec}, \mathsf{radec}, \mathsf{proj}_1, \mathsf{proj}_2\}$ and in such a case, because $u\mathsf{tr}_\gamma(\sigma)$ is a message, we have

- Case $\mathsf{f} = \mathsf{sdec}$: $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{senc}(v_1, v_2)$ and $\mathsf{tr}_\gamma(u_2\sigma\downarrow) = v_2$ for some v_1, v_2. By Lemma 4 and by Property 9 of Definition 12, we deduce that $u_1\sigma\downarrow = \mathsf{senc}(V_1, V_2)$ and $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{senc}(\mathsf{tr}_\omega(V_1), \mathsf{tr}_\omega(V_2))$ for some V_1, V_2, ω. Hence, $\mathsf{tr}_\omega(V_2) = \mathsf{tr}_\gamma(u_2\sigma\downarrow)$ which implies by Lemma 3 that $V_2 = u_2\sigma\downarrow$. Thus, $u\sigma\downarrow = V_1$. Since $u_1\sigma$ is a message than we conclude that $u\sigma\downarrow$ does not contain destructor function symbol which allows us to conclude.
- Case $\mathsf{f} = \mathsf{rsdec}$: Similar to the previous case.
- Case $\mathsf{f} = \mathsf{check}$: $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{sign}(v_1, v_2)$ and $\mathsf{tr}_\gamma(u_2\sigma\downarrow) = \mathsf{vk}(v_2)$ for some v_1, v_2. By Lemma 4, we deduce that $u_1\sigma\downarrow = \mathsf{sign}(V_1, V_2)$ and $u_2\sigma\downarrow = \mathsf{vk}(V_3)$ for some V_1, V_2, V_3. Note that we showed that $u_2\sigma$ is a message. Moreover, by Property 10 of Definition 16 and by Lemma 7, we obtain that $\mathsf{tr}_\gamma(u_2\sigma\downarrow) = \mathsf{vk}(\mathsf{tr}_\gamma(V_3))$. Moreover, by Property 9 of Definition 12, we also have $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{sign}(\mathsf{tr}_\omega(V_1), \mathsf{tr}_\omega(V_2))$ for some ω. This gives us $\mathsf{vk}(\mathsf{tr}_\omega(V_2)) = \mathsf{vk}(\mathsf{tr}_\gamma(V_3))$ and so $V_2 = V_3$ by Lemma 3. Thus, $u\sigma\downarrow = V_1$. Since $u_1\sigma$ is a message than we conclude that $u\sigma\downarrow$ does not contain destructor function symbol which allows us to conclude.
- Case $\mathsf{f} = \mathsf{adec}$: $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{aenc}(v_1, \mathsf{pk}(v_2))$ and $\mathsf{tr}_\gamma(u_2\sigma\downarrow) = v_2$ for some v_1, v_2. By Lemma 4, we deduce that $u_1\sigma\downarrow = \mathsf{aenc}(V_1, \mathsf{pk}(V_2))$ and $u_2\sigma\downarrow = V_3$ for some V_1, V_2 and V_3. Moreover, we also obtain that $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \mathsf{aenc}(\mathsf{tr}_\omega(V_1), \mathsf{pk}(\delta(\omega, V_2)))$ and $\mathsf{tr}_\gamma(u_2\sigma\downarrow) = \mathsf{tr}_\gamma(V_3)$ for some $\delta \in \{\mathsf{tr}, \mathsf{trH}\}$ and ω. Thus, $\delta(\omega, V_2) = \mathsf{tr}_\gamma(V_3)$. By Lemma 3, we obtain that $V_2 = V_3$. Therefore, $u\sigma\downarrow = V_1$. Since $u_1\sigma$ is a message than we conclude that $u\sigma\downarrow$ does not contain destructor function symbol which allows us to conclude.
- Case $\mathsf{f} = \mathsf{radec}$: Similar to previous case.
- Case $\mathsf{proj}_j, j = 1, 2$: $\mathsf{tr}_\gamma(u_1\sigma\downarrow) = \langle v_1, v_2\rangle$. By Lemma 4, we deduce that $u_1\sigma\downarrow = \langle V_1, V_2\rangle$ for some V_1, V_2. Hence $u\sigma\downarrow = V_j$. Since $u_1\sigma$ is a message than we conclude that $u\sigma\downarrow$ does not contain destructor function symbol which allows us to conclude.

Recall that given two terms u and v, and given a substitution σ, $\sigma \models u = v$ iff $u\sigma\downarrow$ is a message, $v\sigma\downarrow$ is a message and $u\sigma\downarrow = v\sigma\downarrow$.

Lemma 12. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup and let tr and trH be the transformation functions of $\mathcal{S}$. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. Let $(u, K_s, K_a), (v, K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$. We have $\sigma \models u = v$ if and only if $\mathsf{tr}_\gamma(\sigma) \models u = v$.*

Proof. By definition, we know that $\sigma \models u = v$ if and only if $u\sigma\downarrow$ is a message, $v\sigma\downarrow$ is a message and $u\sigma\downarrow = v\sigma\downarrow$. By Lemmas 11 and 10, we obtain that $u\sigma\downarrow$ and $v\sigma\downarrow$ are messages if and only if $\mathsf{tr}_\gamma(u\sigma\downarrow)$ and $\mathsf{tr}_\gamma(v\sigma\downarrow)$ are messages. Moreover, Lemma 10 also gives us that $\mathsf{tr}_\gamma(()u\sigma\downarrow) = u\mathsf{tr}_\gamma(\sigma)\downarrow$ and $\mathsf{tr}_\gamma(v\sigma\downarrow) = v\mathsf{tr}_\gamma(\sigma)\downarrow$. Therefore, if $\sigma \models u = v$ then $u\mathsf{tr}_\gamma(\sigma)\downarrow$ is a message, $v\mathsf{tr}_\gamma(\sigma)\downarrow$ is a message and $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{tr}_\gamma(v\sigma\downarrow)$ which implies $u\mathsf{tr}_\gamma(\sigma)\downarrow\downarrow = v\mathsf{tr}_\gamma(\sigma)\downarrow\downarrow$. Hence $\mathsf{tr}_\gamma(\sigma) \models u = v$. On the other hand, if $\mathsf{tr}_\gamma(\sigma)\downarrow\downarrow \models u = v$ then $u\sigma\downarrow$ is a message, $v\sigma\downarrow$ is a message and $\mathsf{tr}_\gamma(u\sigma\downarrow) = \mathsf{tr}_\gamma(v\sigma\downarrow)$. By Lemma 3, we deduce that $u\sigma\downarrow = v\sigma\downarrow$ and so $\sigma \models u = v$. □

E Derived frame

In the next definition, we will need to consider a total order on variables from $\mathcal{X}$. For some minimality purpose, we will consider a special variable $\mathsf{x}_0 \in \mathcal{X}$ that will only use for defining such orders (meaning that this variable never appear in processes and is never used in the derivation of a process). Moreover, given a set of name $\mathcal{E}$ and a frame Φ, we define $\mathsf{Recipe}(\mathcal{E}, \Phi)$ as the set of terms M such that $fv(M) \subseteq \mathrm{dom}(\Phi)$, $names(M) \cap \mathcal{E}$ and $M\Phi$ is a message.

Definition 17. *Let $(\sigma, \rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{Ks}, \mathsf{Ka}) \in$ Setup. Let Φ be a substitution of ground messages in normal form. Let $\mathcal{E}$ be a set of names. Let $\prec$ a strict total order on variables. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. Let x be a variable.*

We define $\mathcal{P}_\prec^{\nu\mathcal{E}.\Phi}(v, x)$ the predicate to hold iff for all $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, if for all $y \in fv(M)$, $y \prec x$ then $M\Phi\downarrow \neq v$.

We define MuTerms$(v, x, \prec, \mathcal{E}, \Phi)$ *as the set such that if $\mathsf{root}(v) \in \{\mathsf{h}, \mathsf{pk}, \mathsf{vk}\}$, $v = C[v_1, \ldots, v_n]$ and*

- *for all $p \in \mathcal{P}os(C)$, $C|_p \neq \_$ implies $\mathsf{root}(v|_p) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\ \rangle\}$ and $\mathcal{P}_\prec^{\nu\mathcal{E}.\Phi}(v|_p, x)$*
- *for all $j \in \{1, \ldots, n\}$ either $\mathsf{root}(v_i) \notin \{\mathsf{h}, \mathsf{pk}, \mathsf{vk}, \langle\ \rangle\}$ or $\neg\mathcal{P}_\prec^{\nu\mathcal{E}.\Phi}(v_i, x)$*

then $\{v_i \mid i \in \{1, \ldots, n\} \wedge \mathcal{P}_\prec^{\nu\mathcal{E}.\Phi}(v_i, x)\} =$ MuTerms$(v, x, \prec, \mathcal{E}, \Phi)$.

Definition 18 (Derived Frame). *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. We define the set* DFrame$(\mathcal{S})$ *as the smallest set such that for all substitutions Φ of ground terms in normal form, for all sets $\mathcal{E}$ of names, for all relation $\prec$ on variables, for all mapping μ_{col} from $\mathrm{dom}(\Phi) \cup \mathrm{dom}(\sigma)$ to $\{1, \ldots, p\}$, if the following conditions hold:*

1. $\mathrm{dom}(\Phi) \cap \mathrm{dom}(\sigma) = \emptyset$
2. *for all $\gamma \in \{\alpha, \beta\}$, for all $x \in \mathrm{dom}(\rho_\gamma)$, $x\mu_{col} \notin \gamma$*
3. *$\prec$ is a strict total order on $\mathrm{dom}(\Phi) \cup \mathrm{dom}(\sigma) \cup \{\mathsf{x}_0\}$ such that for all $x \in \mathrm{dom}(\Phi) \cup \mathrm{dom}(\sigma)$, $\mathsf{x}_0 \prec x$*
4. *$\mathrm{img}(\rho_\alpha, \rho_\beta) \subseteq \mathcal{E}$, $(n_{min} \cup \mathrm{img}(\mu_\alpha, \mu_\beta)) \cap \mathcal{E} = \emptyset$ and $names(\Phi) \cap \mathcal{N}_{abs} = \emptyset$*
5. *for all $x \in \mathrm{dom}(\Phi)$ (resp. $\mathrm{dom}(\sigma)$), either*
   (a) *there exist $\gamma \in \{\alpha, \beta\}$, $i \in \gamma$ and $(u, K_s, K_a) \in$ E-terms$_i(\mathcal{S})$ such that $i = x\mu_{col}$, $u\sigma\downarrow = x\Phi$ (resp. $x\sigma$), $u\sigma$ is a message and for all $z \in fv(u)$, $z \prec x$ and either $z\mu_{col} = i$ or $z \in \mathrm{dom}(\rho_\gamma)$*
   (b) *there exists $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $fv(M) \subseteq \{z \mid z \prec x\}$ and $M\Phi\downarrow = x\Phi$ (resp. $x\sigma$)*
6. *for all $\gamma, \omega \in \{\alpha, \beta\}.\gamma \neq \omega$, for all terms v, $v \in \mathrm{dom}(\mathsf{H}_\gamma)$ if and only if there exist $(x, u) \in$ ProTerm$(\Phi, \mathcal{S})$, $u' \in st(u)$ such that*
   (a) *$x\mu_{col} \in \omega$ and $u'\sigma\downarrow = v$; and*
   (b) *$\mathsf{root}(v) \in \{\mathsf{h}, \mathsf{pk}, \mathsf{vk}\}$; and*
   (c) *$\mathcal{P}_\prec^{\nu\mathcal{E}.\Phi}(v, x)$.*

   Moreover, we have MuTerms$(v, x, \prec, \mathcal{E}, \Phi) \subseteq \mathrm{dom}(\mu_\gamma)$.
7. *for all $(x, u), (y, v) \in$ ProTerm$(\Phi, \mathcal{S})$, if $x\mu_{col} \neq y\mu_{col}$ then for all $n \in \mathcal{N} \cap names(u) \cap names(v)$, $n \notin \mathcal{E}$*

then $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in$ DFrame$(\mathcal{S})$ where ProTerm$(\Phi, \mathcal{S})$ *denote the sets of elements of the form (x, u) where $x \in \mathrm{dom}(\Phi) \cup \mathrm{dom}(\sigma)$ and x satisfies Property 5a with the term u.*

Definition 19. *Let* $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ *be a setup and let* tr *and* trH *be the transformation functions of* $\mathcal{S}$*. Let* $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \text{DFrame}(\mathcal{S})$*.*

We denote by $\mathsf{tr}(\Phi)$ *the substitution such that:*

- $\text{dom}(\Phi) = \text{dom}(\mathsf{tr}(\Phi))$
- *for all* $x \in \text{dom}(\Phi)$*, for all* $\gamma \in \{\alpha, \beta\}$*,* $x\mu_{col} \in \gamma$ *implies* $x\mathsf{tr}(\Phi) = \mathsf{tr}_\gamma(x\Phi)$

In the rest of this section, we will try to show that if a term is deducible in a frame, then its abstract version is also deducible in the abstract version of the frame. In order to do so, we need to consider a measure on terms that will be useful in the proofs.

Definition 20. *Let* $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ *be a setup. Let* $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \text{DFrame}(\mathcal{S})$*. We define the measure* $\mathcal{M}_\prec^{\mathcal{E},\Phi}$ *defined on terms* M *such that* $fv(M) \subseteq \text{dom}(\Phi)$ *and* $names(M) \cap \mathcal{E} = \emptyset$ *and such that* $\mathcal{M}_\prec^{\mathcal{E},\Phi}(M) = (x, |M|)$ *when the following properties hold:*

- *if* $fv(M) = \emptyset$ *then* $x = \mathsf{x}_0$ *else* $x \in fv(M)$
- *for all* $z \in fv(M)$*,* $x \not\prec z$
- $|M|$ *denotes the size of the term* M*,* i.e. *the number of symbols that occur in* M*.*

Moreover, we consider the strict total order relation $<$ *such that given two terms* M_1, M_2 *with* $\mathcal{M}_\prec^{\mathcal{E},\Phi}(M_1) = (x_1, i_1)$ *and* $\mathcal{M}_\prec^{\mathcal{E},\Phi}(M_2) = (x_2, i_2)$*,* $\mathcal{M}_\prec^{\mathcal{E},\Phi}(M_1) < \mathcal{M}_\prec^{\mathcal{E},\Phi}(M_2)$ *when either* $x_1 \prec x_2$ *or* $x_1 = x_2$ *and* $i_1 < i_2$*.*

E.1 Tagged factors

Definition 21. *Let* $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ *be a setup. Let* $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \text{DFrame}(\mathcal{S})$*. Let* t *be a ground message in normal form. Let* $\gamma, \omega \in \{\alpha, \beta\}$ *such that* $\gamma \neq \omega$*. We define* $Fct_\gamma(t)$ *as the smallest set such that:*

- $Fct_\gamma(t) = \{(t, \varepsilon)\}$ *when* $t \in \mathcal{N} \setminus \{n \in names(u) \cup \{n_{min}\} \mid (x, u) \in \text{ProTerm}(\Phi, \mathcal{S}) \wedge x\mu_{col} \in \gamma\}$
- $Fct_\gamma(\mathsf{f}(t_1, \ldots, t_n)) = \bigcup_{i=1}^n \{(u, i{\cdot}p) \mid (u, p) \in Fct_\gamma(t_i)\}$ *when* $\mathsf{f} \in \bigcup_{i \in \gamma} \Sigma_i \cup \{\mathsf{tag}_i\} \cup \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$
- $Fct_\gamma(\mathsf{tagk}_i(t)) = \{(u, 1 \cdot p) \mid (u, p) \in Fct_\gamma(t)\}$ *when* $i \in \gamma$ *and* $t \notin \text{dom}(\rho_\gamma^\sigma)$
- $Fct_\gamma(\mathsf{f}(t_1, \ldots, t_n)) = \{(u, 1 \cdot p) \mid (u, p) \in Fct_\gamma(t_1)\}$ *when* $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(\mathsf{f}(t_1, \ldots, t_n)) \in \gamma$ *and* $\mathsf{f} \in \Sigma_0$
- $Fct_\gamma(t) = \{(t, \varepsilon)\}$ *when* $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t) \in \omega$ *or when* $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t) = 0$ *and* $\mathsf{root}(t) \notin \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$*.*

Definition 22. *Let* t *be a ground message in normal form. Let* $\gamma \in \{\alpha, \beta\}$*. Let* u, v *two terms. Let* $p \in \mathcal{P}os(t)$*. We define the predicate* $\mathcal{P}_{Fct}((u, p), t, v)$ *to hold if and only if when* $u = v$ *or there exists* $q \in \mathcal{P}os(t)$ *such that:*

- $\mathsf{root}(v) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$
- $v = t|_q$
- $q < q$
- $\forall q' \in \mathcal{P}os(t)$*,* $q < q' < p$ *implies* $\mathsf{root}(t|_{q'}) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$*.*

We define the predicate $\mathcal{P}^m_{Fct}((u, p), t, v)$ *to hold if and only if* $\mathcal{P}_{Fct}((u, p), t, v)$ *and for all terms* v'*,* $\mathcal{P}_{Fct}((u, p), t, v')$ *implies* $v' \in st(v)$*.*

Lemma 13. *Let* $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ *be a setup. Let* $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \text{DFrame}(\mathcal{S})$*. Let* $\gamma \in \{\alpha, \beta\}$*. Let* $i \in \gamma$*. For all* $(u, K_s, K_a) \in \text{E-terms}_i(\mathcal{S})$*, for all* $(t, p) \in Fct_\gamma(u\sigma\downarrow)$*, if* $u\sigma$ *is a message and* $names(u) \subseteq \{n \in names(u) \mid (x, v) \in \text{ProTerm}(\Phi, \mathcal{S}) \wedge x\mu_{col} \in \gamma\}$ *then there exist a term* v*,* $x \in fv(u) \setminus \text{dom}(\rho_\gamma)$ *and* $q \in \mathcal{P}os(x\sigma)$ *such that:*

- $(t, q) \in Fct_\gamma(x\sigma)$
- $\mathcal{P}_{Fct}((t, p), u\sigma\downarrow, v)$
- $\mathcal{P}^m_{Fct}((t, q), x\sigma, v)$*.*

Proof. We prove this result by induction on $|u|$. Since $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$, we know that Property 1 of Definition 16 holds, meaning that $(u, K_s, K_a) \in \text{TAGT}(\gamma)$.

Base case $|u| = 1$*:* In such a case, $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ or $u \in \mathcal{X} \setminus \text{dom}(\rho_\gamma)$. If $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ then $u\sigma\downarrow = u$ and by hypothesis, $u \in \{n \in names(u) \mid (x, v) \in \text{PROTERM}(\Phi, \mathcal{S}) \wedge x\mu_{col} \in \gamma\}$ meaning that $Fct_\gamma(u\sigma\downarrow) = \emptyset$. Hence $u \in \mathcal{X} \setminus \text{dom}(\rho_\gamma)$ and so $u\sigma\downarrow = u\sigma$. Note that $\mathcal{P}_{Fct}((t, p), u\sigma, t)$ meaning that there exists a term v such that $\mathcal{P}^m_{Fct}((t, p), u\sigma, v)$. Therefore, the result holds with $q = p$, $x = u$ and v.

Inductive step $|u| > 1$*:* In such a case, $u = \mathsf{f}(u_1, \ldots, u_n)$. We can do a case analysis on u following Definition 5:

- Case $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$: In such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Moreover, since $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$, we deduce that $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u\sigma\downarrow) = i$. Hence $Fct_\gamma(u\sigma\downarrow) = \{(v, 1 \ldots q) \mid (v, q) \in Fct_\gamma(u_1\sigma\downarrow)\}$. Therefore, there exists $p' \in \mathcal{P}os(u_1\sigma\downarrow)$ such that $p = 1 \cdot p'$ and $(t, p') \in Fct_\gamma(u_1\sigma\downarrow)$. Thanks to Lemma 8 and by Definition 5 and 16, we deduce that there exist K'_s, K'_a such that $(u_1, K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$. Moreover, $names(u_1) \subseteq names(u)$ thus $names(u_1) \subseteq \{n \in names(u) \mid (x, v) \in \text{PROTERM}(\Phi, \mathcal{S}) \wedge x\mu_{col} \in \gamma\}$. Therefore, by our inductive hypothesis on (u_1, K'_s, K'_a) and (t, p'), we deduce that there exist a term v, $x \in fv(u_1) \setminus \text{dom}(\rho_\gamma)$ and $q \in \mathcal{P}os(x\sigma)$ such that
  - $(t, q) \in Fct_\gamma(x\sigma)$
  - $\mathcal{P}_{Fct}((t, p'), u_1\sigma\downarrow, v)$
  - $\mathcal{P}^m_{Fct}((t, q), x\sigma, v)$

  Since $fv(u_1) \subseteq fv(u)$ and $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$, we obtain that $x \in fv(u) \setminus \text{dom}(\rho_\gamma)$ and $\mathcal{P}_{Fct}((t, 1 \cdot p'), u\sigma\downarrow, v)$. Hence the result holds.
- Case $\mathsf{f} \in \{\langle\rangle, \mathsf{pk}, \mathsf{vk}, \mathsf{h}, \mathsf{tag}_i, \mathsf{tagk}_i\}$: In such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Moreover, by Definition 21, since $(t, p) \in eFct_\gamma(u\sigma\downarrow)$, we obtain that $Fct_\gamma(u\sigma\downarrow) = \bigcup_{j=1}^{n} \{(v, j \cdot q) \mid (v, q) \in Fct_\gamma(u_j\sigma\downarrow)\}$ and $\mathsf{f} = \mathsf{tagk}_i$ implies $u_1\sigma\downarrow \notin \text{dom}(\rho^\sigma_\gamma)$. Therefore, there exist $j \in \{1, \ldots, n\}$ and $p' \in \mathcal{P}os(u_j\sigma\downarrow)$ such that $p = j \cdot p'$ and $(t, p') \in Fct_\gamma(u_j\sigma\downarrow)$. Thanks to Lemma 8 and by Definition 5 and 16, we deduce that there exist K'_s, K'_a such that $(u_j, K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$. Moreover, $names(u_j) \subseteq names(u)$ thus $names(u_j) \subseteq \{n \in names(u) \mid (x, v) \in \text{PROTERM}(\Phi, \mathcal{S}) \wedge x\mu_{col} \in \gamma\}$. Thus, by our inductive hypothesis on (u_j, K'_s, K'_a) and (t, p'), we deduce that there exist a term v, $x \in fv(u_j) \setminus \text{dom}(\rho_\gamma)$ and $q \in \mathcal{P}os(x\sigma)$ such that
  - $(t, q) \in Fct_\gamma(x\sigma)$
  - $\mathcal{P}_{Fct}((t, p'), u_j\sigma\downarrow, v)$
  - $\mathcal{P}^m_{Fct}((t, q), x\sigma, v)$

  Since $fv(u_j) \subseteq fv(u)$ and $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$, we obtain that $x \in fv(u) \setminus \text{dom}(\rho_\gamma)$ and $\mathcal{P}_{Fct}((t, j \cdot p'), u\sigma\downarrow, v)$. Hence the result holds.
- Case $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$: We know that $u\sigma$ is a message. Therefore, we deduce that there exists $\mathsf{g} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$ and $v_1, \ldots, v_m$ such that $u_1\sigma\downarrow = \mathsf{g}(v_1, \ldots, v_m)$ and $u\sigma\downarrow = v_1$. Moreover, we also know from Definition 16 that $\mathsf{tagroot}_{\mathsf{Ks,Ka}}(u_1\sigma\downarrow) = i$. Hence $Fct_\gamma(u_1\sigma\downarrow) = \{(v, 1 \cdot q) \mid (v, q) \in Fct_\gamma(v_1)\}$. Since $(t, p) \in Fct_\gamma(u\sigma\downarrow)$, we deduce that $(t, 1 \cdot p) \in Fct_\gamma(u_1\sigma\downarrow)$. Thanks to Lemma 8 and by Definition 5 and 16, we deduce that there exist K'_s, K'_a such that $(u_1, K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$. Moreover, $names(u_1) \subseteq names(u)$ thus $names(u_1) \subseteq \{n \in names(u) \mid (x, v) \in \text{PROTERM}(\Phi, \mathcal{S}) \wedge x\mu_{col} \in \gamma\}$. Therefore, by our inductive hypothesis on (u_1, K'_s, K'_a) and $(t, 1 \cdot p)$, we deduce that there exist a term v, $x \in fv(u_1) \setminus \text{dom}(\rho_\gamma)$ and $q \in \mathcal{P}os(x\sigma)$ such that
  - $(t, q) \in Fct_\gamma(x\sigma)$
  - $\mathcal{P}_{Fct}((t, 1 \cdot p), u_1\sigma\downarrow, v)$
  - $\mathcal{P}^m_{Fct}((t, q), x\sigma, v)$

  Note that by Definition 21, $v = t$ or $\mathsf{root}(v) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$. Moreover, we know that $t \in st(v_1)$ and so it implies that $v \in st(v_1)$ meaning that $\mathcal{P}_{Fct}((t, p), v_1, v)$. Lastly, $fv(u_j) \subseteq fv(u)$ implies $x \in fv(u) \setminus \text{dom}(\rho_\gamma)$ and so the result holds.
- Case $\mathsf{f} = \mathsf{untag}$: Similar to the previous case.

– Case $\mathsf{f} \in \Sigma_i$: Since such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)\downarrow$. Hence, there exists $C[\_, \ldots, \_]$ and $v_1, \ldots, v_m$ such that $C[v_1, \ldots, v_m] = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$ and $v_1, \ldots, v_m$ are factors of $\mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Thanks to Lemma 1, we deduce that there exists D and $i_1, \ldots, i_k \in \{0, \ldots, m\}$ such that $u\sigma\downarrow = D[v_{i_1}, \ldots, v_{i_k}]$ and $v_0 = n_{min}$. Following Definition 21, we deduce that $Fct_\gamma(u\sigma\downarrow) = \bigcup_{j=1}^{k}\{(v, p_{i_j} \cdot q) \mid (v, q) \in Fct_\gamma(v_{i_j})\}$ where $p_{i_1}, \ldots, p_{i_m}$ are the positions of $v_{i_1}, \ldots, v_{i_k}$ in $u\sigma\downarrow$. Considering that $(t, p) \in Fct_\gamma(u\sigma\downarrow)$, there exist $j \in \{1, \ldots, k\}$ and $p' \in \mathcal{P}os(v_{i_j})$ such that $p = p_{i_j} \cdot p'$ and $(t, p') \in Fct_\gamma(v_{i_j})$. Moreover, since $v_0 = n_{min}$ then we deduce that $i_j \neq 0$ and so there exists $\ell \in \{1, \ldots, n\}$ such that either $u_\ell\sigma\downarrow = v_{i_j}$ or $v_{i_j} \in Fct(u_\ell\sigma\downarrow)$. In both cases, we obtain that if p'' is the position of v_{i_j} in $u_\ell\sigma\downarrow$ then $(t, p'' \cdot p') \in Fct_\gamma(u_\ell\sigma\downarrow)$. By applying our induct
We know that $(t, p) \in Fct_\gamma(u\sigma\downarrow)$. By Definition 21, it implies that $\mathsf{root}(t) \notin \Sigma_i$. Thanks to Lemma 8 and by Definition 5 and 16, we deduce that there exist K'_s, K'_a such that $(u_\ell, K'_s, K'_a) \in$ E-TERMS$_i(\mathcal{S})$. Moreover, $names(u_\ell) \subseteq names(u)$ thus $names(u_\ell) \subseteq \{n \in names(u) \mid (x, v) \in$ PROTERM$(\Phi, \mathcal{S}) \wedge x\mu_{col} \in \gamma\}$. Thus, by our inductive hypothesis on (u_ℓ, K'_s, K'_a) and $(t, p'' \cdot p')$, we deduce that there exist a term v, $x \in fv(u_\ell) \setminus \mathrm{dom}(\rho_\gamma)$ and $q \in \mathcal{P}os(x\sigma)$ such that
  - $(t, q) \in Fct_\gamma(x\sigma)$
  - $\mathcal{P}_{Fct}((t, p'' \cdot p'), u_\ell\sigma\downarrow, v)$
  - $\mathcal{P}^m_{Fct}((t, q), x\sigma, v)$

  Note that by Definition 21, $v = t$ or $\mathsf{root}(v) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$. Moreover, we know that $t \in st(v_{i_j})$ and so it implies that $v \in st(v_{i_j}) \subseteq st(u\sigma\downarrow)$ meaning that $\mathcal{P}_{Fct}((t, p), u\sigma\downarrow, v)$. Lastly, $fv(u_j) \subseteq fv(u)$ implies $x \in fv(u) \setminus \mathrm{dom}(\rho_\gamma)$ and so the result holds. □

Definition 23. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let t be a ground message in normal form. We define $AFct(t)$ as the smallest set such that:*

– $AFct(t) = Fct_\gamma(t) \cup \{(v, p \cdot q) \mid (u, p) \in Fct_\gamma(t) \wedge (v, q) \in AFct(u)\}$ *when* $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t) \in \gamma$ *and* $\gamma \in \{\alpha, \beta\}$
– $AFct(\mathsf{f}(t_1, \ldots, t_n)) = \bigcup_{i=1}^{n}\{(v, i \cdot p) \mid (v, p) \in AFct(t_i)\}$ *when* $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t) = 0$

Lemma 14. *Let $\mathcal{S}$ be a setup. Let $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in$ DFRAME$(\mathcal{S})$. For all $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, for all $\gamma \in \{\alpha, \beta\}$, for all $(t, p) \in Fct_\gamma(M\Phi\downarrow)$, there exist $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ and $n \in \mathbb{N}$ such that:*

– $q_M = 1 \cdot \ldots \cdot 1$, $|q_M| = n$ *and* $N|_{q_M} = M$ *and for all* $q < q_M$, $N|_q \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$
– *one of the following properties holds:*
  - $\mathcal{P}^m_{Fct}((t, p), M\Phi\downarrow, N\Phi\downarrow)$
  - *there exists* $q \in \mathcal{P}os(N\Phi\downarrow)$ *such that* $(t, q) \in AFct(N\Phi\downarrow)$ *and* $\forall u$, $\mathcal{P}^m_{Fct}((t, p), M\Phi\downarrow, u) \Leftrightarrow \mathcal{P}^m_{Fct}((t, q), N\Phi\downarrow, u)$.

Proof. Let $\omega \in \{\alpha, \beta\}$ such that $\omega \neq \gamma$. We prove this result by induction on $|M\Phi\downarrow|$.

Base case $|M\Phi\downarrow| = 1$: In such a case, $M\Phi\downarrow \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$. Hence, by Definition 21, $t = M\Phi\downarrow$ and $p = \varepsilon$. Moreover, $\mathcal{P}^m_{Fct}((t, p), M\Phi\downarrow, M\Phi\downarrow)$ meaning that the result holds with $N = M$.

Inductive step $|M\Phi\downarrow| > 1$: Otherwise, $M\Phi\downarrow = \mathsf{f}(u_1, \ldots, u_n)$. If $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M\Phi\downarrow) \in \gamma$ then by Definition 23, $Fct_\gamma(M\Phi\downarrow) \subseteq AFct(M\Phi\downarrow)$. Hence $(t, p) \in AFct(M\Phi\downarrow)$ and so the result directly holds with $N = M$. If $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M\Phi\downarrow) \in \omega$ or $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M\Phi\downarrow) = 0$ with $\mathsf{f} \notin \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$ then by Definition 21, $Fct_\gamma(M\Phi\downarrow) = \{(M\Phi\downarrow, \varepsilon)\}$ and so $t = M\Phi\downarrow$ and $p = \varepsilon$. Since $\mathcal{P}^m_{Fct}((t, p), M\Phi\downarrow, M\Phi\downarrow)$, the result directly holds with $N = M$. Else we obtain that $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$. By Definition 21, we deduce that $Fct_\gamma(M\Phi\downarrow) = \bigcup_{i=1}^{n}\{(v, i \cdot p) \mid (v, p) \in Fct_\gamma(u_i)\}$. Thus, there exists $i \in \{1, \ldots, n\}$ and $p' \in \mathcal{P}os(u_i)$ such that $p = i \cdot p'$ and $(t, p') \in Fct_\gamma(u_i)$. Let us do another case analysis on f:

If $\mathsf{f} = \langle\,\rangle$ then $n = 2$ and $\mathsf{proj}_i(M)\Phi\downarrow = u_i$. Note that if $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) = (x, |M|)$ for some x then $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(\mathsf{proj}_i(M)) = (x, |\mathsf{proj}_i(M)|)$. Hence by applying our inductive hypothesis on $\mathsf{proj}_i(M)$ and (t, p'), we deduce that there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that

– $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(x, |N|) = (x, |N|)$
– one of the following properties holds:
  - $\mathcal{P}^m_{Fct}((t, p'), \mathsf{proj}_i(M)\Phi\downarrow, N\Phi\downarrow)$

- there exists $q \in \mathcal{P}os(N\Phi\downarrow)$ such that $(t,q) \in AFct(N\Phi\downarrow)$ and $\forall u$, $\mathcal{P}^m_{Fct}((t,p'), \mathsf{proj}_i(M)\Phi\downarrow, u) \Leftrightarrow \mathcal{P}^m_{Fct}((t,q), N\Phi\downarrow, u)$.

Since $\mathsf{f} = \langle\,\rangle$ then by Definition 22, $\forall u$, $\mathcal{P}^m_{Fct}((t,p'), \mathsf{proj}_i(M)\Phi\downarrow, u) \Leftrightarrow \mathcal{P}^m_{Fct}((t,p), M\Phi\downarrow, u)$. This allows us to conclude that one of the following properties holds:

- $\mathcal{P}^m_{Fct}((t,p), M\Phi\downarrow, N\Phi\downarrow)$
- there exists $q \in \mathcal{P}os(N\Phi\downarrow)$ such that $(t,q) \in AFct(N\Phi\downarrow)$ and $\forall u$, $\mathcal{P}^m_{Fct}((t,p), M\Phi\downarrow, u) \Leftrightarrow \mathcal{P}^m_{Fct}((t,q), N\Phi\downarrow, u)$.

Hence the result holds.

If $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ then $n = 1$. Since $(t,p) \in Fct_\gamma(M\Phi\downarrow)$, we deduce that either (a) $\mathcal{P}^m_{Fct}((t,p), M\Phi\downarrow, M\Phi\downarrow)$ or (b) there exists q, q' such that $p = q \cdot q'$, $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M\Phi\downarrow|_\rangle) \in \gamma$. In case (a), the result holds with $M = N$. In case (b), let us take the pair (q,q') where $|q|$ is the smallest. In such that a case, $\mathcal{P}^m_{Fct}((M\Phi\downarrow|_q, q), M\Phi\downarrow, M\Phi\downarrow)$ and $(t,q') \in Fct_\gamma(M\Phi\downarrow|_q)$. But by Definition 23, we obtain that $(t,q') \in AFct(M\Phi\downarrow|_q)$. Thus a quick induction on $|q|$ allows us to prove that $(t,p) \in AFct(M\Phi\downarrow)$. Thus the result also holds with $M = N$. □

Lemma 15. *Let $\mathcal{S}$ be a setup. Let $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \text{DFrame}(\mathcal{S})$. Let $\gamma \in \{\alpha, \beta\}$. Let $(x,u) \in \text{ProTerm}(\Phi, \mathcal{S})$ such that $x\mu_{col} \in \gamma$. For all $(t,p) \in Fct_\gamma(u\sigma\downarrow)$, there exist $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, a term v and $q \in \mathcal{P}os(M\Phi\downarrow)$ such that:*

- $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x,1)$
- $\mathcal{P}_{Fct}((t,p), u\sigma\downarrow, v)$
- *either $(t,q) \in AFct(M\Phi\downarrow)$ and $\mathcal{P}^m_{Fct}((t,q), M\Phi\downarrow, v))$ or $M\Phi\downarrow = v$.*

Proof. By Definition 18, $(x,u) \in \text{ProTerm}(\Phi, \mathcal{S})$ implies that there exists K_s, K_a such that $(u, K_s, K_a) \in \text{E-terms}_{x\mu_{col}}(\mathcal{S})$ and $u\sigma$ is a message. Thus, by Lemma 13, there exist a term v, $x' \in fv(u) \setminus \text{dom}(\rho_\gamma)$ and $q \in \mathcal{P}os(x\sigma)$ such that

- $(t,q) \in Fct_\gamma(x'\sigma)$
- $\mathcal{P}_{Fct}((t,p), u\sigma\downarrow, v)$
- $\mathcal{P}^m_{Fct}((t,q), x'\sigma, v)$.

Once again by Definition 18, $x' \in fv(u) \setminus \text{dom}(\rho_\gamma)$ implies $x' \prec x$ and $x'\mu_{col} = x\mu_{col}$. Hence, we obtain that either there exists u' such that $(x',u') \in \text{ProTerm}(\Phi, \mathcal{S})$ or there exists $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x',1)$ and $M\Phi\downarrow = x'\sigma$.

In the latter case, we obtain that $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x,1)$ and $(t,q) \in Fct_\gamma(M\Phi\downarrow)$. Hence by Lemma 14, there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that:

- $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N) < (x',1) < (x,1)$
- one of the following properties holds:
  - $\mathcal{P}^m_{Fct}((t,q), M\Phi\downarrow, N\Phi\downarrow)$: In such a case, since $x'\sigma = M\Phi\downarrow$ and $\mathcal{P}^m_{Fct}((t,q), x'\sigma, v)$, we deduce that $N\Phi\downarrow = v$ and so the result holds.
  - there exists $q' \in \mathcal{P}os(N\Phi\downarrow)$ such that $(t,q') \in AFct(N\Phi\downarrow)$ and $\forall u$, $\mathcal{P}^m_{Fct}((t,q), M\Phi\downarrow, u) \Leftrightarrow \mathcal{P}^m_{Fct}((t,q'), N\Phi\downarrow, u)$: In such a case, we know that $\mathcal{P}^m_{Fct}((t,q), x'\sigma, v)$ meaning $\mathcal{P}^m_{Fct}((t,q), M\Phi\downarrow, v)$ and so $\mathcal{P}^m_{Fct}((t,q'), N\Phi\downarrow, v)$. To summarize, we have $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N) < (x,1)$, $\mathcal{P}^m_{Fct}((t,q'), N\Phi\downarrow, v)$ and $(t,q') \in AFct(N\Phi\downarrow)$. Hence the result holds.

In the former case ($(x',u') \in \text{ProTerm}(\Phi, \mathcal{S})$), by our inductive hypothesis on (x',u'), we obtain that there exists $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, a term v' and $q' \in \mathcal{P}os(M\Phi\downarrow)$ such that:

- $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x',1)$
- $\mathcal{P}_{Fct}((t,q), u'\sigma\downarrow, v')$
- either $(t,q') \in AFct(M\Phi\downarrow)$ and $\mathcal{P}^m_{Fct}((t,q'), M\Phi\downarrow, v'))$ or $M\Phi\downarrow = v'$.

Since $x' \prec x$ then $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x,1)$. Moreover, with $x'\sigma = u'\sigma\downarrow$, $\mathcal{P}^m_{Fct}((t,q), x'\sigma, v)$ and $\mathcal{P}_{Fct}((t,q), u'\sigma\downarrow, v')$, we deduce that $v' \in st(v)$. Since $\mathcal{P}_{Fct}((t,p), u\sigma\downarrow, v)$, we deduce that $\mathcal{P}_{Fct}((t,p), u\sigma\downarrow, v')$. Thus, the result holds with M, v' and q'. □

Lemma 16. *Let u be a ground message in normal form. For all $(t,p) \in AFct(u)$, for all $\gamma \in \{\alpha,\beta\}$, one of the following properties holds:*

- *there exist $(v,q) \in Fct_\gamma(u)$ and $p' \in \mathcal{P}os(v)$ such that $(t,p') \in AFct(v)$ and $p = q \cdot p'$.*
- *$(t,p) \in Fct_\gamma(u)$.*

Proof. Let us denote $\omega \in \{\alpha,\beta\}$ such that $\gamma \neq \omega$. We prove this lemma by induction on $|u|$.

Base case $|u| = 1$: In such a case, $AFct(u) = \emptyset$ and so the result trivially holds.

Inductive step $|u| > 1$: Otherwise, $u = \mathsf{f}(u_1,\ldots,u_n)$. We do a case analysis on u:

- Case $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) \in \gamma$: $AFct(u) = Fct_\gamma(u) \cup \{(r, q\cdot q') \mid (v,q) \in Fct_\gamma(u) \wedge (r,q') \in AFct(v)\}$. Therefore, either $(t,p) \in Fct_\gamma(u)$ or there exist $(v,q) \in Fct_\gamma(u)$ and q' such that $p = q \cdot q'$ and $(t,q') \in AFct(v)$. In both cases, the result holds.
- Case $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) \in \omega$: $Fct_\gamma(u) = \{(u,\varepsilon)\}$. Thus, by considering $(v,q) = (u,\varepsilon)$, we deduce that $(t,p) \in AFct(u)$ and $p = \varepsilon \cdot p$. Hence the result holds.
- Case $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = 0$ and $\mathsf{root}(u) \notin \{\mathsf{pk},\mathsf{vk},\mathsf{h},\langle\,\rangle\}$: In such a case, $Fct_\gamma(u) = \{(u,\varepsilon)\}$. Therefore, the result holds with $(v,q) = (u,\varepsilon)$ and $p' = p$.
- Case $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(u) = 0$ and $\mathsf{root}(u) \in \{\mathsf{pk},\mathsf{vk},\mathsf{h},\langle\,\rangle\}$: In such a case, $AFct(u) = \bigcup_{i=1}^n \{(v, i\cdot q) \mid (v,q) \in AFct(u_i)\}$ and $Fct_\gamma(u) = \bigcup_{i=1}^n \{(v, i\cdot q) \mid (u,q) \in Fct_\gamma(u_i)\}$. Hence there exist $i \in \{1,\ldots,n\}$ and $p' \in \mathcal{P}os(u_i)$ such that $(t,p') \in AFct(u_i)$ and $p = i \cdot p'$. Thus, by our inductive hypothesis on u_i, we obtain that either (a) $(t,p') \in Fct_\gamma(u_i)$ or (b) there exist $(v,q) \in Fct_\gamma(u_i)$ and $q' \in \mathcal{P}os(v)$ such that $(t,q') \in AFct(v)$ and $p' = q \cdot q'$. In case (a), $(t,p') \in Fct_\gamma(u_i)$ implies that $(t, i\cdot p') \in Fct_\gamma(u)$ and so $(t,p) \in Fct_\gamma(u)$. Thus the result holds. In case (b), $(v, i\cdot q) \in Fct_\gamma(u)$, $q' \in \mathcal{P}os(v)$, $(t,q') \in AFct(v)$ and $p = (i\cdot q)\cdot q'$. Therefore, the result holds. ◻

Lemma 17. *Let $\mathcal{S} = (\rho_\alpha,\rho_\beta,\mu_\alpha,\mu_\beta,\mathsf{H}_\alpha,\mathsf{H}_\beta,\sigma,\mathsf{Ks},\mathsf{Ka})$ be a setup. Let $(\mathcal{E},\Phi,\prec,\mu_{col}) \in \textsc{DFrame}(\mathcal{S})$. For all $M \in \mathsf{Recipe}(\mathcal{E},\Phi)$, for all $(t,p) \in AFct(M\Phi{\downarrow})$, there exist $N \in \mathsf{Recipe}(\mathcal{E},\Phi)$ and $q_N \in \mathcal{P}os(N)$ such that*

- *$\mathcal{M}_\prec^{\mathcal{E},\Phi}(N|_{q_N}) < \mathcal{M}_\prec^{\mathcal{E},\Phi}(M)$*
- *for all $q < q_N$, $N|_q \in \{\mathsf{proj}_1,\mathsf{proj}_2\}$*
- *$\mathcal{P}_{Fct}((t,p), M\Phi{\downarrow}, N\Phi{\downarrow})$*

Proof. We prove this result by induction on $\mathcal{M}_\prec^{\mathcal{E},\Phi}(M)$.

Base case $\mathcal{M}_\prec^{\mathcal{E},\Phi}(M) = (\mathsf{x}_0, 0)$: Trivial since no recipe has size 0.

Inductive step $\mathcal{M}_\prec^{\mathcal{E},\Phi}(M) > (\mathsf{x}_0,0)$: Assume first that $|M| = 1$. In such a case, $M \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$ or $M \in \mathrm{dom}(\Phi)$. If $M \notin \mathrm{dom}(\Phi)$ then $M\Phi{\downarrow} = M$ and $AFct(M\Phi{\downarrow}) = \emptyset$ which contradicts the fact that $(t,p) \in AFct(M\Phi{\downarrow})$. Therefore, $M \in \mathrm{dom}(\Phi)$. Let $\gamma \in \{\alpha,\beta\}$ such that $M\mu_{col} \in \gamma$. By Definition 18, we know that either Property 5a or 5b of the definition holds. If Property 5b holds then the result directly holds by application on our inductive hypothesis. Therefore, let us assume that Property 5a holds, meaning that there exists u such that $(M,u) \in \textsc{ProTerm}(\Phi,\mathcal{S})$. From Lemma 16, we deduce that one of the following properties hold:

1. $(t,p) \in Fct_\gamma(M\Phi{\downarrow})$.
2. there exist $(v,q) \in Fct_\gamma(M\Phi{\downarrow})$ and $p' \in \mathcal{P}os(v)$ such that $(t,p') \in AFct(v)$ and $p = q \cdot p'$

In Case (1), by Lemma 15, we deduce that there exists $N \in \mathsf{Recipe}(\mathcal{E},\Phi)$, a term v and $q \in \mathcal{P}os(N\Phi{\downarrow})$ such that $\mathcal{M}_\prec^{\mathcal{E},\Phi}(N) < \mathcal{M}_\prec^{\mathcal{E},\Phi}(M)$, $\mathcal{P}_{Fct}((t,p), M\Phi{\downarrow}, v)$ and either $(t,q) \in AFct(N\Phi{\downarrow})$ and $\mathcal{P}^m_{Fct}((t,q), N\Phi{\downarrow}, v)$ or $N\Phi{\downarrow} = v$.

In the latter case, the result directly holds. In the former case, we can apply our inductive hypothesis on N and (t,q) meaning that there exist $N' \in \mathsf{Recipe}(\mathcal{E},\Phi)$ and $q_{N'} \in \mathcal{P}os(N')$ such that:

- $\mathcal{M}_\prec^{\mathcal{E},\Phi}(N'|_{q_{N'}}) < \mathcal{M}_\prec^{\mathcal{E},\Phi}(N) < \mathcal{M}_\prec^{\mathcal{E},\Phi}(M)$; and

– for all $q' < q_{N'}$, $N'|_{q'} \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$; and
– $\mathcal{P}_{Fct}((t,q), N\Phi\downarrow, N'\Phi\downarrow)$.

Since $\mathcal{P}^m_{Fct}((t,q), N\Phi\downarrow, v), \mathcal{P}_{Fct}((t,q), N\Phi\downarrow, N'\Phi\downarrow)$ implies that $N'\Phi\downarrow \in st(v)$. But $\mathcal{P}_{Fct}((t,p), M\Phi\downarrow, v)$. Therefore, $\mathcal{P}_{Fct}((t,p), M\Phi\downarrow, N'\Phi\downarrow)$.

In Case (2), by Lemma 15, we deduce that there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, a term w and $r \in \mathcal{P}os(N\Phi\downarrow)$ such that $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$, $\mathcal{P}_{Fct}((v,q), M\Phi\downarrow, w)$ and either $(v,r) \in AFct(N\Phi\downarrow)$ and $\mathcal{P}^m_{Fct}((v,r), N\Phi\downarrow, w)$ or $N\Phi\downarrow = w$.

In the former case, by our inductive hypothesis on N and (v,r), we deduce that there exists $N' \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ and $q_{N'} \in \mathcal{P}os(N')$ such that

– $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N'|_{q_{N'}}) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$; and
– for all $q' < q_{N'}$, $N'|_{q'} \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$; and
– $\mathcal{P}_{Fct}((v,r), N\Phi\downarrow, N'\Phi\downarrow)$.

Let us denote $r = r'' \cdot r'$ such that $N\Phi\downarrow|_{r''} = N'\Phi\downarrow$. By Definition 23, $(t,p') \in AFct(v)$, $p = q \cdot p'$ and $(v,q) \in Fct_\gamma(M\Phi\downarrow)$ implies that $(t, r' \cdot p') \in AFct(N'\Phi\downarrow)$. Note that since for all $q' < q_{N'}$, $N'|_{q'} \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$, there exists q'' such that $(t, q''\cdot r'\cdot p') \in AFct(N'|_{q_{N'}}\Phi\downarrow)$. But $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N'|_{q_{N'}}) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$ hence by our inductive hypothesis, we deduce that there exists $N'' \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ and $q_{N''}$ such that:

– $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N''|_{q''}) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N'|_{q_{N'}})$
– for all $q < q_{N''}$, $N''|_q \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$
– $\mathcal{P}_{Fct}((t, q'' \cdot r' \cdot p'), N'|_{q_{N'}}\Phi\downarrow, N''\Phi\downarrow)$

Note that $\mathcal{P}_{Fct}((t, q'' \cdot r' \cdot p'), N'|_{q_{N'}}\Phi\downarrow, N''\Phi\downarrow)$ implies $\mathsf{root}(N''\Phi\downarrow) \neq \langle\,\rangle$. Thus we obtain that $\mathcal{P}_{Fct}((t, r' \cdot p'), N'\Phi\downarrow, N''\Phi\downarrow)$. Hence $N''\Phi\downarrow \in st(N'\Phi\downarrow)$. Moreover, $\mathcal{P}_{Fct}((v,r), N\Phi\downarrow, N'\Phi\downarrow)$ and $\mathcal{P}^m_{Fct}((v,r), N\Phi\downarrow, w)$ implies that $N'\Phi\downarrow \in st(w)$. Lastly, $\mathcal{P}_{Fct}((v,q), M\Phi\downarrow, w)$ implies $w \in st(M\Phi\downarrow)$. Therefore, we deduce that $N''\Phi\downarrow \in st(M\Phi\downarrow)$ and so $\mathcal{P}_{Fct}((t,p), M\Phi\downarrow, N''\Phi\downarrow)$.

In the latter case, we have $\mathcal{P}_{Fct}((v,q), M\Phi\downarrow, N\Phi\downarrow)$. But by Definition 23, if we denote $q = r'' \cdot r'$ such that $M\Phi\downarrow|_{r''} = N\Phi\downarrow$ then $(t,p') \in AFct(v)$ implies that $(t, r' \cdot p') \in AFct(N\Phi\downarrow)$. By our inductive hypothesis, we deduce that there exist $N' \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ and $q_{N'}$ such that

– $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N'|_{q_{N'}}) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$; and
– for all $q' < q_{N'}$, $\mathsf{root}(N'|_{q'}) \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$; and
– $\mathcal{P}_{Fct}((t, r' \cdot p'), N\Phi\downarrow, N'\Phi\downarrow)$.

Since $\mathcal{P}_{Fct}((v,q), M\Phi\downarrow, N\Phi\downarrow)$, $q = r'' \cdot r'$ and $p = q \cdot p'$, we obtain that $\mathcal{P}_{Fct}((t,p), M\Phi\downarrow, N'\Phi\downarrow)$ which allows us to conclude.

Assume now that $|M| > 1$ and so $M = \mathsf{f}(M_1, \ldots, M_n)$. We do a case analysis on f.

– Case $\mathsf{f} \in \Sigma_0 \setminus \{\mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$ when $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M\Phi\downarrow) = 0$. In such a case, $M\Phi\downarrow = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_n\Phi\downarrow)$. Moreover, by Definition 23, we know that there exist $i \in \{1, \ldots, n\}$ and $p' \in \mathcal{P}os(M_i\Phi\downarrow)$ such that $(t,p') \in AFct(M_i\Phi\downarrow)$. By applying our inductive hypothesis on M_i and (t,p'), we conclude.
– Case $\mathsf{f} \in \Sigma_0 \setminus \{\mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$ when $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M\Phi\downarrow) \in \gamma$ with $\gamma \in \{\alpha, \beta\}$. In such a case, $M\Phi\downarrow = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_n\Phi\downarrow)$. By Definitions 23 and 21, we deduce that either $(t,p') \in Fct_\gamma(M_1\Phi\downarrow)$ and $p = 1 \cdot p'$ or there exist $(v,q) \in Fct_\gamma(M_1\Phi\downarrow)$ and q' such that $p = 1 \cdot q \cdot q'$ and $(t,q') \in AFct(v)$. In the former case, by Lemma 14, we obtain that there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ and q_N such that $N|_{q_N} = M_1$, for all $q < q_N$, $\mathsf{root}(N|_q) \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$ and one of the following properties holds:
  - $\mathcal{P}^m_{Fct}((t,p'), M_1\Phi\downarrow, N\Phi\downarrow)$: Note that since $\mathsf{root}(M\Phi\downarrow) \notin \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$, $\mathcal{P}^m_{Fct}((t,p'), M_1\Phi\downarrow, N\Phi\downarrow)$ implies $\mathcal{P}^m_{Fct}((t,p), M\Phi\downarrow, N\Phi\downarrow)$. Thus the result directly holds since $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M_1) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$
  - there exists $q \in \mathcal{P}os(N\Phi\downarrow)$ such that $(t,q) \in AFct(N\Phi\downarrow)$ and for all u, $\mathcal{P}^m_{Fct}((t,p'), M_1\Phi\downarrow, u) \Leftrightarrow \mathcal{P}^m_{Fct}((t,q), N\Phi\downarrow, u)$: Note that $(t,q) \in AFct(N\Phi\downarrow)$ implies $(t,p') \in AFct(M_1\Phi\downarrow)$. By applying our inductive hypothesis on (t,p') and M_1, there exist N' and $q_{N'}$ such that

* $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(N'|_{q_{N'}}) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M_1) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M)$; and
* for all $q' < q_{N'}$, $\mathsf{root}(N'|_{q'}) \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$; and
* $\mathcal{P}_{Fct}((t,p'), M_1\Phi\downarrow, N'\Phi\downarrow)$ which implies $\mathcal{P}_{Fct}((t,p), M\Phi\downarrow, N'\Phi\downarrow)$

In the latter case, $(v,q) \in Fct_\gamma(M_1\Phi\downarrow)$ and $(t,q') \in AFct(v)$ implies that $(t, q{\cdot}q') \in AFct(M_1\Phi\downarrow)$. We conclude by applying our inductive hypothesis on $(t, q \cdot q')$ and $M_1\Phi\downarrow$.

– Case $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$: We know that $M\Phi$ is a message. Hence, there exists $\mathsf{g} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$ and $u_1, \ldots, u_n$ such that $M_1\Phi\downarrow = \mathsf{g}(u_1, \ldots, u_n)$ and $M\Phi\downarrow = u_1$. Note that if $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M_1\Phi\downarrow)$ then we directly have by definition that $(t, 1 \cdot p) \in AFct(M_1\Phi\downarrow)$ and so we conclude by applying our inductive hypothesis. If $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M_1\Phi\downarrow) \in \gamma$ with $\gamma \in \{\alpha, \beta\}$ then from Lemma 16 we also obtain that $(t, 1 \cdot p) \in AFct(M_1\Phi\downarrow)$ which allows us to conclude.

– Case $\mathsf{f} \in \Sigma_i$, $i \in \gamma$, $\gamma \in \{\alpha, \beta\}$: In such a case $M\Phi\downarrow = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_n\Phi\downarrow)\downarrow = u\downarrow$. □

E.2 Potential deducible terms

Definition 24. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let t be a ground message in normal form. We define $DFct(t)$ the smallest set such that:*

– $DFct(\mathsf{f}(u_1, \ldots, u_n)) = \{\mathsf{f}(u_1, \ldots, u_n)\} \cup \bigcup_{i=1} DFct(u_i)$ *when* $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\} \cup \{\mathsf{tag}_i, \mathsf{tagk}_i \mid i \in \{\alpha, \beta\}\}$ *and* $t \neq \mathsf{tagk}_i(t')$ *for some* $i \in \gamma$, $\gamma \in \{\alpha, \beta\}$ *and* $t' \in \mathrm{dom}(\rho_\gamma^\sigma)$
– $DFct(\mathsf{f}(u_1, \ldots, u_n)) = \{\mathsf{f}(u_1, \ldots, u_n)\} \cup DFct(u_1)$ *when* $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$
– $DFct(\mathsf{f}(u_1, \ldots, u_n)) = \bigcup_{i=1}^{n} DFct(u_i)$ *when* $\mathsf{f} \in \Sigma_\alpha \cup \Sigma_\beta$

Lemma 18. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $\gamma \in \{\alpha, \beta\}$. Let $i \in \gamma$. For all $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$, for all $t \in DFct(u\sigma\downarrow)$, if $u\sigma$ is a message then*

– *either there exists $(v, K_s', K_a') \in \text{E-TERMS}_i(\mathcal{S})$ such that $v \in st(u)$, $\mathsf{root}(v) = \mathsf{root}(t)$ and $v\sigma\downarrow = t$.*
– *or there exists $x \in fv(u) \setminus \mathrm{dom}(\rho_\gamma)$ such that $t \in DFct(x\sigma)$.*

Proof. We prove the result by induction on $|u|$.

Base case $|u| = 1$: In such a case, $u \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$ or $u \in \mathcal{X} \setminus \mathrm{dom}(\rho_\gamma)$ (by Property 1 of Definition 16). By Definition 24, $t \in DFct(u\sigma\downarrow)$ implies that $u \notin \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$. Therefore, $u \in \mathcal{X} \setminus \mathrm{dom}(\rho_\gamma)$. Hence, we directly obtain the result.

Inductive step $|u| > 1$: Otherwise by Definition 16, we know that $(u, K_s, K_a) \in \text{TAGT}(i)$. Hence we do a case analysis on the Definition 5:

Case 2,3,5 of Definition 5 when $u = \mathsf{f}(u_1, \ldots, u_n)$ and $\mathsf{f} \in \{\mathsf{sign}, \mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}\}$: In such a case, we know that $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Moreover, by Definition 24, we also know that either $t = u\sigma\downarrow$ or $t \in DFct(u_1\sigma\downarrow)$. In the former case, the result directly holds. Note that by Lemma 8 and since $u_1 \notin \mathrm{dom}(\rho_\gamma)$, we deduce that there exists K_s', K_a' such that $(u_1, K_s', K_a') \in \text{E-TERMS}_i(\mathcal{S})$ and $t \in DFct(u_1\sigma\downarrow)$. We conclude by applying our inductive hypothesis on (u_1, K_s', K_a').

Case 2,3,4 of Definition 5 when $u = \mathsf{f}(u_1, \ldots, u_n)$ and $\mathsf{f} \in \{\mathsf{check}, \mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}\}$: In such a case, we know that $u\sigma$ is a message, meaning that there exist $\mathsf{g} \in \{\mathsf{sign}, \mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}\}$ and $v_1, \ldots, v_m$ such that $u_1\sigma\downarrow = \mathsf{g}(v_1, \ldots, v_m)$ and $u\sigma\downarrow = v_1$. Therefore, by Definition 24, we know that $DFct(u\sigma\downarrow) \subseteq DFct(u_1\sigma\downarrow)$. Note that by Lemma 8 and since $u_1 \notin \mathrm{dom}(\rho_\gamma)$, we deduce that there exists K_s', K_a' such that $(u_1, K_s', K_a') \in \text{E-TERMS}_i(\mathcal{S})$. We conclude by applying our inductive hypothesis on (u_1, K_s', K_a').

Case 6,7 of Definition 5: Similar to the two previous cases.

Case 8 of Definition 5 when $u = \mathsf{f}(u_1, \ldots, u_n)$ and $\mathsf{f} \in \Sigma_\gamma$: In such a case $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Note that $t \in DFct(u\sigma\downarrow)$ implies $\mathsf{root}(t) \notin \Sigma_\gamma$. Thus, by Lemma 1 and by Definition 24, we deduce that there exists $j \in \{1, \ldots, n\}$ such that $t \in DFct(u_j\sigma\downarrow)$. Therefore, by Definition 24, we know that $DFct(u\sigma\downarrow) \subseteq DFct(u_j\sigma\downarrow)$. Note that by Lemma 8 and since $u_j \notin \mathrm{dom}(\rho_\gamma)$, we deduce that

there exists K'_s, K'_a such that $(u_j, K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$. We conclude by applying our inductive hypothesis on (u_j, K'_s, K'_a).

Case 8 of Definition 5 when $u = \mathsf{f}(u_1, \ldots, u_n)$ *and* $\mathsf{f} \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$*:* Similar to case 2,3,4 when $\mathsf{f} \in \{\mathsf{check}, \mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}\}$.

Case 8 of Definition 5 when $u = \mathsf{f}(u_1, \ldots, u_n)$ *and* $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle, \mathsf{tag}_i, \mathsf{tagk}_i\}$*:* In such a case, we know that $u\sigma\!\downarrow = \mathsf{f}(u_1\sigma\!\downarrow, \ldots, u_n\sigma\!\downarrow)$. Moreover, if $\mathsf{f} = \mathsf{tagk}_i$ then $n = 1$. In such a case, if $u_i \in \text{dom}(\rho_\gamma)$ then by Definition 24, we obtain that $DFct(u\sigma\!\downarrow) = \emptyset$ which contradicts our hypothesis $t \in DFct(u\sigma\!\downarrow)$. As such, we deduce that for all $j \in \{1, \ldots, n\}$, $u_j \notin \text{dom}(\rho_\gamma)$ and so by Lemma 8, we deduce that there exists K^j_s, K^j_a such that $(u_j, K^j_s, K^j_a) \in \text{E-TERMS}_i(\mathcal{S})$. From Definition 24, either $t = u\sigma\!\downarrow$ or there exists $j \in \{1, \ldots, n\}$ such that $t \in DFct(u_j\sigma\!\downarrow)$. In the former case, the result directly holds, otherwise we can apply our inductive hypothesis on (u_j, K^j_s, K^j_a) which allows us to conclude. □

Lemma 19. *Let* $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ *be a setup. Let* $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \text{DFRAME}(\mathcal{S})$*. For all* $(x, u) \in \text{PROTERM}(\Phi, \mathcal{S})$*, for all* $t \in DFct(u\sigma\!\downarrow)$*,*

- *either there exist* $(x', u') \in \text{PROTERM}(\Phi, \mathcal{S})$ *and* $(v, K_s, K_a) \in \text{E-TERMS}_{x'\mu_{col}}(\mathcal{S})$ *such that* $\neg(x \prec x')$*,* $x\mu_{col} = x'\mu_{col}$*,* $v \in st(u')$*,* $\mathsf{root}(v) = \mathsf{root}(t)$ *and* $v\sigma\!\downarrow = t$*.*
- *there exists* $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ *such that* $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x, 1)$ *and* $t \in DFct(M\Phi\!\downarrow)$

Proof. We prove this result by induction on x with respect to the order $\prec$.

Base case $x = \mathsf{x}_0$*:* Such a case is impossible since we assumed that $\mathsf{x}_0 \notin \text{dom}(\Phi) \cup \text{dom}(\sigma)$.

Inductive step $\mathsf{x}_0 \prec x$*:* In such a case, $(x, u) \in \text{PROTERM}(\Phi, \mathcal{S})$ implies that there exist $\gamma \in \{\alpha, \beta\}$, $i \in \gamma$ and K_s, K_a such that $i = x\mu_{col}$, $(u, K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$, $u\sigma$ is a message and $x\Phi\sigma = u\sigma\!\downarrow$. By Lemma 18, we deduce that:

- either there exists $(v, K'_s, K'_a) \in \text{E-TERMS}_i(\mathcal{S})$ such that $v \in st(u)$, $\mathsf{root}(v) = \mathsf{root}(t)$ and $v\sigma\!\downarrow = t$: In such a case, the result directly holds.
- or there exists $y \in fv(u) \setminus \text{dom}(\rho_\gamma)$ such that $t \in DFct(y\sigma)$. By Definition 18, we know that either Property 5a or Property 5b holds on y. If Property 5b of Definition 18 holds on y then the result directly holds too. Otherwise, Property 5a of Definition 18 holds on y and so there exists u' such that $y\mu_{col} = i$, $(y, u') \in \text{PROTERM}(\Phi, \mathcal{S})$ and $t \in DFct(u'\sigma\!\downarrow)$. We conclude by applying ur inductive hypothesis on (y, u'). □

Lemma 20. *Let* $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ *be a setup. Let* $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \text{DFRAME}(\mathcal{S})$*. For all* $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$*, for all* $\mathsf{f}(t_1, \ldots, t_n) \in DFct(M\Phi\!\downarrow)$*,*

- *either there exist* $(x, u) \in \text{PROTERM}(\Phi, \mathcal{S})$ *and* $(v, K_s, K_a) \in \text{E-TERMS}_{x\mu_{col}}(\mathcal{S})$ *such that* $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) \geq (x, 1)$*,* $v \in st(u)$*,* $\mathsf{root}(v) = \mathsf{f}$ *and* $v\sigma\!\downarrow = \mathsf{f}(t_1, \ldots, t_n)$*.*
- *there exists* $M_1, \ldots, M_n \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ *such that for all* $i \in \{1, \ldots, n\}$*,* $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M_i) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$ *and* $M_i\Phi\!\downarrow = t_i$*.*

Proof. We prove this result by induction on $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$.

Base case $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) = (\mathsf{x}_0, 0)$*:* Such a case is impossible since no recipes has size 0.

Inductive step $\mathcal{M}^{Ec,\Phi}_{\prec}(M) > (\mathsf{x}_0, 0)$*:* Assume first that $|M| = 1$. In such a case, $\mathsf{f}(t_1, \ldots, t_n) \in DFct(M\Phi\!\downarrow)$ and Definition 24 allows us to deduce that $M \in \text{dom}(\Phi)$. Hence from Definition 18, we know that either Property 5b of Definition 18 holds on M or Property 5a. If it is the former then there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $\mathcal{M}^{Ec,\Phi}_{\prec}(N) < \mathcal{M}^{Ec,\Phi}_{\prec}(M)$ and $N\Phi\!\downarrow = M\Phi\!\downarrow$. Thus, we conclude by applying our inductive hypothesis on N. If it is the latter, then there exists u such that $(M, u) \in \text{PROTERM}(\Phi, \mathcal{S})$ and $\mathsf{f}(t_1, \ldots, t_n) \in DFct(u\sigma\!\downarrow)$. By Lemma 19, we know that

- either there exist $(x', u') \in \text{PROTERM}(\Phi, \mathcal{S})$ and $(v, K_s, K_a) \in \text{E-TERMS}_{x'\mu_{col}}(\mathcal{S})$ such that $\neg(M \prec x')$*,* $M\mu_{col} = x'\mu_{col}$*,* $v \in st(u')$*,* $\mathsf{root}(v) = \mathsf{f}$ and $v\sigma\!\downarrow = \mathsf{f}(t_1, \ldots, t_n)$*.*

– there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(N) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M)$ and $\mathsf{f}(t_1, \ldots, t_n) \in DFct(N\Phi\downarrow)$

In the latter case, we conclude by applying our inductive hypothesis on N. In the former case, the result directly holds since $\neg(M \prec x')$ implies $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M) \geq (x', 1)$.

Assume now that $|M| > 1$. Therefore, assume that $M = \mathsf{g}(M_1, \ldots, M_m)$. We do a case analysis on g.

– Case $\mathsf{g} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\} \cup \{\mathsf{tag}_i, \mathsf{tagk}_i \mid i \in \{\alpha, \beta\}\}$: In such a case, $M\Phi\downarrow = \mathsf{g}(M_1\Phi\downarrow, \ldots, M_m\Phi\downarrow)$. Moreover, $\mathsf{f}(t_1, \ldots, t_n) \in DFct(M\Phi\downarrow)$ implies that $M\Phi\downarrow \neq \mathsf{tagk}_i(t)$ for some $i \in \gamma$, $\gamma \in \{\alpha, \beta\}$ and $t \in \mathrm{dom}(\rho_\gamma^\sigma)$. Note that by Definition 24, we also have that either $\mathsf{f}(t_1, \ldots, t_n) = M\Phi\downarrow$ or there exists $i \in \{1, \ldots, m\}$ such that $\mathsf{f}(t_1, \ldots, t_n) \in DFct(M_i\Phi\downarrow)$. In the former case, we have in fact $\mathsf{f} = \mathsf{g}$, $n = m$ and for all $i \in \{1, \ldots, n\}$, $M_i\Phi\downarrow = t_i$ and $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M_i) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M)$. Therefore, the result holds. In the latter case, we conclude by applying our inductive hypothesis on M_i.
– Case $\mathsf{g} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$: Similar to the previous case. Indeed, $M\Phi\downarrow = \mathsf{g}(M_1\Phi\downarrow, \ldots, M_m\Phi\downarrow)$. Moreover, by Definition 24, we also have that either $\mathsf{f}(t_1, \ldots, t_n) = M\Phi\downarrow$ or $\mathsf{f}(t_1, \ldots, t_n) \in DFct(M_1\Phi\downarrow)$. In the former case, the result holds and in the latter case, we conclude by applying our inductive hypothesis.
– Case $\mathsf{g} \in \{\mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$: Since $M\Phi$ is a message, we deduce that there exists $\mathsf{g}' \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{raenc}, \mathsf{sign}\}$ and $v_1, \ldots, v_k$ such that $M_1\Phi\downarrow = \mathsf{g}'(v_1, \ldots, v_k)$ and $v_1 = M\Phi\downarrow$. By Definition 24, we obtain that $DFct(M\Phi\downarrow) \subseteq DFct(M_1\phi\downarrow)$ meaning that we conclude by applying our inductive hypothesis on M_1.
– Case $\mathsf{g} \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$: Similar to previous case.
– Case $\mathsf{g} \in \Sigma_i$, $i \in \gamma$, $\gamma \in \{\alpha, \beta\}$: In such a case, $M\Phi\downarrow = \mathsf{g}(M_1\Phi\downarrow, \ldots, M_m\Phi\downarrow)\downarrow$. From Definition 24, we know that $\mathsf{f} \notin \Sigma_i$. Thus by Lemma 1, we deduce that there exists $i \in \{1, \ldots, m\}$ such that $\mathsf{f}(t_1, \ldots, t_n) \in DFct(M_i\Phi\downarrow)$. We conclude by applying our inductive hypothesis on M_i. □

E.3 Link between the frames Φ and $\mathbf{tr}(\Phi)$

Lemma 21. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup. Let $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \mathrm{DFRAME}(\mathcal{S})$. For all $\gamma, \omega \in \{\alpha, \beta\}.\gamma \neq \omega$, for all $i \in \omega$, for all terms t, for all $(x, u) \in \mathrm{PROTERM}(\Phi, \mathcal{S})$, for all $(u', K_s, K_a) \in \text{E-TERMS}_i(\mathcal{S})$, for all context C built on $\{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$, for all terms $t_1, \ldots, t_n$, if the following properties hold:*

– $t = C[t_1, \ldots, t_n] = u'\sigma\downarrow$
– $x\mu_{col} = i$
– $u' \in st(u)$
– $\mathsf{root}(u') = \mathsf{root}(t)$
– *for all $p \in \mathcal{P}os(C)$, $C|_p \neq \_$ implies $\mathcal{P}_{\prec}^{\nu\mathcal{E}.\Phi}(t|_p, x)$*
– *for all $j \in \{1, \ldots, n\}$, $\neg\mathcal{P}_{\prec}^{\nu\mathcal{E}.\Phi}(t_j, x)$ or $\mathsf{root}(t_j) \notin \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\rangle\}$*

then the following properties hold:

– *for all $j \in \{1, \ldots, n\}$, $\mathcal{P}_{\prec}^{\nu\mathcal{E}.\Phi}(t_j, x)$ implies that either $t_j \in \mathcal{N}_\omega^{\Phi,\mathcal{S}}$ or $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t_j) \in \omega$*
– *for all $p \in \mathcal{P}os(C)$, $\mathsf{root}(C|_p) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ implies $t|_p \in \mathsf{H}_\gamma$*

Proof. Let us first show that for all $j \in \{1, \ldots, n\}$, $\mathcal{P}_{\prec}^{\nu\mathcal{E}.\Phi}(t_j, x)$ implies that either $t_j \in \mathcal{N}_\omega^{\Phi,\mathcal{S}}$ or $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t_j) \in \omega$. Let us assume that $t_j \notin \mathcal{N}_\omega^{\Phi,\mathcal{S}}$ and $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t_j) \notin \omega$. As such, assume that $p_j \in \mathcal{P}os(C)$ such that $t|_{p_j} = t_j$. In such a case, if $t_j \in \mathcal{N}$ then $t_j \in \mathcal{N} \setminus \mathcal{N}_\omega^{\Phi,\mathcal{S}}$ and so $(t_j, p_j) \in Fct_\omega(t)$. If $t_j \notin \mathcal{N}$ then $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t_j) \notin \omega$ implies that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t_j) \in \gamma \cup \{0\}$. Note that since $\mathcal{P}_{\prec}^{\nu\mathcal{E}.\Phi}(t_j, x)$ then $\mathsf{root}(t_j) \notin \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\rangle\}$. Thus $(t_j, p_j) \in Fct_\omega(t)$.

Therefore, we obtained that for all $j \in \{1, \ldots, n\}$, $\mathcal{P}_{\prec}^{\nu\mathcal{E}.\Phi}(t_j, x)$ implies $(t_j, p_j) \in Fct_\omega(t)$. Moreover, by Lemma 13, we deduce that there exists a term v, $y \in fv(u') \setminus \mathrm{dom}(\rho_\omega)$ and $q \in \mathcal{P}os(y\sigma)$ such that:

– $(t_j, q) \in Fct_\omega(y\sigma)$
– $\mathcal{P}_{Fct}((t_j, p_j), u'\sigma\downarrow, v)$
– $\mathcal{P}^m_{Fct}((t_j, q), y\sigma, v)$

Note that $\mathcal{P}_{Fct}((t_j, p_j), u'\sigma\downarrow, v)$ implies there exists $p' \in \mathcal{P}os(C)$ such that $p' \leq p_j$ and $t|_{p'} = v$. Therefore, we obtain that $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(v, x)$. By Definition 18 and by Lemma 15, we obtain that there exists $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, a term v' and $q' \in \mathcal{P}os(M\Phi\downarrow)$ such that:

– $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x, 1)$
– $\mathcal{P}_{Fct}((t_j, q), y\sigma, v')$
– $\mathcal{P}^m_{Fct}((t_j, q'), M\Phi\downarrow, v')$
– $(t_j, q') \in AFct(M\Phi\downarrow)$

Note that $\mathcal{P}_{Fct}((t_j, q), y\sigma, v')$ and $\mathcal{P}^m_{Fct}((t_j, q), y\sigma, v)$ implies that once again that there exists $p' \in \mathcal{P}os(C)$ such that $p' \leq p_j$, $t|_{p'} = v'$ and so $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(v', x)$. By Lemma 17, $(t_j, q') \in AFct(M\Phi\downarrow)$ implies that there exist $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ and $q_N \in \mathcal{P}os(N)$ such that:

– $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N|_{q_N}) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$
– for all $q < q_N$, $N|_q \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$
– $\mathcal{P}_{Fct}((t_j, q'), M\Phi\downarrow, N\Phi\downarrow)$

Once again since $\mathcal{P}^m_{Fct}((t_j, q'), M\Phi\downarrow, v')$, $\mathcal{P}_{Fct}((t_j, q'), M\Phi\downarrow, N\Phi\downarrow)$ and there exists $p' \in \mathcal{P}os(C)$ such that $p' \leq p_j$, $t|_{p'} = v'$ then we obtain that there exists $p'' \in \mathcal{P}os(C)$ such that $p'' \leq p_j$, $t|_{p''} = N\Phi\downarrow$. But we know that $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N|_{q_N}) < \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$, for all $q < q_N$, $N|_q \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$ and $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x, 1)$. Therefore, $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N) < (x, 1)$ which is a contradiction with the fact that for all $p \in \mathcal{P}os(C)$, $C|_p \neq \_$ implies $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(t|_p, x)$. We thus conclude that either $t_j \in \mathcal{N}^{\Phi,\mathcal{S}}_\omega$ or $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t_j) \in \omega$.

Let us now prove that $p \in \mathcal{P}os(C)$, $\mathsf{root}(C|_p) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ implies $t|_p \in \mathsf{H}_\omega$. Let $p \in \mathcal{P}os(C)$ such that $\mathsf{root}(C|_p) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$. In such a case, we deduce that $t|_p \in DFct(u'\sigma\downarrow)$. By relying on Lemma 18, 19 and Definition 18, we obtain that one of the following properties holds:

– there exists $(y, v) \in \textsc{ProTerm}(\Phi, \mathcal{S})$ and $(v', K'_s, K'_a) \in \text{E-}\textsc{terms}_i(\mathcal{S})$ such that $\neg(x \prec y)$, $y\mu_{col} = i$, $v' \in st(v)$, $\mathsf{root}(v') = \mathsf{root}(t|_p)$ and $v'\sigma\downarrow = t|_p$.
– there exists $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x, 1)$ and $t|_p \in DFct(M\Phi\downarrow)$.

In the first case, since we know that $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(t|_p, x)$ holds and since $\neg(x \prec y)$, we directly have that $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(t|_p, y)$. Moreover, $i \in \omega$ and so we deduce from Definition 18 that $t|_p \in \mathsf{H}_\gamma$.

In the second case, since $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(t|_p, x)$ and $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x, 1)$, we can apply Lemma 20 and obtain that there exists $(y, v) \in \textsc{ProTerm}(\Phi, \mathcal{S})$ and $(v', K'_s, K'_a) \in \text{E-}\textsc{terms}_{y\mu_{col}}(\mathcal{S})$ such that $(y, 1) \leq \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$, $v' \in st(v)$, $\mathsf{root}(v') = \mathsf{root}(t|_p)$ and $v'\sigma\downarrow = t|_p$. If $y\mu_{col} \in \omega$ then we obtain as previously that $t|_p \in \mathsf{H}_\gamma$. Hence, it remains the case where $y\mu_{col} \in \gamma$. Note that $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(t|_p, x)$ implies that there exists $j \in \{1, \ldots, n\}$ and $p_j \in \mathcal{P}os(C)$ such that $p \leq p_j$ and $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(t_j, x)$. But we proved that either $t_j \in \mathcal{N}^{\Phi,\mathcal{S}}_\omega$ or $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(t_j) \in \omega$.

As such, if we denote p'_j such that $p_j = p \cdot p'_j$ then we obtain that $(t_j, p'_j) \in Fct_\gamma(v'\sigma\downarrow)$. By Lemma 13, we deduce that there exists a term w, $z \in fv(v') \setminus \mathrm{dom}(\rho_\gamma)$ and $q \in \mathcal{P}os(z\sigma)$ such that:

– $(t_j, q) \in Fct_\gamma(z\sigma)$
– $\mathcal{P}_{Fct}((t_j, p'_j), v'\sigma\downarrow, w)$
– $\mathcal{P}^m_{Fct}((t_j, q), z\sigma, w)$

Note that $\mathcal{P}_{Fct}((t_j, p'_j), v'\sigma\downarrow, w)$ implies there exists $p' \in \mathcal{P}os(C)$ such that $p < p' \leq p \cdot p'_j$ and $t|_{p'} = w$. Therefore, we obtain that $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(w, x)$. By Definition 18 and by Lemma 15, we obtain that there exists $M' \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, a term w' and $q' \in \mathcal{P}os(M\Phi\downarrow)$ such that:

– $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M') < (y, 1) \leq \mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) < (x, 1)$
– $\mathcal{P}_{Fct}((t_j, q), z\sigma, w')$

– $\mathcal{P}^m_{Fct}((t_j, q'), M'\Phi\downarrow, w')$
– $(t_j, q') \in AFct(M'\Phi\downarrow)$

Once again, we deduce that there exists $p' \in \mathcal{P}os(C)$ such that $t|_{p'} = w'$ and so $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(w', x)$. Lastly, by applying Lemma 17 on (t_j, q') and M', we deduce that existence of $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(N) < (x, 1)$ and $\mathcal{P}_{Fct}((t_j, q'), M'\Phi\downarrow, N\Phi\downarrow)$. But $\mathcal{P}_{Fct}((t_j, q'), M'\Phi\downarrow, N\Phi\downarrow)$ and $\mathcal{P}^m_{Fct}((t_j, q'), M'\Phi\downarrow, w')$ implies that there exists $p'' \in \mathcal{P}os(C)$ such that $t|_{p'} = N\Phi\downarrow$ with $p'' \leq p_j$. Thus, we know that $\mathcal{P}^{\nu\mathcal{E}.\Phi}_{\prec}(N\Phi\downarrow, x)$ holds which is a contradiction. We therefore conclude that the case $y\mu_{col} \in \gamma$ is impossible and so the result holds. □

Lemma 22. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup and let tr and trH be the transformation functions of $\mathcal{S}$. Let $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \mathrm{DFrame}(\mathcal{S})$. Assume the following property:*

$$\text{for all } t \in \mathrm{dom}(\rho^\sigma_\alpha) \cup \mathrm{dom}(\rho^\sigma_\beta),\ \nu\mathcal{E}.\mathsf{tr}(\Phi) \not\vdash \mathsf{tr}_\alpha(t) \text{ and } \nu\mathcal{E}.\mathsf{tr}(\Phi) \not\vdash \mathsf{tr}_\beta(t)$$

For all $M \in \mathsf{Recipe}(\mathcal{E} \cup \mathcal{N}_{abs}, \Phi)$, for all $\gamma \in \{\alpha, \beta\}$, if there exist $N \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M\Phi\downarrow)$ then $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(M\Phi\downarrow, \gamma)$.

Proof. Let us show that for all $M \in \mathsf{Recipe}(\mathcal{E} \cup \mathcal{N}_{abs}, \Phi)$, for all $\gamma \in \{\alpha, \beta\}$, if there exists $N \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ and $p \in \mathcal{P}os(M\Phi\downarrow)$ such that:

– $M\Phi\downarrow|_p \in \mathrm{dom}(\rho^\sigma_\gamma)$
– for all p' strict prefix of p, $\mathsf{root}(M\Phi\downarrow|_{p'}) = \langle\rangle$
– $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M\Phi\downarrow)$

then there exist $L \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$, $\omega \in \{\alpha, \beta\}$ and $t \in \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta)$ such that $L\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\omega(t)$.

We show this result by induction on $|p|$.

Base case $|p| = 0$: In such a case, $M\Phi\downarrow \in \mathrm{dom}(\rho^\sigma_\gamma)$ and since $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M\Phi\downarrow)$, the result holds with $L = N$, $\omega = \gamma$ and $t = M\Phi\downarrow$.

Inductive step $|p| > 0$: In such a case, $p = i \cdot p'$ for some strict prefix p' and $i \in \mathbb{N}$. Hence, by hypothesis, we know that $\mathsf{root}(M\Phi\downarrow) = \langle\rangle$. Thus, $M\Phi\downarrow = \langle t_1, t_2\rangle$ and $i \in \{1, 2\}$. Moreover, by considering $M' = \mathsf{proj}_i(M)$, we obtain that $M'\Phi\downarrow = t_i$, $M\Phi\downarrow|_p = M'\Phi\downarrow|_{p'}$ and for all p'' strict prefix of p', $i \cdot p''$ is a strict prefix of p and so $\mathsf{root}(M\Phi\downarrow|_{i\cdot p'}) = \langle\rangle$ which implies $\mathsf{root}(M'\Phi\downarrow|_{p''}) = \langle\rangle$. Lastly, we know that $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M\Phi\downarrow)$. Since $\mathsf{root}(M\Phi\downarrow) = \langle\rangle$, we deduce from Properties 8 and 6 of Definition 12 that $M\Phi\downarrow \notin \mathsf{H}_\gamma \cup \mathrm{dom}(\mu_\gamma)$. Moreover, we assumed that $M\Phi\downarrow \notin \mathrm{dom}(\rho^\sigma_\gamma)$. Therefore, we conclude that $N\mathsf{tr}(\Phi)\downarrow = \langle\mathsf{tr}_\gamma(t_1), \mathsf{tr}_\gamma(t_2)\rangle$. Hence, $\mathsf{proj}_i(N)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(t_i)$. By applying our inductive hypothesis on $\mathsf{proj}_i(M)$ and γ, we conclude that there exists $L \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$, $\omega \in \{\alpha, \beta\}$ and $t \in \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta)$ such that $L\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\omega(t)$. Hence the result holds. □

Lemma 23. *Let $\mathcal{S} = (\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka})$ be a setup and let tr and trH be the transformation functions of $\mathcal{S}$. Let $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \mathrm{DFrame}(\mathcal{S})$. Assume the following hypothesis:*

H1- for all $t \in \mathrm{dom}(\rho^\sigma_\alpha) \cup \mathrm{dom}(\rho^\sigma_\beta)$, $\nu\mathcal{E}.\mathsf{tr}(\Phi) \not\vdash \mathsf{tr}_\alpha(t)$ and $\nu\mathcal{E}.\mathsf{tr}(\Phi) \not\vdash \mathsf{tr}_\beta(t)$

For all $M \in \mathsf{Recipe}(\mathcal{E} \cup \mathcal{N}_{abs}, \Phi)$, there exist two terms $M_\alpha, M_\beta \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that for all $\gamma \in \{\alpha, \beta\}$, $M_\gamma\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M\Phi\downarrow)$.

Proof. Let us denote $\mathcal{E} \cup \mathcal{N}_{abs}$ by $\mathcal{E}'$. Let $M \in \mathsf{Recipe}(\mathcal{E}', \Phi)$. Note that w.l.o.g. we can assume that $M\downarrow = M$ since $M\downarrow\Phi\downarrow = M\Phi\downarrow$. Let $\gamma \in \{\alpha, \beta\}$. For the purpose of this proof, we define the predicate $P(\gamma, M)$ to hold if and only if there exists $M_\gamma \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $M_\gamma\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M\Phi\downarrow)$. Therefore, we need to show that for all $M \in \mathsf{Recipe}(\mathcal{E}', \Phi)$, $M\downarrow = M$ implies $P(\alpha, M)$ and $P(\beta, M)$. We prove this result by induction on $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M)$.

Base case $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) = (\mathsf{x}_0, 0)$: Such a case is impossible since there is no term M with $|M| = 0$.

Inductive step $\mathcal{M}^{\mathcal{E},\Phi}_{\prec}(M) > (\mathsf{x}_0, 0)$: First, notice that $M\Phi\downarrow = C[u_1, \ldots, u_n]$ where C is built over $\{\langle\rangle\}$, and for all $i \in \{1, \ldots, n\}$, $\mathsf{root}(u_i) \neq \langle\rangle$. Before showing the main result, we show the two properties:

Property U1: We first show that for all $\gamma, \eta \in \{\alpha, \beta\}.\gamma \neq \eta$, if $P(\gamma, M)$ and for all $i \in \{1, \ldots, n\}$, $u_i \in \mathsf{H}_\gamma \cup \mathrm{dom}(\mu_\gamma)$ implies there exists $N \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\eta(u_i)$ then $P(\eta, M)$.

Let us assume that $P(\gamma, M)$ and for all $i \in \{1, \ldots, n\}$, $u_i \in \mathsf{H}_\gamma \cup \mathrm{dom}(\mu_\gamma)$ implies there exists $N \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\eta(u_i)$. Considering that C is built over $\{\langle\,\rangle\}$, $P(\gamma, M)$ and by our hypothesis H1, notice that for all $\varepsilon \in \{\alpha, \beta\}$, $\mathsf{tr}_\varepsilon(M\Phi\downarrow) = C[\mathsf{tr}_\varepsilon(u_1), \ldots, \mathsf{tr}_\varepsilon(u_n)]$ and for all $i \in \{1, \ldots, n\}$, $u_i \notin \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta)$ and there exists $N_i \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $N_i\Phi\downarrow = u_i$. We will show that for all $i \in \{1, \ldots, n\}$, there exists $N^\eta_i \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N^\eta_i\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\eta(u_i)$. With such property, we will directly obtain that $C[N^\eta_1, \ldots, N^\eta_n]\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\eta(M\Phi\downarrow)$.

Since for all $i \in \{1, \ldots, n\}$, $u_i \notin \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta)$, we know that one of the following properties hold:

1. $u_i \in \mathsf{H}_\gamma$: The result holds by hypothesis.
2. $u_i \in \mathsf{H}_\eta$: Since $N_i\Phi\downarrow = u_i$, Definition 18 gives us that there exists $(x, u) \in \textsc{ProTerm}(\Phi, \mathcal{S})$, $u' \in st(u)$, two sets K_s, K_a such that $x\mu_{col} \in \gamma$, $\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(u_i, x)$, $u'\sigma\downarrow = u_i$, $\mathsf{root}(u') = \mathsf{root}(u_i)$ and $(u', K_s, K_a) \in \text{E-}\textsc{terms}_{x\mu_{col}}(\mathcal{S})$. Thus, $\mathcal{M}^{\mathcal{E},\Phi}_\prec(M) \geq (x, 1)$.
   Moreover, we also know that $u_i = D[v_1, \ldots, v_m]$ for some $v_1, \ldots v_m$ and context D built on $\{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$ where:
   - for all $j \in \{1, \ldots, m\}$, either $v_j \in \mathrm{dom}(\mu_\eta)$ or $\neg\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(v_j, x)$.
   - for all $p \in \mathcal{P}os(D)$, $D|_p \neq \_$ implies $\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(u_i|_p, x)$

   By Lemma 21, we deduce that for all $p \in \mathcal{P}os(D)$, $\mathsf{root}(D|_p) \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ implies $u_i|_p \in \mathsf{H}_\eta$. As such, $\mathsf{tr}_\eta(u_i) = D[\mathsf{trH}_\eta(v_1), \ldots, \mathsf{trH}_\eta(v_m)]$. Note that for all $j \in \{1, \ldots, m\}$, $v_j \in \mathrm{dom}(\mu_\eta)$ or $\neg\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(v_j, x)$. In the former case, by Property 3 of Definition 18, we know that $\mathrm{img}(\mu_\alpha, \mu_\beta) \cap \mathcal{E} = \emptyset$. Thus, $\mathsf{trH}_\eta(v_j) \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ and so the result holds. In the latter case, $\neg\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(v_j, x)$ implies that there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $N\Phi\downarrow = v_j$. Since $\mathcal{M}^{\mathcal{E},\Phi}_\prec(M) \geq (x, 1)$, we obtain that $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N) < \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$. Thus, by Lemmas 22 and 6 and by our inductive hypothesis, we deduce that $\mathsf{tr}_\eta(v_j) = \mathsf{trH}_\eta(v_j)$ and there exists $N^\eta_j \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N^\eta_j\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\eta(v_j)$. As such we conclude that there exist $R_1, \ldots, R_m \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that for all $j \in \{1, \ldots, m\}$, $R_j\mathsf{tr}(\Phi)\downarrow = \mathsf{trH}_\eta(v_j)$. Therefore, $D[R_1, \ldots, R_j]\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\eta(u_i)$. Hence the result holds.
3. $u_i \in \mathrm{dom}(\mu_\gamma)$: The result holds by hypothesis.
4. $u_i \in \mathrm{dom}(\mu_\eta)$: By Property 3 of Definition 18, we know that $\mathrm{img}(\mu_\alpha, \mu_\beta) \cap \mathcal{E} = \emptyset$. Thus, $\mathsf{trH}_\eta(v_j) \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ and so the result holds.
5. $\mathsf{tagroot}_{\mathsf{Ka},\mathsf{Ks}}(u_i) \in \{\alpha, \beta\}$ and $u_i \notin \mathrm{dom}(\mu_\gamma, \mu_\eta) \cup \mathsf{H}_\gamma \cup \mathsf{H}_\eta$: In such a case, by Definition 13, we directly obtain $\mathsf{tr}_\alpha(u_i) = \mathsf{tr}_\beta(u_i)$. Since we know that $P(\gamma, M)$ then there exists $M_\gamma \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $M_\gamma\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(C[u_1, \ldots, u_n]) = C[\mathsf{tr}_\gamma(u_1), \ldots, \mathsf{tr}_\gamma(u_n)]$. Considering that C is built on $\langle\,\rangle$, we obtain that there exists $M'_\gamma \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $M'_\gamma\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(u_i) = \mathsf{tr}_\eta(u_i)$.
6. $\mathsf{tagroot}_{\mathsf{Ka},\mathsf{Ks}}(u_i) = 0$ and $u_i \notin \mathrm{dom}(\mu_\gamma, \mu_\eta) \cup \mathsf{H}_\gamma \cup \mathsf{H}_\eta$: In such a case, we know that there exist $\mathsf{f}/m \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$ and terms $t_1, \ldots, t_m$ such that $u_i = \mathsf{f}(t_1, \ldots, t_m)$. Moreover, $u_i \in DFct(M\Phi\downarrow)$ therefore by Lemma 20 and by Definition 16, we obtain that there exist $N_1, \ldots, N_m \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that for all $j \in \{1, \ldots, m\}$, $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N_j) < \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$ and $N_j\Phi\downarrow = t_j$. We can thus apply our inductive hypothesis on $N_1, \ldots, N_m$ which allows us to deduce that there exist $N^\eta_1, \ldots, N^\eta_m \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that for all $j \in \{1, \ldots, n\}$, $N^\eta_j\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\eta(t_j)$. We can thus conclude with $\mathsf{f}(N^\eta_1, \ldots, N^\eta_m)$.
7. $u_i \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ and $u_i \notin \mathrm{dom}(\mu_\gamma, \mu_\eta) \cup \mathsf{H}_\gamma \cup \mathsf{H}_\eta$. In such a case, we have also $\mathsf{tr}_\alpha(u_i) = \mathsf{tr}_\beta(u_i)$ and so we conclude as in the last but two case.

Property U2: We now show for all $t \in \mathsf{H}_\gamma$

Main proof: Assume first that $|M| = 1$. In such a case, either (a) $M \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ or (b) $M \in \mathrm{dom}(\Phi)$.

In Case (a), we deduce that $M\Phi\downarrow = M\mathsf{tr}(\Phi)\downarrow = M$. Assume that there exists $\omega \in \{\alpha, \beta\}$ such that $M \in \mathrm{dom}(\rho^\sigma_\alpha)$. Let $\varepsilon \in \{\alpha, \beta\}$ such that $\varepsilon \neq \omega$. By Property 2 of Definition 12, we deduce that $M \notin \mathrm{dom}(\rho^\sigma_\varepsilon, \mu_\varepsilon)$. Moreover, by Property 8 of Definition 12, we deduce that $M \notin \mathsf{H}_\alpha \cup \mathsf{H}_\beta$. Hence,

$\mathsf{tr}_\varepsilon(M) = M$. But this contradicts our hypothesis H1 as $M \in \mathsf{Recipe}(\mathcal{E}', \Phi)$ and $M \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ implies $M \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$, and so $\nu\mathcal{E}.\mathsf{tr}(\Phi) \vdash \mathsf{tr}_\varepsilon(M)$ with $M \in \mathrm{dom}(\rho^\sigma_\omega)$. Therefore, we deduce that $M \notin \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta)$. Moreover, by Property 6 of Definition 18, we know that for all $\gamma \in \{\alpha, \beta\}$, for all $t \in \mathrm{dom}(\mu_\gamma)$, there exists $x \in \mathrm{dom}(\Phi)$ such that $\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(t, x)$. But $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that for all $y \in fv(M)$, $y \prec x$ (since $fv(M) = \emptyset$). Hence, $M\Phi\!\downarrow \neq t$. Since $M\Phi\!\downarrow = M$, we deduce that $M \notin \mathrm{dom}(\mu_\alpha, \mu_\beta)$. This allows us to conclude that $\mathsf{tr}_\alpha(M\Phi\!\downarrow) = \mathsf{tr}_\beta(M\Phi\!\downarrow) = M = M\mathsf{tr}(\Phi)\!\downarrow$ and so $P(\alpha, M)$ and $P(\beta, M)$ hold.

In Case (b), let us denote $M = x$. By definition, we know that there exists $\gamma \in \{\alpha, \beta\}$ such that $x\mu_{col} \in \gamma$. Let $\omega \in \{\alpha, \beta\}$ such that $\omega \neq \gamma$. By Definition 19, we deduce that $x\mathsf{tr}(\Phi) = \mathsf{tr}_\gamma(x\Phi)$. But $\mathrm{img}(\Phi)$ is a set of messages in normal form. Hence, $x\Phi = M\Phi\!\downarrow$. Moreover, by Lemma 4 and Property 4 of Definition 18, we deduce that $\mathsf{tr}_\gamma(x\Phi)$ is in normal form and so $M\mathsf{tr}(\Phi)\!\downarrow = \mathsf{tr}_\gamma(M\Phi\!\downarrow)$. This allows us to deduce that $P(\gamma, M)$ holds. Let us now show that $P(\omega, M)$ holds. Note that there exist a context C built over $\{\langle\,\rangle\}$ and terms $u_1, \ldots, u_n$ such that $M\Phi\!\downarrow = C[u_1, \ldots, u_n]$ and for all $i \in \{1, \ldots, n\}$, $\mathsf{root}(u_i) \neq \langle\,\rangle$. Let $i \in \{1, \ldots, n\}$ such that $u_i \in \mathsf{H}_\gamma \cup \mu_\gamma$. By Definition 18, we obtain that $u_i = D[v_1, \ldots, v_m]$ where D is built on $\{\mathsf{h}, \mathsf{pk}, \mathsf{vk}, \langle\,\rangle\}$:

- for all $j \in \{1, \ldots, m\}$, $v_j \in \mathrm{dom}(\mu_\gamma)$ or $\neg\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(v_j, y)$
- for all $q \in \mathcal{P}os(D)$, $D|_p \neq \_$ implies $\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(u_i|_q, y)$

for some y such that $\neg(M \prec y)$.

For all $j \in \{1, \ldots, m\}$, if $\neg\mathcal{P}^{\nu\mathcal{E}.\Phi}_\prec(v_j, y)$ then there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N) < \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$ and $N\Phi\!\downarrow = v_j$. Else if $v_j \in \mathrm{dom}(\mu_\gamma)$ then by denoting q the position of v_j in $M\Phi\!\downarrow$ and p the position of u_i in $M\Phi\!\downarrow$, we obtain that $p \leq q$, $(v_j, q) \in\in Fct_{M\Phi\downarrow}(\gamma)$ and $\mathcal{P}^m_{Fct}((v_j, q), M\Phi\!\downarrow, u_i)$. By applying Lemmas 15 and 17, we obtain that there exist $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ and $q' \in \mathcal{P}os(M\Phi\!\downarrow)$ such that $p \leq q' \leq q$, $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N) < \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$ and $N\Phi\!\downarrow = M\Phi\!\downarrow|_{q'}$. Therefore, we have proved that for all $j \in \{1, \ldots, m\}$, there exists $q_j, p_j \in \mathcal{P}os(u_i)$ and $N_j \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $u_i|_{q_j} = v_j$, $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N_j) < \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$, $p_j \leq q_j$ and $N_j\Phi\!\downarrow = u_j|_{p_j}$. Therefore, we conclude that there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N) < \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$ and $N\Phi\!\downarrow = u_i$. Therefore, we can apply our inductive hypothesis on N and obtain that there exists $N_\omega \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_\omega\mathsf{tr}(\Phi)\!\downarrow = \mathsf{tr}_\omega(u_i)$. We conclude by applying Property U1.

Assume now that $|M| > 1$. In such a case there exist $M_1, \ldots, M_n$ and a function symbol f such that $M = \mathsf{f}(M_1, \ldots, M_n)$. We do a case analysis on f.

Case (A), $\mathsf{f} \in \Sigma_i^+$, $\gamma \in \{\alpha, \beta\}$, $i \in \gamma$*:* We know that $M\Phi\!\downarrow = \mathsf{f}(M_1\Phi\!\downarrow, \ldots, M_n\Phi\!\downarrow)\!\downarrow$. Let us denote $u = \mathsf{f}(M_1\Phi\!\downarrow, \ldots, M_n\Phi\!\downarrow)$. Hence, there exists a context C built on Σ_i^+ and $u_1, \ldots, u_m$ such that $u = C[u_1, \ldots, u_m]$, $Fct(u) = \{u_1, \ldots, u_m\}$ and $u_1, \ldots, u_m$ are in normal form. By Properties 6, 7 and 8 of Definition 12, we deduce that for all position p of C different from a hole, $u|_p \notin \mathrm{dom}(\rho^\sigma_\gamma, \mu_\gamma)$ and $u|_p \notin \mathsf{H}_\gamma$. Hence, $\mathsf{tr}_\gamma(u) = C[\mathsf{tr}_\gamma(u_1), \ldots, \mathsf{tr}_\gamma(u_m)]$. Note that by Lemma 1, we deduce that $u\!\downarrow = D[u_{j_1}, \ldots, u_{j_k}]$ for some context D built on Σ_i^+ and $\{j_1, \ldots, j_k\} \subseteq \{0, \ldots, n\}$ with $u_0 = n_{min}$. Moreover, by Lemmas 2 and 3 we deduce that $\mathsf{tr}_\gamma(u)\!\downarrow = D[\mathsf{tr}_\gamma(u_{j_1}), \ldots, \mathsf{tr}_\gamma(u_{j_k})]$. Once again by Properties 6, 7 and 8 of Definition 12, $u\!\downarrow = D[u_{j_1}, \ldots, u_{j_k}]$ implies that $\mathsf{tr}_\gamma(u\!\downarrow) = D[\mathsf{tr}_\gamma(u_{j_1}), \ldots, \mathsf{tr}_\gamma(u_{j_k})]$ and so we obtain that $\mathsf{tr}_\gamma(u\!\downarrow) = \mathsf{tr}_\gamma(u)\!\downarrow$.

By inductive hypothesis on $M_1, \ldots, M_n$, we know that there exist $M_1^\gamma, \ldots, M_n^\gamma \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that for all $j \in \{1, \ldots, n\}$, $M_j^\gamma\mathsf{tr}(\Phi)\!\downarrow = \mathsf{tr}_\gamma(M_j\Phi\!\downarrow)$. But $u = \mathsf{f}(M_1\Phi\!\downarrow, \ldots, M_n\Phi\!\downarrow)$ and $\mathsf{tr}_\gamma(u) = \mathsf{f}(\mathsf{tr}_\gamma(M_1\Phi\!\downarrow), \ldots, \mathsf{tr}_\gamma(M_n))$. Thus $\mathsf{tr}_\gamma(u) = \mathsf{f}(M_1^\gamma\mathsf{tr}(\Phi)\!\downarrow, \ldots, M_n^\gamma\mathsf{tr}(\Phi)\!\downarrow)$. Hence, $\mathsf{tr}_\gamma(u)\!\downarrow = \mathsf{f}(M_1^\gamma, \ldots, M_n^\gamma)\mathsf{tr}(\Phi)\!\downarrow$. Since $\mathsf{tr}_\gamma(u\!\downarrow) = \mathsf{tr}_\gamma(u)\!\downarrow$, we obtain that $\mathsf{f}(M_1^\gamma, \ldots, M_n^\gamma)\mathsf{tr}(\Phi)\!\downarrow = \mathsf{tr}_\gamma(M\Phi\!\downarrow)$. This allows us to deduce that $P(\gamma, M)$ holds with $M_\gamma = \mathsf{f}(M_1^\gamma, \ldots, M_n^\gamma)$.

Assume now that $M\Phi\!\downarrow = E[t_1, \ldots, t_m]$ with E built on $\{\langle\,\rangle\}$ and for all $j \in \{1, \ldots, m\}$, $\mathsf{root}(t_j) \neq \langle\,\rangle$. For all $j \in \{1, \ldots, m\}$, if $t_j \in \mathsf{H}_\gamma \cup \mathrm{dom}(\mu_\gamma)$ then we obtain that there exists $k \in \{1, \ldots, n\}$ such that either $M_k\Phi\!\downarrow = M\Phi\!\downarrow$ or $Fct_{t_j}(\gamma) \subseteq AFct(M_k\Phi\!\downarrow)$. Using a similar reasoning as in Case (b) and relying Lemma 17, we deduce that there exists $N_\omega \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_\omega\mathsf{tr}(\Phi)\!\downarrow = \mathsf{tr}_\omega(t_j)$. We conclude by applying Property U1.

Case (B), $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}, \mathsf{h}, \mathsf{pk}, \mathsf{vk}, \langle\,\rangle\}$*:* In such a case, $M\Phi\!\downarrow = \mathsf{f}(M_1\Phi\!\downarrow, \ldots, M_n\Phi\!\downarrow)$. By Property 6 of Definition 12, we deduce that $M\Phi\!\downarrow \notin \mathrm{dom}(\mu_\alpha, \mu_\beta)$. If $M\Phi\!\downarrow \in \mathrm{dom}(\rho^\sigma_\alpha)$ or

$M\Phi\downarrow \in \mathsf{H}_\alpha$ then by Property 2, we deduce that $M\Phi\downarrow \notin \mathrm{dom}(\rho^\sigma_\beta)$ and $M\Phi\downarrow \notin \mathsf{H}_\beta$. Hence, we deduce that there exists $\gamma \in \{\alpha, \beta\}$ such that $M\Phi\downarrow \notin \mathrm{dom}(\rho^\sigma_\gamma, \mu_\gamma) \cup \mathsf{H}_\gamma$. By Definition 13, there exists $\omega \in \{\alpha, \beta\}$ such that $\mathsf{tr}_\gamma(M\Phi\downarrow) = \mathsf{f}(\mathsf{tr}_\omega(M_1\Phi\downarrow), \ldots, \mathsf{tr}_\omega(M_n\Phi\downarrow))$. By our inductive hypothesis on $M_1, \ldots, M_n$, we deduce that there exist $M^\omega_1, \ldots, M^\omega_n \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that for all $j \in \{1, \ldots, n\}$, $M^\omega_j\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\omega(M_j\Phi\downarrow)$. Hence, $\mathsf{tr}_\gamma(M\Phi\downarrow) = \mathsf{f}(M^\omega_1\mathsf{tr}(\Phi)\downarrow, \ldots, M^\omega_n\mathsf{tr}(\Phi)\downarrow) = \mathsf{f}(M^\omega_1, \ldots, M^\omega_n)\mathsf{tr}(\Phi)\downarrow$. This allows us to deduce $P(\gamma, M)$ holds with $M_\gamma = \mathsf{f}(M^\omega_1, \ldots, M^\omega_n)$.

Note that since $P(\gamma, M)$ then by our hypothesis H1, we obtain that $M\Phi\downarrow \notin \mathrm{dom}(\rho^\sigma_\alpha, \rho^\sigma_\beta)$. To prove $P(\omega, M)$, we do a case analysis on f:

- If $\mathsf{f} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$ then we conclude directly with Property U1.
- If $\mathsf{f} = \langle\ \rangle$ then thanks to $M\Phi\downarrow \notin \mathrm{dom}(\rho^\sigma_\omega)$, we have $\mathsf{tr}_\omega(M\Phi\downarrow) = \mathsf{f}(\mathsf{tr}_\omega(M_1\Phi\downarrow), \ldots, \mathsf{tr}_\omega(M_n\Phi\downarrow))$ and so we conclude by applying our inductive hypothesis on $M_1, \ldots, M_n$.
- If $\mathsf{f} \in \{\mathsf{h}, \mathsf{pk}, \mathsf{vk}\}$ and $M\Phi\downarrow \in \mathsf{H}_\omega$ then in such a case, $n = 1$ and $\mathsf{tr}_\omega(M\Phi\downarrow) = \mathsf{f}(\mathsf{trH}_\omega(M_1\Phi\downarrow))$. By inductive hypothesis on M_1, we know that $P(\omega, M_1)$ holds. Hence by Lemmas 22 and 6, we deduce that there exists $M'_1 \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $M'_1\mathsf{tr}(\Phi)\downarrow = \mathsf{trH}_\omega(M_1\Phi\downarrow)$. Thus the result holds with $\mathsf{f}(M'_1)$.
- If $\mathsf{f} \in \{\mathsf{h}, \mathsf{pk}, \mathsf{vk}\}$ and $M\Phi\downarrow \notin \mathsf{H}_\omega$ then in such a case, $n = 1$ and $\mathsf{tr}_\omega(M\Phi\downarrow) = \mathsf{f}(\mathsf{tr}_\omega(M_1\Phi\downarrow))$. Thus we conclude by applying our inductive hypothesis on M_1.

Case (C), $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$*:* In such a case, $n = 2$. Moreover, we know that $M\Phi$ is a message. Hence, there exists $\mathsf{g} \in \{\mathsf{senc}, \mathsf{rsenc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}\}$ (more specifically, $\mathsf{g} = \mathsf{senc}$ when $\mathsf{f} = \mathsf{sdec}$, $\mathsf{g} = \mathsf{rsenc}$ when $\mathsf{f} = \mathsf{rsenc}$, etc) and some terms $u_1, \ldots, u_m$ such that $M_1\Phi\downarrow = \mathsf{g}(u_1, \ldots, u_m)$, $u_1 = M\Phi\downarrow$ and:

- $M_2\Phi\downarrow = u_m$ when $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}\}$
- $\mathsf{pk}(M_2\Phi\downarrow) = u_m$ when $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}\}$
- $M_2\Phi\downarrow = \mathsf{vk}(u_m)$ when $\mathsf{f} = \mathsf{check}$

If $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M_1\Phi\downarrow) = 0$ or if there exist $N_1 \in \mathsf{Recipe}(\mathcal{E} \cup \mathcal{N}_{abs}, \Phi)$ such that $N_1\Phi\downarrow = u_1$ and $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N_1) < \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$ then the result holds by applying Lemma 20 and the inductive hypothesis. Hence, assume that there exists $\gamma \in \{\alpha, \beta\}$ such that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(M_1\Phi\downarrow) \in \gamma$ and for all $N_1 \in \mathsf{Recipe}(\mathcal{E} \cup \mathcal{N}_{abs}, \Phi)$, $N_1\Phi\downarrow = u_1$ implies $\mathcal{M}^{\mathcal{E},\Phi}_\prec(N_1) \geq \mathcal{M}^{\mathcal{E},\Phi}_\prec(M)$.

By Property 8 of Definition 12, we deduce that $M_1\Phi\downarrow \notin \mathsf{H}_\alpha \cup \mathrm{dom}(\rho^\sigma_\gamma, \mu_\gamma)$. By Definition 13, we deduce that $\mathsf{tr}_\gamma(M_1\Phi\downarrow) = \mathsf{g}(\mathsf{tr}_\gamma(u_1), \ldots, \mathsf{tr}_\gamma(u_m))$. By applying our inductive hypothesis on M_1 and M_2, we obtain that $P(M_1, \gamma)$ and $P(M_2, \gamma)$ hold and so there exist M'_1, $M'_2 \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$, for all $j \in \{1, 2\}$, $M'_j\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M_j\Phi\downarrow)$. Hence, $M'_1\mathsf{tr}(\Phi)\downarrow = \mathsf{g}(\mathsf{tr}_\gamma(u_1), \ldots, \mathsf{tr}_\gamma(u_m))$ and $M'_2\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M_2\Phi\downarrow)$. Let us do a small case analysis on f.

- Case $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsdec}\}$: We know that $M_2\Phi\downarrow = u_m$ thus $M'_2\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(u_m)$ which allows us to deduce that $\mathsf{f}(M'_1\mathsf{tr}(\Phi)\downarrow, M'_2\mathsf{tr}(\Phi)\downarrow)\downarrow = \mathsf{tr}_\gamma(u_1) = \mathsf{tr}_\gamma(M\Phi\downarrow)$. Therefore, $\mathsf{f}(M'_1, M'_2)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M\Phi\downarrow)$ and so $P(\gamma, M)$ holds with $M_\gamma = \mathsf{f}(M'_1, M'_2)$.
- Case $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}\}$: We know that $\mathsf{pk}(M_2\Phi\downarrow) = u_m$. Let us show that $\mathsf{tr}_\gamma(u_m) = \mathsf{pk}(\mathsf{tr}_\gamma(M_2\Phi\downarrow))$. Assume first $u_m \in \mathrm{dom}(\rho^\sigma_\gamma)$. In such a case, by Property 2 of Definition 12, we deduce that $u_m \notin \mathrm{dom}(\rho^\sigma_\omega, \mu_\omega) \cup \mathsf{H}_\omega$. Thus, $\mathsf{tr}_\omega(\mathsf{pk}(M_2\Phi\downarrow)) = \mathsf{pk}(\mathsf{tr}_\omega(M_2\Phi\downarrow))$. By applying our inductive hypothesis on M_2, we know that $P(\omega, M_2)$ holds meaning that there exists $N \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\omega(M_2\Phi\downarrow)$. Hence, $\mathsf{pk}(N)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\omega(u_m)$ where $u_m \in \mathrm{dom}(\rho^\sigma_\gamma)$ which contradicts our hypothesis H1. Therefore, we obtain that $u_m \notin \mathrm{dom}(\rho^\sigma_\gamma)$. By Property 6 of Definition 12, we also have that $u_m \notin \mathrm{dom}(\mu_\gamma)$. Hence by Definition 13, we obtain that $\mathsf{tr}_\gamma(u_m) = \mathsf{pk}(\delta(\gamma, M_2\Phi\downarrow))$ where $\delta \in \{\mathsf{tr}, \mathsf{trH}\}$. However, we already proved that $M'_2\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(M_2\Phi\downarrow)$. Thus, by Lemma 22, we deduce that $\mathcal{P}^{\mathcal{S}}_{\langle\rangle}(M_2\Phi\downarrow, \gamma)$. By Lemma 6, it implies $\mathsf{tr}_\gamma(M_2\Phi\downarrow) = \mathsf{trH}_\gamma(M_2\Phi\downarrow)$ and so $\mathsf{tr}_\gamma(u_m) = \mathsf{pk}(\mathsf{tr}_\gamma(M_2\Phi\downarrow))$. This allows us to prove that $\mathsf{f}(M'_1, M'_2)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_\gamma(u_1) = \mathsf{tr}_\gamma(M\Phi\downarrow)$ and so $P(\gamma, M)$ holds with $M_\gamma = \mathsf{f}(M'_1, M'_2)$.
- Case $\mathsf{f} = \mathsf{check}$: In such a case, $m = 2$ and $M_2\Phi\downarrow = \mathsf{vk}(u_2)$. We know that $M_1\Phi\downarrow = \mathsf{sign}(u_1, u_2)$. By Lemma 20, we deduce that either:

- there exist $N_1, N_2 \in \mathsf{Recipe}(\mathcal{E} \cup \mathcal{N}_{abs}, \Phi)$ such that $\mathsf{sign}(N_1, N_2)\Phi\downarrow = \mathsf{sign}(u_1, u_2)$, $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(N_1) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M_1)$ and $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(N_2) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M_1)$: This case goes against our assumption.
- there exist $(x, u) \in \textsc{ProTerm}(\Phi, \mathcal{S})$ and $(v, K_s, K_a) \in \text{E-}\textsc{terms}_i(\mathcal{S})$ such that $x\mu_{col} = i$, $\mathsf{root}(v) = \mathsf{sign}$, $v \in st(u)$, $v\sigma$ is a message, $v\sigma\downarrow = \mathsf{sign}(u_1, u_2)$ and $\mathcal{M}_{\prec}^{\mathcal{E},\Phi} \geq (x, 1)$. Let $\gamma' \in \{\alpha, \beta\}$ such that $i \in \gamma'$. In such a case, by Properties 1 and 8 of Definition 16, we deduce that $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(v\sigma\downarrow) = i$ and $\mathcal{P}^{\mathcal{S}}_{\text{e-keys}}(\mathsf{vk}(u_2), i)$. Since $\mathsf{tagroot}_{\mathsf{Ks},\mathsf{Ka}}(v\sigma\downarrow) \in \gamma$, we obtain that $\gamma = \gamma'$. Moreover, from Properties 8 and 7 of Definition 12 we know that $M_1\Phi\downarrow \notin \mathrm{dom}(\rho^{\sigma}_{\gamma}, \mu_{\gamma}) \cup \mathsf{H}_{\gamma}$. Moreover, by Definition 13, we obtain that $\mathsf{tr}_{\gamma}(M_1\Phi\downarrow) = \mathsf{sign}(\mathsf{tr}_{\gamma}(u_1), \mathsf{tr}_{\gamma}(u_2))$. Furthermore, by Lemma 7, we obtain that $\mathsf{tr}_{\gamma}(\mathsf{vk}(u_2)) = \mathsf{vk}(\mathsf{tr}_{\gamma}(u_2))$. By inductive hypothesis on M_1, M_2, we know that $P(\gamma, M_1)$ and $P(\gamma, M_2)$ holds meaning that there exists $N_1', N_2' \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_1'\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\gamma}(M_1\Phi\downarrow)$ and $N_2'\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\gamma}(M_2\Phi\downarrow) = \mathsf{vk}(\mathsf{tr}_{\gamma}(u_2))$. Thus, we conclude that $\mathsf{check}(N_1', N_2')\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\gamma}(u_1) = \mathsf{tr}_{\gamma}(M\Phi\downarrow)$. This allows us to deduce that $P(\gamma, M)$ holds.

Assume now that $M\Phi\downarrow = E[t_1, \ldots, t_m]$ with E built on $\{\langle\rangle\}$ and for all $j \in \{1, \ldots, m\}$, $\mathsf{root}(t_j) \neq \langle\rangle$. For all $j \in \{1, \ldots, m\}$, if $t_j \in \mathsf{H}_{\gamma} \cup \mathrm{dom}(\mu_{\gamma})$ then we obtain that there exists $k \in \{1, \ldots, n\}$ such that either $M_k\Phi\downarrow = M\Phi\downarrow$ or $Fct_{t_j}(\gamma) \subseteq AFct(M_k\Phi\downarrow)$. Using a similar reasoning as in Case (b) and relying Lemma 17, we deduce that there exists $N_{\omega} \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_{\omega}\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\omega}(t_j)$. We conclude by applying Property U1.

Case (D), $\mathsf{f} = \mathsf{proj}_j$*,* $j \in \{1, 2\}$*:* In such a case, $n = 1$. Since $M\Phi$ is a message, we know that there exist u_1, u_2 such that $M_1\Phi\downarrow = \langle u_1, u_2\rangle$. By Property 8 of Definition 12, we deduce that $M_1\Phi\downarrow \notin \mathsf{H}_{\alpha} \cup \mathsf{H}_{\beta}$. Moreover, by Property 6 of Definition 12, we also deduce that $M_1\Phi\downarrow \notin \mathrm{dom}(\mu_{\alpha}, \mu_{\beta})$. Lastly, by Property 2 of Definition 12, we deduce that there exists $\gamma \in \{\alpha, \beta\}$ such that $M_1\Phi\downarrow \notin \mathrm{dom}(\rho^{\sigma}_{\gamma})$. Thus, $\mathsf{tr}_{\gamma}(M_1\Phi\downarrow) = \langle \mathsf{tr}_{\gamma}(u_1), \mathsf{tr}_{\gamma}(u_2)\rangle$. By applying our inductive hypothesis on M_1, we obtain that there exists $N_1 \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_1\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\gamma}(M_1\Phi\downarrow)$. Hence, $\mathsf{proj}_j(N_1)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\gamma}(u_j) = \mathsf{tr}_{\gamma}(M\Phi\downarrow)$. Therefore, we conclude that $P(\gamma, M)$ holds.

Note that $N_1\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\gamma}(M_1\Phi\downarrow)$ and our hypothesis H1 that $M_1\Phi\downarrow \in \mathrm{dom}(\rho^{\sigma}_{\omega})$. Thus $\mathsf{tr}_{\omega}(M_1\Phi\downarrow) = \langle \mathsf{tr}_{\omega}(u_1), \mathsf{tr}_{\omega}(u_2)\rangle$. By applying our inductive hypothesis on M_1, we also deduce that there exists $N_2 \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_2\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\omega}(M_1\Phi\downarrow)$. Hence, $\mathsf{proj}_j(N_2)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}_{\omega}(u_j) = \mathsf{tr}_{\omega}(M\Phi\downarrow)$. Therefore, we conclude that $P(\omega, M)$ holds. □

Theorem 1. *Let $P[\_A, \_B]$ be a context process and $Q = Q_A \mid Q_B$ be a process such that P and Q satisfy hypotheses H_1 to H_4. Let ϕ be a composable property.*

If the following conditions are satisfied

- $!^i\,\mathsf{agent}(A, \{H[i], D[i]\}).!^j\,\mathsf{agent}(B, \{H[j], D[j]\}).$ $P[O_A, O_B] \models \phi_{\mathsf{PKI}}$ *(that is, P is a secure PKI)*
- $Q_{perm} \models \phi_{sec} \wedge \phi$ *(that is, Q is a secure protocol)*

then $P[Q_A, Q_B]$ is secure, that is

$$!^i\,\mathsf{agent}(A, \{H[i], D[i]\}).!^j\,\mathsf{agent}(B, \{H[j], D[j]\}).P[Q_A, Q_B] \models \phi$$

where $\phi_{sec} \hat{=} \forall \tau \in \overline{\mathtt{secret}}_H.\forall x \in \tau.\not\vdash x$.

Proof (Sketch of proof). The beginning of the proof is quite standard w.r.t. existing composition results. It is well known that reachability properties compose well when processes do no share any secret. Hence from our hypothesis H_2, we obtain that $C[P[O_A, O_B]] \mid Q_{perm} \models \phi_{sec}$ where $C[\_] = !^i\,\mathsf{agent}(A, \{H[i], D[i]\}).!^j\,\mathsf{agent}(B, \{H[j], D[j]\}).\_$. From there we reason by contradiction. If $C[P[Q_A, Q_B]] \not\models \phi_{sec}$ then it is easy to see that $C[P[O_A[Q_A], O_B[Q_B]]] \not\models \phi_{sec}$ since O_A and O_B are just outputs. Applying the same reasoning with fresh inputs, we can build two processes R_{real} and R_{perm} such that

- $C[P[Q_A, Q_B]] \not\models \phi_{sec}$ implies $R_{real} \not\models \phi_{sec}$
- $C[P[O_A, O_B]] \mid Q_{perm} \models \phi_{sec}$ implies $R_{perm} \models \phi_{sec}$
- R_{real} and R_{perm} only differs by the messages in the process.

For example, to any occurrence of a variable x_{skA} of an honest agent A in R_{real} corresponds an occurrence of $sk[A]$ at the same position. The heart and most difficult part of the proof consist in showing that $R_{real} \not\models \phi_{sec}$ in fact implies $R_{perm} \not\models \phi_{sec}$. For this we consider a transformation δ on terms whose purpose is to dynamically replace the occurrences of the instantiation of x_{skA}, x_{sigB}, etc in a configuration of R_{real} by their counterpart in R_{perm}. In particular we show that

1. for all $R_{real} \to^* (\mathcal{E}; P; \Phi; \sigma; \mu)$, we have $R_{perm} \to^* (\mathcal{E}; P; \delta(\Phi); \delta(\sigma); \delta(\mu))$
2. $(\mathcal{E}; P; \Phi; \sigma; \mu) \models_c \vdash u$ implies $(\mathcal{E}; P; \delta(\Phi); \delta(\sigma); \delta(\mu)) \models_c \vdash \delta(u)$.

In the first bullet point, we show by induction on the size of the trace that there exists $\rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta$, $\mathsf{H}_\alpha, \mathsf{H}_\beta, \sigma, \mathsf{Ks}, \mathsf{Ka}$ such that $\mathcal{S} = (\sigma, \rho_\alpha, \rho_\beta, \mu_\alpha, \mu_\beta, \mathsf{Ks}, \mathsf{Ka}) \in \textsc{Setup}$ and $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \textsc{DFrame}(\mathcal{S})$. To prove that $\sigma \in \textsc{Compatible}(\rho_\alpha, \rho_\beta)$, we rely on the fact that $R_{perm} \models \phi_{PKI}$ and Lemma 3. When the conditions C_1 and C_2 are satisfied (i.e. when fully tagged) then Ks and Ka are empty. The rest of properties in $\mathcal{S} \in \textsc{Setup}$ are given by construction. To prove that $(\mathcal{E}, \Phi, \prec, \mu_{col}) \in \textsc{DFrame}(\mathcal{S})$, we need to show that all terms of the protocols are e-terms. Properties 3 and 4 are given by construction. The rest of the properties is done by contradiction with the fact that all terms in $\mathrm{dom}(\rho^\sigma_\alpha) \cup \mathrm{dom}(\rho^\sigma_\beta)$ are not deducible. For instance, for Property 6, to show that $u|_p\sigma\!\downarrow \notin \mathrm{dom}(\rho^\sigma_\gamma)$, we first recall that terms in $\mathrm{dom}(\rho^\sigma_\gamma)$ have been generated by the process of color $\omega \neq \gamma$. Since terms in $\mathrm{dom}(\rho^\sigma_\alpha) \cup \mathrm{dom}(\rho^\sigma_\beta)$ are not deducible, we deduce that $u|_p\sigma\!\downarrow$ is of the form $C[v_1, \ldots, v_n]$ where C is built on $\{\langle\rangle, \mathsf{pk}, \mathsf{vk}, \mathsf{h}\}$ where all v_i non deducible when generated by the process of color ω are in fact in $Fct_\gamma(u|_p\sigma\!\downarrow)$. Then thanks to Lemmas 15 and 17, we obtain a contradiction by proving that all these v_i are in fact deducible which would thus lead to a term in $\mathrm{dom}(\rho^\sigma_\gamma)$ to be deducible. The second bullet point is given by Lemma 23. □

F Ideal scenario

For the ideal scenario, we redefine a similar but simpler transformation as in the previous section.

Definition 25 (Ideal setup). *An* ideal setup *is a tuple (ρ, σ) where ρ and σ are two substitutions of ground messages in normal form such that:*

- $\mathrm{dom}(\rho) \subseteq \mathrm{dom}(\sigma)$
- *for all* $x \in \mathrm{dom}(\rho)$, $x\rho \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sig[A]) \mid A \in \mathcal{A}_D\}$
- *for all* $x, y \in \mathrm{dom}(\rho)$, $x\sigma = y\sigma$ *if and only if* $x\rho = y\rho$

Definition 26 (i-terms). *Let $\mathcal{S} = (\rho, \sigma)$ be an ideal setup. We define the set of ideal terms w.r.t. $\mathcal{S}$, denote* I-terms$(\mathcal{S})$*, as the set of terms u such that for all $p \in \mathcal{P}os(u)$,*

- $\mathsf{root}(u|_p) = \mathsf{tagk}$ *implies there exists* $x \in \mathrm{dom}(\rho)$ *such that* $u|_p = \mathsf{tagk}(x)$
- $u|_p \in \mathrm{dom}(\rho)$ *implies there exist* $p' \in \mathcal{P}os(u)$ *and a function symbol* $\mathsf{f}/n \in \mathcal{F}$ *such that* $\mathsf{root}(u|_{p'}) = \mathsf{f}$ *and one of the following properties hold:*
  - $\mathsf{f} = \mathsf{tagk}$ *and* $p = p' \cdot 1$
  - $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}, \mathsf{check}\}$ *and* $p = p' \cdot n$
- $\forall \mathsf{f}/n \in \Sigma$, *if* $\mathsf{f} = \mathsf{root}(u|_p)$ *and* $\mathsf{f} = \mathsf{aenc}$ *(resp.* $\mathsf{raenc}, \mathsf{check}$*) then* $u|_{p\cdot n} \in \mathrm{dom}(\rho)$ *and* $\mathsf{root}(u|_{p\cdot n}\rho) = \mathsf{pk}$ *(resp.* pk, vk*) or* $u|_{p\cdot n} \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sk[A]) \mid A \in \overline{\mathcal{A}}_H\}$
- $\forall \mathsf{f}/n \in \Sigma$, *if* $\mathsf{f} = \mathsf{root}(u|_p)$ *and* $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}, \mathsf{sign}\}$ *then* $u|_{p\cdot n} \in \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_H\}$
- $names(u) \cap \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_D\} = \emptyset$

Definition 27. *Let $\mathcal{S} = (\rho, \sigma)$ be an ideal setup. The transformation function of $\mathcal{S}$ is a mapping* tr *from terms to terms and defined as follows:*

- $\mathsf{tr}(u) = u$ *when* $u \in \mathcal{X} \cup \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$
- $\mathsf{tr}(\mathsf{f}(u_1, \ldots, u_n)) = \mathsf{f}(\mathsf{tr}(u_1), \ldots, \mathsf{tr}(u_{n-1}), u_n\rho^\sigma)$ *when* $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$ *and* $u_n \in \mathrm{dom}(\rho^\sigma)$
- $\mathsf{tr}(\mathsf{sign}(u_1, u_2)) = \mathsf{sign}(\mathsf{tr}(u_1), a)$ *when* $\mathsf{vk}(u_2) \in \mathrm{dom}(\rho^\sigma)$ *and* $\mathsf{vk}(u_2)\rho^\sigma = \mathsf{vk}(a)$.
- $\mathsf{tr}(\mathsf{tagk}(u)) = \mathsf{tagk}(u\rho^\sigma)$
- $\mathsf{tr}(\mathsf{f}(u_1, \ldots, u_n)) = \mathsf{f}(\mathsf{tr}(u_1), \ldots, \mathsf{tr}(u_n))$ *otherwise.*

We also define $\mathsf{tr}(\sigma)$ *as the substitution such that* $\mathrm{dom}(\sigma) = \mathrm{dom}(\mathsf{tr}(\sigma))$ *and:*

- *for all* $x \in \mathrm{dom}(\rho)$, $x\mathsf{tr}(\sigma) = x\rho$
- *for all* $x \in \mathrm{dom}(\sigma) \setminus \mathrm{dom}(\rho)$, $x\mathsf{tr}(\sigma) = \mathsf{tr}(x\sigma)$

Lemma 24. *Let* $\mathcal{S} = (\rho, \sigma)$ *be an idea setup. Let* tr *be the transformation function of* $\mathcal{S}$*. For all ground terms* u_1, u_2*, if* $names(u_1, u_2) \cap \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_D\} = \emptyset$ *then* $\mathsf{tr}(u_1) = \mathsf{tr}(u_2)$ *implies* $u_1 = u_2$*.*

Proof. By induction on $|u_1| + |u_2|$.

Base case $|u_1| + |u_2| = 1$*:* In such a case, $u_1, u_2 \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$. Hence the result directly holds since $\mathsf{tr}(u_1) = u_1$ a dn $\mathsf{tr}(u_2) = u_2$.

Inductive step $|u_1| + |u_2| > 1$*:* W.l.o.g. $u_1 = \mathsf{f}(t_1, \ldots, t_n)$. By Definition 27, we deduce that $\mathsf{root}(\mathsf{tr}(u_1)) = \mathsf{f}$ and so $\mathsf{root}(\mathsf{tr}(u_2)) = \mathsf{f}$. This implies that there exists $v_1, \ldots, v_n$ such that $u_2 = \mathsf{f}(v_1, \ldots, v_n)$. We do a case analysis on f:

- If $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$ and $t_n \in \mathrm{dom}(\rho^\sigma)$ then $\mathsf{tr}(u_1) = \mathsf{f}(\mathsf{tr}(t_1), \ldots, \mathsf{tr}(t_{n-1}), t_n\rho^\sigma) = \mathsf{tr}(u_2)$. Note that by Definition 27, $\mathsf{tr}(u_2) = \mathsf{f}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_{n-1}), v_n\rho^\sigma)$ or $\mathsf{f}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_{n-1}), \mathsf{tr}(v_n))$. But $names(u_1, u_2) \cap \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_D\} = \emptyset$ and $t_n\rho^\sigma \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sig[A]) \mid A \in \overline{\mathcal{A}}_D\}$. Hence, following Definition 27, we deduce that $v_n \in \mathrm{dom}(\rho^\sigma)$ and $v_n\rho^\sigma = t_n\rho^\sigma$. Since ρ^σ is injective, we obtain that $v_n = t_n$. Moreover by our inductive hypothesis on v_i, t_i for all $i \in \{1, \ldots, n-1\}$, we conclude that $u_1 = u_2$.
- If $\mathsf{f} = \mathsf{sign}$ and $\mathsf{vk}(t_2) \in \mathrm{dom}(\rho^\sigma)$: In such a case, we deduce that $\mathsf{tr}(\mathsf{sign}(t_1, t_2)) = \mathsf{sign}(\mathsf{tr}(t_1), a)$ where $\mathsf{vk}(t_2)\rho^\sigma = \mathsf{vk}(a)$ and so $a \in \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_D\}$. Note that by our hypothesis $names(u_1, u_2) \cap \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_D\} = \emptyset$, we deduce that $a \neq v_2$ and so $\mathsf{vk}(v_2) \in \mathrm{dom}(\rho^\sigma)$ and $\mathsf{vk}(v_2)\rho^\sigma = \mathsf{vk}(a)$. Since ρ^σ is injective, we obtain that $v_2 = t_2$. We conclude by our inductive hypothesis on v_1 and t_1.
- If $\mathsf{f} = \mathsf{sign}$ and $\mathsf{vk}(v_2) \in \mathrm{dom}(\rho^\sigma)$: Similar
- If $\mathsf{f} = \mathsf{tagk}$ then $\mathsf{tr}(u_1) = \mathsf{tagk}(t_1\rho^\sigma)$ and $\mathsf{tr}(u_2) = \mathsf{tagk}(v_1\rho^\sigma)$. Since ρ^σ is injective the result holds.
- Else $\mathsf{tr}(u_1) = \mathsf{f}(\mathsf{tr}(t_1), \ldots, \mathsf{tr}(t_n))$ and $\mathsf{tr}(u_2) = \mathsf{f}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_n))$ and so we conclude by applying inductive hypothesis on t_i, v_i for all $i \in \{1, \ldots, n\}$. □

Lemma 25. *Let* $\mathcal{S} = (\rho, \sigma)$ *be an idea setup. Let* tr *be the transformation function of* $\mathcal{S}$*. For all ground message in normal form* u*, if* $names(u) \cap \{n_{min}, sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_D\} = \emptyset$ *then* $\mathsf{tr}(u)$ *is in normal form and* $\mathsf{root}(\mathsf{tr}(u)) = \mathsf{root}(u)$*.*

Proof. Simple induction on $|u|$. □

Lemma 26. *Let* $\mathcal{S} = (\rho, \sigma)$ *be an idea setup. Let* $u \in$ I-TERMS$(\mathcal{S})$*. If* $u\sigma$ *is a message then* $\mathsf{tr}(u\sigma\downarrow) = u\mathsf{tr}(\sigma)\downarrow$ *and* $u\mathsf{tr}(\sigma)$ *is a message.*

Proof. We prove this result by induction on $|u|$.

Base case $|u| = 1$*:* In such a case $u \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$ or $u \in \mathcal{X}$. In the former case, the result directly holds since $\mathsf{tr}(u) = u$ and $u\sigma\downarrow = u = u\mathsf{tr}(\sigma)\downarrow$. In the latter case, by Definition 26, we deduce that $u \notin \mathrm{dom}(\rho)$ and so $\mathsf{tr}(u\sigma) = u\mathsf{tr}(\sigma)$ which allows us to conclude.

Inductive step $|u| > 1$*:* Otherwise $u = \mathsf{f}(u_1, \ldots, u_n)$ for some $u_1, \ldots, u_n$. Let us do a case analysis on f.

- Case $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$: In such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Moreover, by Definition 26, we know that $u_n \in \mathrm{dom}(\rho) \cup \{\mathsf{pk}(sk[A]), \mathsf{vk}(sk[A]) \mid A \in \overline{\mathcal{A}}_H\}$.
  In the former case, by Definition 27, we know that $\mathsf{tr}(u\sigma\downarrow) = \mathsf{f}(\mathsf{tr}(u_1\sigma\downarrow), \ldots, \mathsf{tr}(u_{n-1}\sigma\downarrow), u_n\sigma\downarrow\rho)$.
  Note that $u\sigma\downarrow = u\sigma$ which leads to $u\sigma\downarrow\rho^\sigma = u_n\rho = u_n\mathsf{tr}(\sigma)\downarrow$
  In the latter case, by Definition 25, we deduce that $u_n \notin \mathrm{dom}(\rho^\sigma)$ and so $\mathsf{tr}(u\sigma\downarrow) = \mathsf{f}(\mathsf{tr}(u_1\sigma\downarrow), \ldots, \mathsf{tr}(u_n\sigma\downarrow))$.
  Note that $u_n \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sk[A]) \mid A \in \overline{\mathcal{A}}_H\}$ implies that $\mathsf{tr}(u_n\sigma\downarrow) = \mathsf{tr}(u_n) = u_n = u_n\mathsf{tr}(\sigma)\downarrow$.

As such we deduce that $\mathsf{tr}(u\sigma\downarrow) = \mathsf{f}(\mathsf{tr}(u_1\sigma\downarrow), \ldots, \mathsf{tr}(u_{n-1}\sigma\downarrow), u_n\mathsf{tr}(\sigma)\downarrow)$. Notice that $u_1, \ldots, u_{n-1} \in$ I-TERMS$(\mathcal{S})$ meaning that we can apply our inductive hypothesis on them and so $\mathsf{tr}(u\sigma\downarrow) = \mathsf{f}(u_1\mathsf{tr}(\sigma)\downarrow, \ldots, u_{n-1}\mathsf{tr}(\sigma)\downarrow, u_n\mathsf{tr}(\sigma)\downarrow) = \mathsf{f}(u_1, \ldots, u_n)\mathsf{tr}(\sigma)\downarrow$ and $u\mathsf{tr}(\sigma)$ is a message.

- Case $\mathsf{f} = \mathsf{check}$: In such a case, $n = 2$. Moreover, since $u\sigma$ is a message, we know that there exist v_1, v_2 such that $u_1\sigma\downarrow = \mathsf{sign}(v_1, v_2)$ where $v_1 = u\sigma\downarrow$ and $\mathsf{vk}(v_2) = u_2\sigma\downarrow$. Note that by Definition 26, we deduce that $u_2 \in \mathrm{dom}(\rho) \cup \{\mathsf{vk}(sk[A]) \mid A \in \overline{\mathcal{A}}_H\}$.
  If $u_2 \in \mathrm{dom}(\rho)$ then we obtain that $u_2\mathsf{tr}(\sigma)\downarrow = u_2\rho$ and $u_2\sigma\downarrow \in \mathrm{dom}(\rho^\sigma)$. Moreover, Definition 26 also gives us that $\mathsf{root}(u_2\rho) = \mathsf{vk}$ meaning that $u_2\rho = \mathsf{vk}(a)$ for some a. Thus, by Definition 27, we deduce that $\mathsf{tr}(\mathsf{sign}(v_1, v_2)) = \mathsf{sign}(\mathsf{tr}(v_1), a)$. By inductive hypothesis on u_1, we know that $u_1\mathsf{tr}(\sigma)\downarrow = \mathsf{tr}(u_1\sigma\downarrow)$ and $u_1\mathsf{tr}(\sigma)$ is a message. Hence $\mathsf{check}(u_1, u_2)\mathsf{tr}(\sigma)\downarrow = \mathsf{check}(\mathsf{tr}(u_1\sigma\downarrow), u_2\mathsf{tr}(\sigma)\downarrow)\downarrow = \mathsf{check}(\mathsf{sign}(\mathsf{tr}(v_1), a), \mathsf{vk}(a))\downarrow = \mathsf{tr}(v_1) = \mathsf{tr}(u\sigma\downarrow)$. Since $u_1\mathsf{tr}(\sigma)$, $u_2\mathsf{tr}(\sigma)$ and $u\mathsf{tr}(\sigma)\downarrow \in st(u_1\mathsf{tr}(\sigma)\downarrow)$ then we also deduce that $u\mathsf{tr}(\sigma)$ is message.
  If $u_2 \in \{\mathsf{vk}(sk[A]) \mid A \in \overline{\mathcal{A}}_H\}$ then $u_2\sigma\downarrow = u_2$, $u_2\sigma\downarrow = u_2\rho^\sigma$ and $u_2 \notin \mathrm{dom}(\rho^\sigma)$. Moreover, $v_2 \in \overline{\mathcal{N}}$. As such, $\mathsf{tr}(v_2) = v_2$ and $\mathsf{tr}(\mathsf{sign}(v_1, v_2)) = \mathsf{sign}(\mathsf{tr}(v_1), v_2)$. By inductive hypothesis on u_1, we know that $u_1\mathsf{tr}(\sigma)\downarrow = \mathsf{tr}(u_1\sigma\downarrow)$ and $u_1\mathsf{tr}(\sigma)$ is a message. Hence $\mathsf{check}(u_1, u_2)\mathsf{tr}(\sigma)\downarrow = \mathsf{check}(\mathsf{sign}(\mathsf{tr}(v_1), v_2), \mathsf{vk}(v_2))\downarrow = \mathsf{tr}(v_1) = \mathsf{tr}(u\sigma\downarrow)$.
- Case $\mathsf{f} = \mathsf{tagk}$. By Definition 26, we deduce that $u_1 \in \mathrm{dom}(\rho)$. Hence, $\mathsf{tr}(u\sigma\downarrow) = \mathsf{tr}(\mathsf{tagk}(u_1\sigma\downarrow)) = \mathsf{tagk}(u_1\sigma\downarrow\rho^\sigma) = \mathsf{tagk}(u_1\rho) = \mathsf{tagk}(u_1\mathsf{tr}(\sigma))$. Hence the result holds.
- Case $\mathsf{f} = \mathsf{adec}$ (resp. radec): In such a case $n = 2$ and since $u\sigma$ is a message, we know that there exists $\mathsf{g} = \mathsf{aenc}$ (resp. *raenc*) and $v_1, \ldots, v_m$ such that $u_1\sigma\downarrow = \mathsf{g}(v_1, \ldots, v_m)$, $v_1 = u\sigma\downarrow$ and $v_m = \mathsf{pk}(u_2\sigma\downarrow)$. Note that by Definition 26, we know that $u_2 \in \{sk[A] \mid A \in \overline{\mathcal{A}}_H\}$ hence $v_m \notin \mathrm{dom}(\rho^\sigma)$. This allow us to deduce that $\mathsf{tr}(u_1\sigma\downarrow) = \mathsf{g}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_{m-1}), \mathsf{pk}(u_2))$. Moreover, since $u_2 \in \{sk[A] \mid A \in \overline{\mathcal{A}}_H\}$ then $u_2\mathsf{tr}(\sigma)\downarrow = u_2$. Therefore, we conclude that $\mathsf{f}(u_1\mathsf{tr}(\sigma)\downarrow, u_2\mathsf{tr}(\sigma)\downarrow)\downarrow = \mathsf{f}(\mathsf{g}(\mathsf{tr}(v_1), \ldots \mathsf{tr}(v_{m-1}), \mathsf{pk}(u_2)), u_2)\downarrow = \mathsf{tr}(v_1) = \mathsf{tr}(u\sigma\downarrow)$. Hence the result holds.
- Case $\mathsf{f} = \mathsf{sign}$: In such a case by Definition 26, $u_2 \in \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_H\}$. Thus $u_2\mathsf{tr}(\sigma)\downarrow = u_2$ and $\mathsf{vk}(u_2) \notin \mathrm{dom}(\rho^\sigma)$ meaning that $u_2\mathsf{tr}(\sigma)\downarrow = u_2 = \mathsf{tr}(u_2\sigma\downarrow)$. Hence $\mathsf{tr}(u\sigma\downarrow) = \mathsf{f}(\mathsf{tr}(u_1\sigma\downarrow), \mathsf{tr}(u_2\sigma\downarrow))$ and we conclude by applying our inductive hypothesis on u_1.
- Case $\mathsf{f} \in \{\mathsf{proj}_1, \mathsf{proj}_2\}$: In such a case, $u\sigma$ being a message implies that $u_1\sigma\downarrow = \langle v_1, v_2\rangle$ for some v_1, v_2 and $u\sigma\downarrow = v_j$ for some $j \in \{1, 2\}$. But $\mathsf{tr}(u_1\sigma\downarrow) = \langle \mathsf{tr}(v_1), \mathsf{tr}(v_2)\rangle$. By our inductive hypothesis on u_1, we deduce that $u_1\mathsf{tr}(\sigma)\downarrow = \langle \mathsf{tr}(v_1), \mathsf{tr}(v_2)\rangle$ and so $\mathsf{f}(u_1)\mathsf{tr}(\sigma)\downarrow = \mathsf{tr}(v_j) = \mathsf{tr}(u\sigma\downarrow)$. Thus the result holds.
- Case $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle, \mathsf{senc}, \mathsf{rsenc}\}$: In such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$ and $\mathsf{tr}(u\sigma\downarrow) = \mathsf{f}(\mathsf{tr}(u_1\sigma\downarrow), \ldots, \mathsf{tr}(u_n\sigma\downarrow))$. We conclude by applying our inductive hypothesis on $u_1, \ldots, u_n$.
- Case $\mathsf{f} \in \{\mathsf{sdec}, \mathsf{rsenc}\}$: In such a case, $n = 2$ and $u\sigma$ being a message implies that $u_1\sigma = \mathsf{g}(v_1, \ldots, v_m)$ for some $\mathsf{g} \in \{\mathsf{senc}, \mathsf{rsenc}\}$ and terms $v_1, \ldots, v_m$ where $v_1 = u\sigma\downarrow$ and $v_m = u_2\sigma\downarrow$. Note that $\mathsf{tr}(u_1\sigma\downarrow) = \mathsf{g}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_m))$. By Inductive hypothesis on u_1 and u_2, we obtain that $u\mathsf{tr}(\sigma)\downarrow = \mathsf{f}(\mathsf{tr}(u_1\sigma\downarrow), \mathsf{tr}(u_2\sigma\downarrow))\downarrow = \mathsf{f}(\mathsf{g}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_m)), \mathsf{tr}(v_m))\downarrow = \mathsf{tr}(v_1) = \mathsf{tr}(u\sigma\downarrow)$.
- Case $\mathsf{f} \notin \Sigma_0$: In such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)\downarrow$. Thus, if we denote $t = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$, we have $t = C[t_1, \ldots, t_m]$ where C does not contain function symbols from Σ_0 and $t_1, \ldots, t_m$ are factors of $\mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Hence $t\downarrow = D[t_{i_1}, \ldots, t_{i_k}]$ form some context D that does not contain function symbols from Σ_0 and $\{i_1, \ldots, i_k\} \subseteq \{0, \ldots, m\}$ with $t_0 = n_{min}$ thanks to Lemma 1. By Definition 27, we also deduce that $\mathsf{tr}(t) = C[\mathsf{tr}(t_1), \ldots, \mathsf{tr}(t_n)]$ and so thanks to Lemmas 24 and 2, we obtain that $\mathsf{tr}(t)\downarrow = D[\mathsf{tr}(t_{i_1}), \ldots, \mathsf{tr}(t_{i_k})]$. But $\mathsf{tr}(t) = \mathsf{f}(\mathsf{tr}(u_1\sigma\downarrow), \ldots, \mathsf{tr}(u_n\sigma\downarrow)) = \mathsf{f}(u_1\mathsf{tr}(\sigma)\downarrow, \ldots, u_n\mathsf{tr}(\sigma)\downarrow)$ thanks to our inductive hypothesis on $u_1, \ldots, u_n$. Thus, $u\mathsf{tr}(\sigma)\downarrow = \mathsf{tr}(t)\downarrow = D[\mathsf{tr}(t_{i_1}), \ldots, \mathsf{tr}(t_{i_k})] = \mathsf{tr}(D[t_{i_1}, \ldots, t_{i_k}]) = \mathsf{tr}(t\downarrow) = \mathsf{tr}(u\sigma\downarrow)$. Hence the result holds. □

Lemma 27. *Let $\mathcal{S} = (\rho, \sigma)$ be an idea setup. Let $u \in$ I-TERMS$(\mathcal{S})$. If $u\mathsf{tr}(\sigma)$ is a message then $u\sigma$ is a message.*

Proof. We prove this result by induction on $|u|$.

Base case $|u| = 1$: In such a case $u \in \mathcal{N} \cup \overline{\mathcal{A}} \cup \overline{\mathcal{N}}$ or $u \in \mathcal{X}$. In the former case, the result directly holds since $\mathsf{tr}(u) = u$ and $u\sigma\downarrow = u = u\mathsf{tr}(\sigma)\downarrow$. In the latter case, by Definition 26, we deduce that $u \notin \mathrm{dom}(\rho)$ and so $\mathsf{tr}(u\sigma) = u\mathsf{tr}(\sigma)$ which allows us to conclude.

Inductive step $|u| > 1$*:* Otherwise $u = \mathsf{f}(u_1, \ldots, u_n)$ for some $u_1, \ldots, u_n$. Let us do a case analysis on f.

- Case $\mathsf{f} \in \{\mathsf{rsenc}, \mathsf{senc}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}, \mathsf{pk}, \mathsf{vk}, \mathsf{h}, \langle\,\rangle\}$: In such a case, $u\sigma\!\downarrow = \mathsf{f}(u_1\sigma\!\downarrow, \ldots, u_n\sigma\!\downarrow)$. Note that $u_1, \ldots, u_{n-1} \in \text{I-TERMS}(\mathcal{S})$ and for all $i \in \{1, \ldots, n-1\}$, $u\mathsf{tr}(\sigma)$ being a message implies that $u_i\mathsf{tr}(\sigma)$ is a message. Hence by induction, we obtain that $u_i\sigma$ is a message. Moreover, by Definition 26, either $u_n \in \text{I-TERMS}(\mathcal{S})$ or $u_n \in \mathrm{dom}(\rho)$. In the former case by inductive hypothesis, we directly have that $u_n\sigma$ is a message. In the latter case, $u_n\sigma$ is directly a message since σ is a substitution of ground messages in normal form. Therefore, we obtain that for all $i \in \{1, \ldots, n\}$, $u_i\sigma$ is a message. Since $u\sigma\!\downarrow = \mathsf{f}(u_1\sigma\!\downarrow, \ldots, u_n\sigma\!\downarrow)$, we conclude that $u\sigma$ is a message.
- Case $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}\}$: In such a case, $n = 2$ and by Definition 26, we know that $u_1, u_2 \in \text{I-TERMS}(\mathcal{S})$. Since $u_1\mathsf{tr}(\sigma)$ being a message implies that there exists $\mathsf{g} \in \{\mathsf{aenc}, \mathsf{raenc}\}$ and $V_1, \ldots, V_m$ such that $u_1\mathsf{tr}(\sigma)\!\downarrow = \mathsf{g}(V_1, \ldots, V_m)$, $V_1 = u\mathsf{tr}(\sigma)\!\downarrow$ and $\mathsf{pk}(u_2\mathsf{tr}(\sigma)\!\downarrow) = V_m$. Thus, by Definition 26, we know that $u_2 \in \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_H\}$. Hence, $u_2\mathsf{tr}(\sigma)\!\downarrow = u_2$. Hence $V_m = \mathsf{pk}(u_2)$. But $u_2 \in \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_H\}$ implies that $\mathsf{pk}(u_2) \notin \mathrm{dom}(\rho^\sigma)$. By inductive hypothesis on u_1, we have that $u_1\sigma$ is a message and so by Lemmas 25 and 26, there exists $v_1, \ldots, v_m$ such that $u_1\sigma\!\downarrow = \mathsf{g}(v_1, \ldots, v_m)$ and $\mathsf{tr}(u_1\sigma\!\downarrow) = \mathsf{g}(V_1, \ldots, V_m)$ meaning that one of the following two cases holds:
  - $v_m \in \mathrm{dom}(\rho^\sigma)$: In such a case $\mathsf{tr}(u_1\sigma\!\downarrow) = \mathsf{g}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_{m-1}), v_m\rho^\sigma)$. Hence $V_m = v_m\rho^\sigma$. But $V_m = \mathsf{pk}(u_2)$ with $u_2 \in \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_H\}$. This is a contradiction with Definition 25. Hence such a case cannot happen.
  - $v_m \notin \mathrm{dom}(\rho^\sigma)$: In such a case, $\mathsf{tr}(u_1\sigma\!\downarrow) = \mathsf{g}(\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_n))$. Thus $V_m = \mathsf{tr}(v_n) = \mathsf{pk}(u_2)$. But $\mathsf{tr}(\mathsf{pk}(u_2)) = \mathsf{pk}(u_2)$ and so $\mathsf{tr}(v_n) = \mathsf{tr}(\mathsf{pk}(u_2))$ which implies by Lemma 24 that $v_n = \mathsf{pk}(u_2)$. Thus we conclude that $u\sigma\!\downarrow = \mathsf{f}(\mathsf{g}(v_1, \ldots, v_{m-1}, \mathsf{pk}(u_2)), u_2)\!\downarrow = v_1$. Note that $v_1 \in st(u_1\sigma\!\downarrow)$ and so we conclude that $u\sigma$ is a message.
- Case $\mathsf{f} = \mathsf{check}$: In such a case $n = 2$. Since $u\mathsf{tr}(\sigma)$ is a message then there exist V_1, V_2 such that $u_1\mathsf{tr}(\sigma)\!\downarrow = \mathsf{sign}(V_1, V_2)$, $u_2\mathsf{tr}(\sigma)\!\downarrow = \mathsf{vk}(V_2)$ and $u\mathsf{tr}(\sigma)\!\downarrow = V_1$. By inductive hypothesis on u_1, we know that $u_1\sigma$ is a message and so by Lemma 26, $u_1\mathsf{tr}(\sigma)\!\downarrow = \mathsf{tr}(u_1\sigma\!\downarrow)$. Hence by Lemma 25, there exists v_1, v_2 such that $u_1\sigma = \mathsf{sign}(v_1, v_2)$. By Definition 26, either $u_2 \in \mathrm{dom}(\rho)$ and $\mathsf{root}(u_2\rho) = \mathsf{vk}$ or $u_2 \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sig[A]) \mid A \in \overline{\mathcal{A}}_H\}$.
  If $u_2 \in \mathrm{dom}(\rho)$ then $u_2\mathsf{tr}(\sigma)\!\downarrow = u_2\rho = \mathsf{vk}(V_2)$ meaning that $V_2 \in \{sig[A] \mid A \in \overline{\mathcal{A}}_D\}$. By our hypothesis in Definition 26 and **??**, we know that $V_2 \notin names(u, \sigma)$ meaning that by Definition 27 that $\mathsf{vk}(v_2) \in \mathrm{dom}(\rho)$ and $\mathsf{vk}(v_2)\rho^\sigma = \mathsf{vk}(V_2)$ which implies that $\mathsf{vk}(v_2) = u_2$. This allows us to conclude that $u\sigma\!\downarrow = v_1$ and so the result holds.
  If $u_2 \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sig[A]) \mid A \in \overline{\mathcal{A}}_H\}$ then we know by definition 27 that $\mathsf{vk}(v_2) \notin \mathrm{dom}(\rho^\sigma)$ and so $\mathsf{tr}(u_1\sigma\!\downarrow) = \mathsf{sign}(\mathsf{tr}(v_1), \mathsf{tr}(v_2))$ and so $V_2 = \mathsf{tr}(v_2)$. But $u_2 = \mathsf{vk}(V_2)$ which implies that $\mathsf{tr}(u_2) = \mathsf{vk}(V_2) = \mathsf{tr}(\mathsf{vk}(v_2))$ and so $u_2 = \mathsf{vk}(v_2)$ thanks to Lemma 24. This allows us to conclude that $u\sigma\!\downarrow = v_1$ and so the result holds.
- Case $\mathsf{f} \notin \Sigma_0$: In such a case, $u\sigma\!\downarrow = \mathsf{f}(u_1\sigma\!\downarrow, \ldots, u_n\sigma\!\downarrow)\!\downarrow$. Thus, if we denote $t = \mathsf{f}(u_1\sigma\!\downarrow, \ldots, u_n\sigma\!\downarrow)$, we have $t = C[t_1, \ldots, t_m]$ where C does not contain function symbols from Σ_0 and $t_1, \ldots, t_m$ are factors of $\mathsf{f}(u_1\sigma\!\downarrow, \ldots, u_n\sigma\!\downarrow)$. Hence $t\!\downarrow = D[t_{i_1}, \ldots, t_{i_k}]$ form some context D that does not contain function symbols from Σ_0 and $\{i_1, \ldots, i_k\} \subseteq \{0, \ldots, m\}$ with $t_0 = n_{min}$ thanks to Lemma 1. By Definition 27, we also deduce that $\mathsf{tr}(t) = C[\mathsf{tr}(t_1), \ldots, \mathsf{tr}(t_n)]$ and so thanks to Lemmas 24 and 2, we obtain that $\mathsf{tr}(t)\!\downarrow = D[\mathsf{tr}(t_{i_1}), \ldots, \mathsf{tr}(t_{i_k})]$. But $\mathsf{tr}(t) = \mathsf{f}(\mathsf{tr}(u_1\sigma\!\downarrow), \ldots, \mathsf{tr}(u_n\sigma\!\downarrow)) = \mathsf{f}(u_1\mathsf{tr}(\sigma)\!\downarrow, \ldots, u_n\mathsf{tr}(\sigma)\!\downarrow)$ thanks to our inductive hypothesis on $u_1, \ldots, u_n$ and Lemma 26. Thus, $u\mathsf{tr}(\sigma)\!\downarrow = \mathsf{tr}(t)\!\downarrow = D[\mathsf{tr}(t_{i_1}), \ldots, \mathsf{tr}(t_{i_k})] = \mathsf{tr}(D[t_{i_1}, \ldots, t_{i_k}]) = \mathsf{tr}(t\!\downarrow)$. Note that since $u_1\sigma, \ldots, u_n\sigma$ are messages, we deduce that $t_1, \ldots, t_m$ are messages and so this allows us to conclude that $u\sigma$ is a message. □

Definition 28 (Ideal Frame). *Let $\mathcal{S} = (\rho, \sigma)$ be a setup. We define the set* $\text{IFRAME}(\mathcal{S})$ *as the smallest set such that for all substitutions Φ of ground terms in normal form, for all sets $\mathcal{E}$ of names, for all relation $\prec$ on variables, if the following conditions hold:*

1. $\mathrm{dom}(\Phi) \cap \mathrm{dom}(\sigma) = \emptyset$

2. $\prec$ *is a strict total order on* $\mathrm{dom}(\Phi) \cup \mathrm{dom}(\sigma) \cup \{\mathsf{x}_0\}$ *such that for all* $x \in \mathrm{dom}(\Phi) \cup \mathrm{dom}(\sigma)$, $\mathsf{x}_0 \prec x$
3. $names(\Phi) \cap \{n_{min}, sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_H\} = \emptyset$
4. *for all* $x \in \mathrm{dom}(\Phi)$ *(resp.* $\mathrm{dom}(\sigma)$*), either*
   (a) *there exist* $u \in$ I-TERMS$(\mathcal{S})$ *such that* $u\sigma\downarrow = x\Phi$ *(resp.* $x\sigma$*),* $u\sigma$ *is a message and for all* $z \in fv(u)$, $z \prec x$
   (b) *there exists* $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ *such that* $fv(M) \subseteq \{z \mid z \prec x\}$ *and* $M\Phi\downarrow = x\Phi$ *(resp.* $x\sigma$*)*
5. *for all* $x \in \mathrm{dom}(\rho)$, *there exists* $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ *such that* $fv(M) \subseteq \{z \mid z \prec x\}$ *and* $M\Phi\downarrow = x\sigma$.

then $(\mathcal{E}, \Phi, \prec) \in$ IFRAME$(\mathcal{S})$. *We also denote* IPROTERM$(\Phi, \mathcal{S})$ *the sets of elements of the form* (x, u) *where* $x \in \mathrm{dom}(\Phi) \cup \mathrm{dom}(\sigma)$ *and* x *satisfies Property 4a with the term* u.

Definition 29. *Let* u *a ground message. We define the predicate* $\mathcal{P}_{flaw}(u)$ *to holds if and only if there exists* $\mathsf{g}/m \in \{\mathsf{aenc}, \mathsf{raenc}\}$, *there exist* $t_1, \ldots, t_m$ *terms such that* $t = \mathsf{g}(t_1, \ldots, t_m)$, $t_m \in \mathrm{dom}(\rho^\sigma)$, $\mathsf{root}(t_m) = \mathsf{pk}$ *and* $\mathsf{root}(t_m\rho^\sigma) \neq \mathsf{pk}$.

Lemma 28. *Let* $\mathcal{S} = (\rho, \sigma)$ *be a setup. Let* $u \in$ I-TERMS$(\mathcal{S})$ *such that* $u\sigma$ *is a message. For all* $t \in st(u\sigma\downarrow)$, *if* $\mathcal{P}_{flaw}(t)$ *then there exists* $x \in fv(u)$ *such that* $t \in st(x\sigma)$.

Proof. Since $\mathcal{P}_{\text{flaw}}(t)$ then there exists $\mathsf{g}/m \in \{\mathsf{aenc}, \mathsf{raenc}\}$, there exist $t_1, \ldots, t_m$ terms such that $t = \mathsf{g}(t_1, \ldots, t_m)$, $t_m \in \mathrm{dom}(\rho^\sigma)$, $\mathsf{root}(t_m) = \mathsf{pk}$ and $\mathsf{root}(t_m\rho^\sigma) \neq \mathsf{pk}$. We prove this result by induction on $|u|$.

Base case $|u| = 1$*:* In such a case, $u \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$ or $u \in \mathcal{X}$. The former case is impossible since $\mathsf{g}(t_1, \ldots, t_m) \in st(u\sigma\downarrow)$ and in the latter case the result directly holds.

Inductive step $|u| > 1$*:* Otherwise, $u = \mathsf{f}(u_1, \ldots, u_n)$. Let us do a case analysis on f:

- Case $\mathsf{f} \in \{\mathsf{sign}, \mathsf{senc}, \mathsf{rsenc}, \mathsf{h}, \langle\,\rangle, \mathsf{vk}, \mathsf{pk}\}$: In such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. Hence, there exists $i \in \{1, \ldots, n\}$, $\mathsf{g}(t_1, \ldots, t_m) \in st(u_i\sigma\downarrow)$. By Definition 26, we know that $u_i \in$ I-TERMS$(\mathcal{S})$ meaning we can conclude by applying our inductive hypothesis on u_i.
- Case $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$: In such a case, $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$. By Definition 26, we know that $u_n \in \mathrm{dom}(\rho)$ or $u_n \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sig[A]) \mid A \in \overline{\mathcal{A}}_H\}$. Thus, we deduce that either there exists $i \in \{1, \ldots, n-1\}$ such that $\mathsf{g}(t_1, \ldots, t_m) \in st(u_i\sigma\downarrow)$ or $\mathsf{g}(t_1, \ldots, t_m) = u\sigma\downarrow$. In the former case, we can conclude by applying our inductive hypothesis on u_i. In the latter case, by hypothesis, we deduce that $u_n\sigma\downarrow \in \mathrm{dom}(\rho^\sigma)$, $\mathsf{root}(u\sigma\downarrow) = \mathsf{pk}$ and $\mathsf{root}(u_n\sigma\downarrow\rho^\sigma) \neq \mathsf{pk}$. By Definition 25, $u_n\sigma\downarrow \in \mathrm{dom}(\rho^\sigma)$ implies that $u_n \notin \{\mathsf{pk}(sk[A]), \mathsf{vk}(sig[A]) \mid A \in \overline{\mathcal{A}}_H\}$. Therefore $u_n \in \mathrm{dom}(\rho)$. Hence $u_n\sigma\downarrow = u\sigma$ and so $u_n\sigma\downarrow\rho^\sigma = u_n\sigma\rho^\sigma = u_n\rho$. But by Definition 26, we also know that $\mathsf{root}(u_n\rho) = \mathsf{pk}$ which comes in contradiction with the fact that $\mathsf{root}(u_n\sigma\downarrow\rho^\sigma) \neq \mathsf{pk}$. We therefore conclude that this case is impossible.
- Case $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}, \mathsf{sdec}, \mathsf{rsdec}, \mathsf{check}, \mathsf{proj}_1, \mathsf{proj}_2\}$: In such a case, since $u\sigma$ is message then we know that there exists $u\sigma\downarrow \in st(u_1\sigma\downarrow)$. Since $u_1 \in$ I-TERMS$(\mathcal{S})$ then we can apply our inductive hypothesis on u_1.
- Case $\mathsf{f} \notin \Sigma_0$: In such a case, we know that $u\sigma\downarrow = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)\downarrow$. By denoting $t = \mathsf{f}(u_1\sigma\downarrow, \ldots, u_n\sigma\downarrow)$, we have $t = C[v_1, \ldots, v_r]$ where C does not contain function symbols from Σ_0 and $v_1, \ldots, v_r$ are factors of t in normal form. Since $\mathsf{g} \in\in \{\mathsf{aenc}, \mathsf{raenc}\}$ then by Lemma 1, we deduce that $i \in \{1, \ldots, n\}$ such that $\mathsf{g}(t_1, \ldots, t_m) \in st(u_i\sigma\downarrow)$. As such we conclude by our inductive hypothesis on u_i. □

Lemma 29. *Let* $\mathcal{S} = (\rho, \sigma)$ *be a setup. Let* $(\mathcal{E}, \Phi, \prec) \in$ IFRAME$(\mathcal{S})$. *For all* $(x, u) \in$ IPROTERM$(\Phi, \mathcal{S})$, *for all* $t \in st(u\sigma\downarrow)$, *if* $\mathcal{P}_{flaw}(t)$ *then there exists* $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ *such that* $t \in st(M\Phi\downarrow)$ *and* $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M) < (x, 1)$.

Proof. This proof is done by induction on x w.r.t. the order $\prec$.

Base case $x = \mathsf{x}_0$*:* This case is impossible by definition of Φ.

Inductive step $\mathsf{x}_0 \prec x$ By Definition 28, $(x, u) \in$ IPROTERM$(\Phi, \mathcal{S})$ implies that $u\sigma$ is a message and $u \in$ I-TERMS$(\mathcal{S})$. By Lemma 28, we deduce that there exists $y \in fv(u)$ such that $t \in st(y\sigma)$. By Definition 28, we know that $y \prec x$ and also one of the following properties holds:

– there exists $v \in$ I-TERMS$(\mathcal{S})$ such that $(y, v) \in$ IFRAME$(\mathcal{S})$ and $y\sigma = v\sigma\downarrow$. Therefore, $t \in st(v\sigma\downarrow)$ and we can apply our inductive hypothesis on (y, v) allows us to conclude.
– there exists $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $fv(M) \subseteq \{z \mid z \prec y\}$ and $M\Phi\downarrow = y\sigma$. Hence $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M) \prec (y, 1) \prec (x, 1)$. We can therefore conclude. □

Lemma 30. *Let $\mathcal{S} = (\rho, \sigma)$ be a setup. Let $(\mathcal{E}, \Phi, \prec) \in$ IFRAME$(\mathcal{S})$. For all $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, for all $\mathsf{g}(t_1, \ldots, t_n) \in st(u\sigma\downarrow)$, if $\mathcal{P}_{flaw}(\mathsf{g}(t_1, \ldots, t_n)$ then there exist $M_1, \ldots, M_n$ such that for all $i \in \{1, \ldots, n\}$, $M_i\Phi\downarrow = t_i$ and $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M_i) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M)$.*

Proof. We prove this result by induction on $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M)$.

Base case $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M) = (\mathsf{x}_0, 0)$: Such a case is impossible since $|M|$ cannot be 0.
Inductive step $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M) > (\mathsf{x}_0, 0)$: Assume first that $|M| = 1$. In such a case, $M \in \mathrm{dom}(\Phi)$ or $M \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$. In the latter case, we trivially have that $M\Phi\downarrow = M$ and so this case is impossible since $\mathsf{g}(t_1, \ldots, t_n) \in st(M\Phi\downarrow)$. In the former case, by Lemma 29 we know that there exists $N \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $t \in st(N\Phi\downarrow)$ and $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(N) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M)$. We conclude by applying our inductive hypothesis on N.

Assume now that $|M| > 1$ meaning that $M = \mathsf{f}(M_1, \ldots, M_m)$. Let us do a case analysis on f.

– $\mathsf{f} \in \{\mathsf{sign}, \mathsf{senc}, \mathsf{rsenc}, \mathsf{h}, \langle\,\rangle, \mathsf{vk}, \mathsf{pk}\}$: In such a case $M\Phi\downarrow = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_m\Phi\downarrow)$. Hence there exists $i \in \{1, \ldots, m\}$ such that $\mathsf{g}(t_1, \ldots, t_n) \in st(M_i\Phi\downarrow)$. We conclude by inductive hypothesis on M_i.
– $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$: If $\mathsf{g}(t_1, \ldots, t_n) = M\Phi\downarrow$ then $n = m$, $\mathsf{g} = \mathsf{f}$ and for all $i \in \{1, \ldots, n\}$, $M_i\Phi\downarrow = t_i$. Therefore the result holds.
– $\mathsf{f} \in \{\mathsf{adec}, \mathsf{radec}, \mathsf{sdec}, \mathsf{rsdec}, \mathsf{check}, \mathsf{proj}_1, \mathsf{proj}_2\}$: Since $M\Phi$ is a message then we deduce that $M\Phi\downarrow \in st(M_1\Phi\downarrow)$. Thus, $\mathsf{g}(t_1, \ldots, t_n) \in st(M_1\Phi\downarrow)$ and so we conclude by induction on M_1.
– Case $\mathsf{f} \notin \Sigma_0$: In such a case, we know that $M\Phi\downarrow = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_m\Phi\downarrow)\downarrow$. By denoting $t = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_m\Phi\downarrow)$, we have $t = C[v_1, \ldots, v_r]$ where C does not contain function symbols from Σ_0 and $v_1, \ldots, v_r$ are factors of t in normal form. Since $\mathsf{g} \in\in \{\mathsf{aenc}, \mathsf{raenc}\}$ then by Lemma 1, we deduce that $i \in \{1, \ldots, m\}$ such that $\mathsf{g}(t_1, \ldots, t_n) \in st(M_i\Phi\downarrow)$. As such we conclude by our inductive hypothesis on M_i. □

Definition 30. *Let $\mathcal{S} = (\rho, \sigma)$ be a setup. Let tr be the transformation function of $\mathcal{S}$. Let $(\mathcal{E}, \Phi, \prec) \in$ IFRAME$(\mathcal{S})$. We define $\mathsf{tr}(\Phi)$ as the substitution with the same domain of Φ and such that $x\mathsf{tr}(\Phi) = \mathsf{tr}(x\Phi)$.*

Lemma 31. *Let $\mathcal{S} = (\rho, \sigma)$ be a setup. Let tr be the transformation function of $\mathcal{S}$. Let $(\mathcal{E}, \Phi, \prec) \in$ IFRAME$(\mathcal{S})$. For all $M \in \mathsf{Recipe}(\mathcal{E}, \Phi)$, if $names(M) \cap \{sk[A], sig[A] \mid A \in \overline{\mathcal{A}}_D\} = \emptyset$ then there exists $N \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M\Phi\downarrow)$.*

Proof. We prove this result by induction on $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}$.

Base case $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M) = (\mathsf{x}_0, 0)$: Such a case is impossible since $|M|$ cannot be 0.

Inductive step $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M) > (\mathsf{x}_0, 0)$: Assume first that $|M| = 1$. In such a case, $M \in \mathrm{dom}(\Phi)$ or $M \in \mathcal{N} \cup \overline{\mathcal{N}} \cup \overline{\mathcal{A}}$. In the latter case, we trivially have that $\mathsf{tr}(M) = M$ and so the result holds. In the former case, by definition $M\mathsf{tr}(\Phi) = \mathsf{tr}(M\Phi)$ and so the result holds.

Assume now that $|M| > 1$. In such a case, $M = \mathsf{f}(M_1, \ldots, M_n)$. We do a case analysis on f:

Case $\mathsf{f} \in \{\mathsf{aenc}, \mathsf{raenc}\}$: In such a case, $M\Phi\downarrow = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_n\Phi\downarrow)$. By our inductive hypothesis on $M_1, \ldots, M_n$, we deduce that there exists $N_1, \ldots, N_n$ such that for all $i \in \{1, \ldots, n\}$, $N_i\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M_i\Phi\downarrow)$. Moreover, if $M_n\Phi\downarrow \in \mathrm{dom}(\rho^\sigma)$ then $\mathsf{tr}(M\Phi\downarrow) = \mathsf{f}(\mathsf{tr}(M_1\Phi\downarrow), \ldots, \mathsf{tr}(M_{n-1}\Phi\downarrow), M_n\Phi\downarrow\rho^\sigma)$. But by Definition 25, we know that $\mathrm{img}(\rho^\sigma) \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$. Hence we obtain that $\mathsf{tr}(M\Phi\downarrow) = \mathsf{f}(N_1\mathsf{tr}(\Phi)\downarrow, \ldots, N_{n-1}\mathsf{tr}(\Phi)\downarrow, M_n\Phi\downarrow\rho^\sigma) = \mathsf{f}(N_1, \ldots, N_{n-1}, M_n\Phi\downarrow\rho^\sigma)\mathsf{tr}(\Phi)\downarrow$ where $\mathsf{f}(N_1, \ldots, N_{n-1}, M_n\Phi\downarrow\rho^\sigma) \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$. Hence the result holds when $M_n\Phi\downarrow \in \mathrm{dom}(\rho^\sigma)$. If

$M_n\Phi\downarrow \notin \mathrm{dom}(\rho^\sigma)$ then $\mathsf{tr}(M\Phi\downarrow) = \mathsf{f}(\mathsf{tr}(M_1\Phi\downarrow), \ldots, \mathsf{tr}(M_n\Phi\downarrow))$ and so $\mathsf{tr}(M\Phi\downarrow) = \mathsf{f}(N_1\mathsf{tr}(\Phi)\downarrow, \ldots, N_n\mathsf{tr}(\Phi)\downarrow) = \mathsf{f}(N_1, \ldots, N_n)\mathsf{tr}(\Phi)\downarrow$ where $\mathsf{f}(N_1, \ldots, N_n) \in \mathsf{Recipe}(\mathcal{E}, \Phi)$.

Case $\mathsf{f} = \{\mathsf{adec}, \mathsf{radec}\}$*:* In such a case, $n = 2$. Moreover, since $M\Phi\downarrow$ is a message then there exists $\mathsf{g} \in \{\mathsf{aenc}, \mathsf{raenc}\}$ and $t_1, \ldots, t_m$ such that $M_1\Phi\downarrow = \mathsf{g}(t_1, \ldots, t_m)$, $M\Phi\downarrow = t_1$ and $\mathsf{pk}(M_2\Phi\downarrow) = t_m$. Let us first consider that $t_m \in \mathrm{dom}(\rho^\sigma)$ then $\mathsf{tr}(\mathsf{g}(t_1, \ldots, t_m)) = \mathsf{g}(\mathsf{tr}(t_1), \ldots, \mathsf{tr}(t_{m-1}), t_m\rho^\sigma)$. By definition of ρ^σ, we know that $t_m\rho^\sigma \in \{\mathsf{pk}(sk[A]), \mathsf{vk}(sig[A]) \mid A \in \overline{\mathcal{A}}_D\}$. Note that if $\mathsf{root}(t_m\rho^\sigma) = \mathsf{vk}$ then $\mathcal{P}_{\mathrm{flaw}}(M_1\Phi\downarrow)$. Hence by Lemma 30 there exists $M_1' \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $M_1'\Phi\downarrow = t_1$ and $\mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M_1') < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M_1) < \mathcal{M}_{\prec}^{\mathcal{E},\Phi}(M)$. Hence we conclude by applying our inductive hypothesis on M_1'. Otherwise $\mathsf{root}(t_m\rho^\sigma) = \mathsf{pk}(sk[A])$ and we know that $sk[A] \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ when $A \in \overline{\mathcal{A}}_D$. Therefore, by applying our inductive hypothesis on M_1, we deduce that there exists $N_1 \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_1\mathsf{tr}(\Phi)\downarrow = \mathsf{g}(\mathsf{tr}(t_1), \ldots, \mathsf{tr}(t_{m-1}), t_m\rho^\sigma)$ meaning that $\mathsf{f}(N_1, sk[A])\downarrow = \mathsf{tr}(t_1) = \mathsf{tr}(M\Phi\downarrow)$. Hence the result holds.

Case $\mathsf{f} = \mathsf{sign}$*:* In such a case, $M\Phi\downarrow = \mathsf{sign}(M_1\Phi\downarrow, M_2\Phi\downarrow)$. If $\mathsf{vk}(M_2\Phi\downarrow) \in \mathrm{dom}(\rho^\sigma)$ and $\mathsf{vk}(M_2\Phi\downarrow)\rho^\sigma = \mathsf{vk}(sig[A])$ for some $A \in \overline{\mathcal{A}}_D$ then $\mathsf{tr}(M\Phi\downarrow) = \mathsf{sign}(\mathsf{tr}(M_1\Phi\downarrow), sig[A])$. In such a case, we know by inductive hypothesis that there exists $N_1 \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that $N_1\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M_1\Phi\downarrow)$ and so $\mathsf{sign}(N_1, sig[A])\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M\Phi\downarrow)$ meaning that there result holds. Otherwise $\mathsf{tr}(M\Phi\downarrow) = \mathsf{sign}(\mathsf{tr}(M_1\Phi\downarrow), \mathsf{tr}(M_2\Phi\downarrow))$. By applying our inductive hypothesis on M_1, M_2, we obtain $N_1, N_2 \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $N_1\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M_1\Phi\downarrow)$ and $N_2\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M_2\Phi\downarrow)$. Hence the result holds with $\mathsf{sign}(N_1, N_2)$.

Case $\mathsf{f} = \mathsf{check}$*:* In such a case, since $M\Phi$ is a message then there exists v_1, v_2 such that $M_1\Phi\downarrow = \mathsf{sign}(v_1, v_2)$, $M\Phi\downarrow = v_1$ and $M_2\Phi\downarrow = \mathsf{vk}(v_2)$. By inductive hypothesis on M_1, M_2, we obtain $N_1, N_2 \in \mathsf{Recipe}(\mathcal{E}, \Phi)$ such that $N_1\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M_1\Phi\downarrow)$ and $N_2\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M_2\Phi\downarrow)$. By definition 27, we know that either $\mathsf{tr}(M_1\Phi\downarrow) = \mathsf{sign}(\mathsf{tr}(v_1), \mathsf{tr}(v_2))$ or $\mathsf{tr}(M_1\Phi\downarrow) = \mathsf{sign}(\mathsf{tr}(v_1), sig[A])$ with $A \in \overline{\mathcal{A}}_D$. In the latter case, we obtain that $\mathsf{check}(N_1, \mathsf{vk}(sig[A]))\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(v_1) = \mathsf{tr}(M\Phi\downarrow)$. In the former case, we know that $\mathsf{tr}(\mathsf{vk}(v_2)) = \mathsf{vk}(\mathsf{tr}(v_2))$ meaning that $\mathsf{check}(N_1, N_2)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(v_1) = \mathsf{tr}(M\Phi\downarrow)$. Hence the result holds.

Case $\mathsf{f} \in \{\mathsf{pk}, \mathsf{vk}\}$*:* By definition $\mathsf{tr}(M\Phi\downarrow) = \mathsf{f}(\mathsf{tr}(M_1\Phi\downarrow))$. Thus we can applying our inductive hypothesis on M_1 which allows us to conclude.

Otherwise: We know that $M\Phi\downarrow = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_m\Phi\downarrow)\downarrow$. By denoting $t = \mathsf{f}(M_1\Phi\downarrow, \ldots, M_n\Phi\downarrow)$, we have $t = C[v_1, \ldots, v_r]$ where C does not contain function symbols from $\{\mathsf{vk}, \mathsf{pk}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$ and $v_1, \ldots, v_r$ are factors of t in normal form. By Lemma 1, we know that $M\Phi\downarrow = D[v_{i_1}, \ldots, v_{i_k}]$ for some D that does not contain function symbols from $\{\mathsf{vk}, \mathsf{pk}, \mathsf{aenc}, \mathsf{raenc}, \mathsf{sign}, \mathsf{adec}, \mathsf{radec}, \mathsf{check}\}$ and $i_1, \ldots, i_k \in \{0, \ldots, r\}$ and $v_0 = n_{min}$. By Definition 27, we know that $\mathsf{tr}(t) = C[\mathsf{tr}(v_1), \ldots, \mathsf{tr}(v_r)]$ and $\mathsf{tr}(M\Phi\downarrow) = D[\mathsf{tr}(v_{i_1}), \ldots, \mathsf{tr}(v_{i_k})]$. Moreover by Lemmas 24 and 2, we deduce that $\mathsf{tr}(t)\downarrow = \mathsf{tr}(M\Phi\downarrow)$. By our inductive hypothesis on $M_1, \ldots, M_n$, we know that there exists $N_1, \ldots, N_n \in \mathsf{Recipe}(\mathcal{E}, \mathsf{tr}(\Phi))$ such that for all $j \in \{1, \ldots, n\}$, $N_j\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(M_j\Phi\downarrow)$. However, $\mathsf{f}(\mathsf{tr}(M_1\Phi\downarrow), \ldots, \mathsf{tr}(M_n\Phi\downarrow)) = \mathsf{tr}(t)$. Hence $\mathsf{f}(N_1, \ldots, N_n)\mathsf{tr}(\Phi)\downarrow = \mathsf{tr}(t)\downarrow = \mathsf{tr}(M\Phi\downarrow)$. Hence the result holds. □