Inferences on Honesty in Compositional Logic for Protocol Analysis

Koji HASEBE and Mitsuhiro OKADA *

Department of Philosophy, Keio University
2-15-45 Mita, Minato-ku, Tokyo 108-8345, Japan
{hasebe,mitsu}@abelard.flet.keio.ac.jp

Abstract. We present an explicit treatment of assumptions on a principal's honesty in compositional logic. Our central idea is to divide an honest principal's role into its components, and these components are composed during the proving steps of a property useful to prove a protocol correctness. We distinguish the monotonic properties and the non-monotonic ones, and give a core inference system for the monotonic properties, which can be extended for non-monotonic ones.

1 Introduction

The main purpose of this paper is to make explicit compositionality of assumptions on honesty in the style of *compositional logic*, which was originally introduced by Durgin-Mitchell-Pavlovic [11] and Datta-Derek-Mitchell-Pavlovic [6, 7]. Especially this paper is aimed at introducing a core inference system of our framework as a first step. An extension is made by the subsequent paper [15] of ours.

Compositional logic is a proof system based on Floyd-Hoare style logical framework for proving protocol correctness. In this framework, a protocol is considered as a program, and a statement "from a principal P's viewpoint, a general property φ holds at the end of his/her protocol action $\vec{\alpha}$" can be represented as a formula of the form $[\vec{\alpha}]_P\ \varphi$ (or of the form $\theta[\vec{\alpha}]_P\ \varphi$ in [7]). One of the most advantageous points of this framework is its compositional approach for reasoning about a compound protocol: for proving a property about a compound protocol we can reuse already established properties about its components.

In the framework of compositional logic, statements are derived not only by means of some axioms about protocol actions but also by means of assumptions about the other principals' honesty. For formalizing such assumptions about honesty (called *honesty assumptions*), in [11, 6, 7] they use conditional statements

* This work was partly supported by Grants-in-Aid for Scientific Research of MEXT, Center of Excellence of MEXT on Humanity Sciences (Keio University), the Japan-US collaborative research program of JSPS-NSF, Oogata-kenkyu-jyosei grant (Keio University) and Global Security Research Center grant (Keio University). The first author was also supported by Fellowship for Japan Young Scientists from Japan Society for the Promotion of Science.

of the form $Honest(Q) \supset \varphi$, which means "if a principal Q is honest, then φ holds in any run of the protocol in question". On the other hand, we propose a way to make more explicit the composing steps of the honesty assumptions during a proving process of a property. For that purpose we use the form of expression $Honest(\vec{\alpha}^Q) \supset \varphi$, instead of $Honest(Q) \supset \varphi$, where $\vec{\alpha}^Q$ represents a sequence of *primitive actions* (i.e., sending, receiving or generating actions) in a role performed by Q. Using this framework, an (often minimal) requirement of Q's honesty to derive a property φ from P's viewpoint is expressed by explicitly mentioning the part $\vec{\alpha}^Q$ of Q's role in a protocol.

The basic form of assertion in our inference system is as follows.

$$Honest(\vec{\alpha}_1^{Q_1}), \ldots, Honest(\vec{\alpha}_n^{Q_n}), \Gamma \vdash [\vec{\beta}]_P \ \varphi,$$

where each $\vec{\alpha}_i^{Q_i}$ represents a component part of role performed by a principal Q_i (for each $i = 1, \ldots, n$). The intended meaning of the above sequent is "if each Q_i honestly performs a part of his/her role $\vec{\alpha}_i^{Q_i}$, and if some properties Γ hold, then after P performs a sequence of actions $\vec{\beta}$, φ holds from P's viewpoint". (Here Q_i may be the same as Q_j for some $i, j = 1, \ldots, n$.)

In our framework during a proving process, such honesty assumptions are derived not only by some special inferences, called *honesty inferences*, but also by the following *weakening rule* which is an analogy to the weakening rule of the traditional logic.

$$\frac{Hon(\vec{\alpha}^Q; \vec{\alpha}'^Q), \Gamma \vdash [\vec{\beta}; \vec{\beta}']_P \ \varphi}{Hon(\vec{\alpha}^Q; \alpha''^Q; \vec{\alpha}'^Q), \Gamma \vdash [\vec{\beta}; \beta''; \vec{\beta}']_P \ \varphi} \ \textbf{Weakening}$$

This means "from P's view, if a property φ is derived from Γ with Q's honesty on $\vec{\alpha}; \vec{\alpha}'$ after P's performance of $\vec{\beta}; \vec{\beta}'$, then φ is also derived from Γ with Q's honesty on $\vec{\alpha}; \alpha''; \vec{\alpha}'$ after P's performance of $\vec{\beta}; \beta''; \vec{\beta}'$, for any addition α'' and β'' in the roles". Here $\vec{\alpha}; \vec{\alpha}'$ ($\vec{\beta}; \vec{\beta}'$, resp.) is the sequential concatenation of two sequences of actions $\vec{\alpha}$ and $\vec{\alpha}'$ ($\vec{\beta}$ and $\vec{\beta}'$, resp.).

Moreover, by means of the weakening rule, honesty assumptions are composed by the following reasoning from P's view.

$$\frac{\dfrac{Hon(\vec{\alpha}^Q) \vdash [\vec{\beta}]_P \ x = t \qquad Hon(\vec{\alpha}'^Q) \vdash [\vec{\beta}]_P \ \varphi}{Hon(\vec{\alpha}^Q), Hon(\vec{\alpha}'^Q) \vdash [\vec{\beta}]_P \ \varphi[t/x]} \ \textbf{Eq}}{Hon(\vec{\alpha}^Q \circ \vec{\alpha}'^Q) \vdash [\vec{\beta}]_P \ \varphi[t/x]} \ \textbf{Comp(Hon)}$$

The intended meaning of this reasoning is as follows. First assume the two assertions from P's view: "if Q follows a part of his/her role $\vec{\alpha}^Q$ honestly, then $x = t$ holds after P performs his/her role $\vec{\beta}$", and "if Q follows another part of his/her role $\vec{\alpha}'^Q$ honestly, then a property φ holds". Then by an equality inference, "if Q follows $\vec{\alpha}^Q$ as well as $\vec{\alpha}'^Q$, then $\varphi[t/x]$" holds from P's view. Then by combining the two separated assumptions on Q's honesty into one assumption on Q's honesty (following his/her combined role $\vec{\alpha}^Q \circ \vec{\alpha}'^Q$), "if Q follows his/her combined role $\vec{\alpha}^Q \circ \vec{\alpha}'^Q$, then $\varphi[t/x]$" holds from P's view. Here $\vec{\alpha}^Q \circ \vec{\alpha}'^Q$ is a sequence of

actions which includes all actions in the components $\vec{\alpha}^Q$ and $\vec{\alpha}'^Q$ and preserving order. This composition is formalized as a derived rule **Comp(Hon)**, which is actually obtained by combining basic and natural logical (structural) inferences (i.e., weakening rule as shown above and usual contraction rule of left hand side of a sequent). Another example of a composition of honesty assumptions using cut rule is as follows.

$$\dfrac{\dfrac{Hon(\vec{\alpha}^Q) \vdash [\vec{\beta}]_P\ \varphi \qquad \varphi, Hon(\vec{\alpha}'^Q) \vdash [\vec{\beta}]_P\ \psi}{Hon(\vec{\alpha}^Q), Hon(\vec{\alpha}^Q) \vdash [\vec{\beta}]_P\ \psi}\ \textbf{Cut}}{Hon(\vec{\alpha}^Q \circ \vec{\alpha}'^Q) \vdash [\vec{\beta}]_P\ \psi}\ \textbf{Comp(Hon)}$$

By using such composing steps, for proving a property about a compound protocol we can directly reuse assertions about its components to construct a proof of the property.

Here we remark a difference on the standpoints between our approach and that of [11, 6, 7]. In order to realize the compositionality on the honesty assumptions, our approach needs to restrict the forms of honesty inferences to a Horn-clause. Therefore, the following kind of inferences, which is considered in [11, 6, 7], is not considered in our system: "if a principal (say P) honestly follows a role $\vec{\alpha} = \alpha_1; \alpha_2; \alpha_3$ of a protocol, then one concludes $Honest(P) \wedge (P \text{ performs } \beta) \supset (\beta = \alpha_1) \vee (\beta = \alpha_2) \vee (\beta = \alpha_3)$" (i.e., if P is honest and he/she performs an primitive action β then it is α_1 or α_2 or α_3). This kind of inferences is not in harmony with the compositionality because our weakening rules may add other possibilities of disjunctions. As a result, our framework is simplified to be the Horn-clause basis while [11, 6, 7] uses more general language including disjunctions and negations.

In our framework if one can freely apply the weakening rule to φ, we call φ a *monotonic* property. Freshness, receiving-fact, which are used in BAN logic [1], are examples of monotonic properties. On the other hand, for example, property $HasAlone(P, m)$ (introduced in [6, 7]), which means that "a message m is possessed only by P", is *non-monotonic*, because if a receiving action of m is added into the component of Q's role, then $HasAlone(P, m)$ does not hold anymore. (Another example of non-monotonic property is $Source$ introduced in [11].) The notion of monotonicity is essentially the same as the notion of *persistency* in the sense of [11, 6, 7]. However, while persistency is related only to the weakening rule for protocol actions (which are described in the square bracket "[ ]"), the notion of monotonicity is related to both weakening rules, for honesty assumptions and for protocol actions.

If we use such non-monotonic properties in our framework, we have to restrict the use of weakening rule by imposing appropriate conditions to preserve the properties, or to introduce a kind of temporal notion. However, so long as the monotonic properties are concerned, we do not need any restriction on the weakening rule nor any introduction of temporal notions. One of our aim in this paper is to explain our framework by restricting our attention within the core part of

our inference system which is made up of only some monotonic properties. As an example, we take a set of properties which are useful for proving *agreement property* (in the sense of Woo-Lam [19]) of a protocol.[1] These properties are mainly chosen from the BAN logic predicates such as "$sends$", "$receives$", "$fresh$" [2], and so on. All of our chosen properties are monotonic except "$sends$".[3] However, if we want to prove a property stronger than the agreement property, we need to introduce some non-monotonic properties, and then to restrict the free use of the weakening rules. In the subsequent work [15] of ours, we show how to extend our framework by introducing some non-monotonic properties. As an example, in [15] we introduce a non-monotonic property, simply called *firstly sends*, means "a principal sends a message m containing n as a subterm, and he/she does not send any other message m' containing n before the sending of m". Moreover, we demonstrate that this property is useful to derive the *matching conversations* of *Challenge Response protocol* [9] (cf. also [6,7]), which is stronger than the agreement property.

In this paper, we use the following notations. (The complete definition of the language of our system is presented in Appendix A.1.) The letters A, B, C,... (P, Q, R,..., resp.) are constants (variables , resp.) of principals' names. The capital letters $K, K', \ldots, K_1, K_2, \ldots$ and $N, N', \ldots, N_1, N_2, \ldots$ are constants of keys and of nonces, respectively, while the small letters $k, k', \ldots, k_1, k_2, \ldots$ and $n, n', \ldots, n_1, n_2, \ldots$ are variables of the same sorts as above. The letters $m, m', \ldots, m_1, m_2, \ldots$ are used to denote messages, and $\{m\}_K$ is the encryption of m with key K, and $\langle m_1, \ldots, m_n \rangle$ is the concatenation of messages $m_1, \ldots, m_n$. We also use the notation $m \sqsubseteq m'$ to represent the subterm relation as a meta symbol.

The rest of this paper is organized as follows. In Chapter 2 we give the definition of our inference system. In Chapter 3 we explain our proving method for a composed protocol by using the same example as [6, 7]. In Chapter 4 we give a semantics of the system by means of the notion of trace. Finally, in Chapter 5 we present our conclusions and some further issues.

2 Inference System

In this section, we give the definition of our inference system. The complete list of the formal definitions is presented in Appendix A.

[1] We do not go into the secrecy issue in this paper.

[2] In [6, 7], they use "t is *fresh*" differently from ours, namely as "no one else has seen any term containing t as a subterm". On the other hand, our use of freshness is the same as BAN logic [1].

[3] the property "$sends$" is non-monotonic with respect to the weakening rule for honesty assumptions. The details shall be explained in Section 2.

2.1 The Language

Predicates of our inference system are as follows: P *generates* n, P *receives* m [4], P *sends* m, $PK(P,k)$, $P \overset{k}{\leftrightarrow} Q$, $fresh(n)$ and $t = t'$. The first three predicates are called *action predicates* (*performed by* P). On the other hand, the last four predicates are called *non-action predicates*. All those predicates except equality are chosen from the BAN logic predicates [1]. Equality is used for explicit treatment of substitutions. As we have mentioned in Section 1, all those predicates except *sends* have *monotonic* properties (i.e., properties independent of the weakening rules for principal's actions and for honesty assumptions).[5] Here we introduce the following meta-symbols. The letters $\varphi, \psi, \ldots, \varphi', \ldots$ are used to denote *atomic formula* (or simply called *atoms*). The letters $\alpha, \beta, \gamma, \delta, \ldots, \alpha', \alpha'', \ldots, \alpha_1, \alpha_2, \ldots$ are used to denote atoms made of an action predicate (called *atomic action formulas*), and also $\alpha^P, \beta^P, \gamma^P, \delta^P, \ldots$ to denote atomic action formulas performed by P. The letters $\theta, \theta', \ldots, \theta_1, \theta_2, \ldots$ are atoms made of an non-action predicate (called *atomic non-action formulas*).

As logical connectives, we introduce only usual conjunction (denoted by ",") and non-commutative conjunction (denoted by ";"). Our intention is to use non-commutative conjunction to represent a sequence of principals' actions. While in [6, 7], they use some temporal operators to reason about the ordering of actions, we do not use any temporal operators: in our system orderings are directly expressed by non-commutative conjunction. We introduce the vector notation such as $\vec{\alpha}$ to denote a sequence (i.e., non-commutative conjunct) of atomic action formulas.

Our inference system uses a sequent calculus style assertion. The basic form of assertion is as follows (where Q_i may be the same as Q_j for some $i, j = 1, \ldots, n$).

$$Honest(\vec{\alpha}_1^{Q_1}), \ldots, Honest(\vec{\alpha}_n^{Q_n}), \Delta \vdash [\vec{\beta}]_A \ \varphi$$

Here $\vec{\alpha}_i^{Q_i}$ is a sequence of atomic action formulas performed by Q_i (for each $i = 1, \ldots, n$), which represents a part of his/her role. $\vec{\beta}$ is a sequence of actions performed by A.[6] φ is an atomic formula (made of an action or non-action predicate). Δ is of the form $\theta_1, \ldots, \theta_m, \vec{\gamma}_1, \ldots, \vec{\gamma}_k$. Each predicate of the form

[4] We distinguish two kinds of "*receives*": the simple receiving and the receiving with decryptions. P *receives* $m(\{m'\}_k^*)$ means that "P receives a message m and decrypts the indicated subterm $\{m'\}_k$ of m. For a more formal description, instead of using $*$, we could introduce a new predicate *decrypts* and describe it by (P *receives* m) $\wedge$ (P *decrypts* $\{m'\}_k$).

[5] As we shall see in the explanation of Matching rule of the honesty inferences in Section 2.2 (III), predicate "*sends*" is monotonic w.r.t. the weakening for concrete actions, however it is non-monotonic w.r.t. the weakening for honesty assumptions. In other words, this predicate is non-monotonic in the sense of our terminology, whereas it is "persistent" in the sense of [11, 6, 7].

[6] For describing a sequence of action, while compositional logic of [11, 6, 7] uses the *cord calculus*, we describe it by a sequence (i.e., non-commutative conjunct) of action predicates.

$Honest(\vec{\alpha}_i^{Q_i})$ represents "principal Q_i honestly follows a part of his/her role $\vec{\alpha}_i^{Q_i}$". We call it Q_i's *honesty assumption*. Here, if $\vec{\alpha}_i^{Q_i}$ is $\alpha_{i_1}^{Q_i}; \cdots ; \alpha_{i_m}^{Q_i}$, we can consider the predicate $Honest(\vec{\alpha}_i^{Q_i})$ as an abbreviation of $Honest(\alpha_{i_1}^{Q_i}); \cdots ; Honest(\alpha_{i_m}^{Q_i})$, which is a conjunct of non-commutative conjunction.

Therefore, the intuitive meaning of the sequent style assertion previously introduced is "if each principal Q_i honestly follows the parts of his/her role $\vec{\alpha}_i^{Q_i}$, and if some properties Δ hold, then after A performs a sequence of actions $\vec{\beta}$, φ holds from A's viewpoint". (Here $\vec{\beta}$ may be empty. In such case we often use the expression $\Gamma \vdash \varphi$, instead of $\Gamma \vdash [\,]\varphi$.)

Finally, we introduce the postfix notation $[\vec{P}, \vec{n}, \vec{k}]$ in order to denote the lists of principal names $\vec{P}$ (list of variables $P_1, \ldots, P_m$), and the lists of variables of nonces and session keys $\vec{n}, \vec{k}$ (as variables). Substitutions are represented in terms of this notation.

2.2 Axioms and Inference Rules

Our inference system consists of the following four classes of axioms and inference rules. The complete list of the axioms and inference rules is presented in Appendix A.2.

(I) Logical inferences with equality
(II) Action properties axioms
(III) Inferences related to the honesty assumption (which are called *honesty inferences*)
(IV) Weakening rules for actions and honesty assumptions

(I) Logical inferences with equality

As logical inferences, we use some structural rules (weakening, contraction, exchange rules of the left hand side, and cut rule) and the equality inference rules. For example, the following inference rules are cut rule (in right below) and a typical equality inference rule which we often use (in left below). (Here t is any term and x is a variable.)

$$\frac{\Gamma \vdash [\vec{\alpha}]\varphi \quad \varphi, \Delta \vdash [\vec{\alpha}]\psi}{\Gamma, \Delta \vdash [\vec{\alpha}]\psi}\ \textbf{Cut} \qquad \frac{\Gamma \vdash [\vec{\alpha}]x = t \quad \Delta \vdash [\vec{\alpha}]\varphi}{\Gamma, \Delta \vdash [\vec{\alpha}]\varphi[t/x]}\ \textbf{Eq}$$

We also introduce the following inference (*substitution rule*) as a logical inference rule.

$$\frac{\Gamma \vdash [\vec{\alpha}]\varphi}{\Gamma[t/x] \vdash [\vec{\alpha}[t/x]]\varphi[t/x]}\ \textbf{Subst}$$

(II) Action properties axioms

Action properties axioms are the *axioms about actions* and the *axioms for relationship between properties* in the sense of [11]. Our proposed axioms are listed in

Appendix A.2. However, our framework does not depend on a specific set of axioms in this category. The followings are some examples of our action properties axioms.

Axioms about primitive actions:

$\vdash [\alpha_1^P; \cdots; \alpha_n^P]\alpha_i^P$ (for any principal P and for any $i = 1, \ldots, n$.)

Nonce Verification (public key):

$(PK(k, Q)), (fresh(m)), (P\ receives\ m'(\{m\}^*_{k^{-1}})) \vdash (Q\ sends\ m'')$

(Here $\{m\}_{K^{-1}} \sqsubseteq m', m''$.)

Note that Nonce Verification is a formalization of the *Incoming tests* of *Authentication tests* based *Strand space* method introduced by [13] (cf. also [12]). On the other hand, we need a non-monotonic property equivalent to the notion of "*uniquely originate*" (in the sense of [13]) to formalize *Outgoing tests*. This formalization is given by using the property "*firstly sends*" in [15].

(III) Honesty inferences

In terms of the classes (I) and (II) of axioms introduced above, we can derive some actions performed by Q from another principal P's viewpoint. For example, we can derive "P knows that Q actually performed a sending action in a current run" from information about encrypted keys or fresh nonces, etc. included in the received message. However, to derive Q's other actions, P may assume Q's honesty and may use P's knowledge about Q's role in the protocol. For example, if P assumes that Q is honest and that P knows that Q sends the message m in the current run, then P can derive that Q also performed a previous action defined by Q's role. That is because Q should not send message m if Q does not perform all previous actions of his/her role.

For formalizing such an inference, compositional logic in [11, 6, 7] uses a special inference aimed at a conclusion of the form $Honest(Q) \supset \varphi$. On the other hand, in our system, inferences on honesty are formalized by the following inference rules, called *honesty inferences*. The central idea of ours is to separate Q's role into his/her primitive actions, and use a predicate of the form $Honest(\vec{\alpha}^Q)$ as an assumption where $\vec{\alpha}^Q$ is a part of his/her role. In this framework, Q's actions are derived directly from a corresponding (often minimal) part of his/her role.

Our honesty inferences are as follows.

Substitution (receives):

$$\frac{\Gamma \vdash [\vec{\alpha}]_P\ Q\ receives\ m[t/x]}{\Gamma, Honest(Q\ receives\ m) \vdash [\vec{\alpha}]_P\ x = t}\ \mathbf{Hon(Subst)}$$

(Here t is a constant, and x is a variable which has the same sort as t.)

We also admit an inference rule obtained from the above rule replacing "*receives*" with "*sends*".

The intended meaning of the inference rules is that if "Q knows that a principal P receives (or sends, resp.) a message m with some concrete values t (i.e., $m[t/x]$)", and if "P assumes that Q is honest and follows a receiving (or sending, resp.) action of message m", then we can conclude "P knows that x should be t".

Matching:

$$\frac{\Gamma \vdash [\vec{\alpha}]_P \ (Q \ sends \ m)}{\Gamma, Honest(Q \ sends \ m', m) \vdash [\vec{\alpha}]_P \ (Q \ sends \ m')} \ \textbf{Hon(Match)}$$

(Here $m \sqsubseteq m'$.)

The intended meaning of this inference rule is that if "P knows that Q sends a message m" and if "P assumes that Q is honest and follows the sending action $Q \ sends \ m'$ containing m", then we can conclude "P knows that Q has sent m'". This inference holds whenever the following additional condition is satisfied: "the set of honesty assumptions does not include any other Q's sending action of a message containing m as a subterm". This means that the formula "$Q \ sends \ m'$" appearing in the lower sequent is non-monotonic. Thus, to keep this formula monotonic, we restrict all applications of honesty inferences and of weakening rule for honesty assumptions (explained in the next item (IV)) so as to preserve this condition. More formally, we extend the language by introducing a new predicate $Honest(\alpha, m)$ (here the usual honesty assumption of the form $Honest(\alpha)$ previously introduced can be regarded as a special case that m is empty), and all applications of honesty inferences and the weakening rule for honesty assumptions are restricted by the following condition (denoted by ($\sharp$)).

($\sharp$) Both honesty assumptions $Honest(Q \ sends \ m', m)$ and $Honest(Q \ sends \ m'')$ (with $m \sqsubseteq m''$) do not appear in the left hand side of the lower sequent.

Note that we do not admit a rule obtained from the Matching rule above by replacing "*sends*" with "*receives*", because even if we assume principal Q is honest and follows a part of role $\vec{\alpha}^Q$, we cannot derive that Q receives only the messages following $\vec{\alpha}^Q$.

Deriving another action (sends):

$$\frac{\Gamma \vdash [\vec{\alpha}]_P \ Q \ sends \ m}{\Gamma, Honest(Q \ receives \ m'; Q \ sends \ m) \vdash [\vec{\alpha}]_P \ Q \ receives \ m'} \ \textbf{Hon(Role)}$$

We also admit an inference rule obtained from the above rule by replacing "*receives*" with "*sends*" or "*generates*".

The intended meaning of this inference rule is that if "P knows that Q actually sends (or receives) a message m and Q follows a sequence of primitive actions $Q \ receives \ m'; Q \ sends \ m$", then "$Q$ actually performs action $Q \ receives \ m'$".

(IV) Weakening rules for honesty assumptions and for actions

The following inferences are *weakening rules* for *honesty assumptions* (in left below) and for *performed actions* (in right below).

$$\frac{\Gamma, Honest(\vec{\alpha}^Q; \vec{\alpha}'^Q) \vdash [\vec{\beta}]_P\ \varphi}{\Gamma, Honest(\vec{\alpha}^Q; \alpha''^Q; \vec{\alpha}'^Q) \vdash [\vec{\beta}]_P\ \varphi}\ \mathbf{W(Hon)} \qquad \frac{\Gamma \vdash [\vec{\alpha}; \vec{\alpha}']_P\ \varphi}{\Gamma \vdash [\vec{\alpha}; \alpha''; \vec{\alpha}']_P\ \varphi}\ \mathbf{W(Act)}$$

As we have mentioned in the explanation of Matching rule of honesty inferences, weakening rule for honesty assumptions should satisfy the ($\sharp$) condition so as to keep the correctness of Matching rule already applied in a proof.

In our system, free applications of the weakening rules are restricted by only ($\sharp$) to keep the monotonicity of predicate *sends*. Of course, if we eliminate the predicate *sends*, all of our predicates are completely monotonic and then we should restrict no application of the weakening rules. However, this property is indispensable to prove protocol correctness. In other words, our choice of predicates is one of the simplest formalism to prove the aimed property in this paper. However, as we have mentioned in Section 1, if some non-monotonic predicates such as "*Source*" in [11] or "$Fresh$" or "$HasAlone$" in [6, 7] are used in our framework, some additional conditions for weakening and honesty inferences should be required. In the subsequent paper [15] of ours, we discuss what kind of additional conditions are required to introduce such non-monotonic properties.

In this paper, we restrict our attention to the protocol which does not include any *duplication of atomic actions*. We assume that each principal in a protocol does not send nor receive the same message twice. This assumption seems to be reasonable because in a protocol including such a duplication, a receiver of the same messages cannot distinguish one from another. Our inference system is sound under this assumption. See Section 4 for a more formal discussion of soundness.

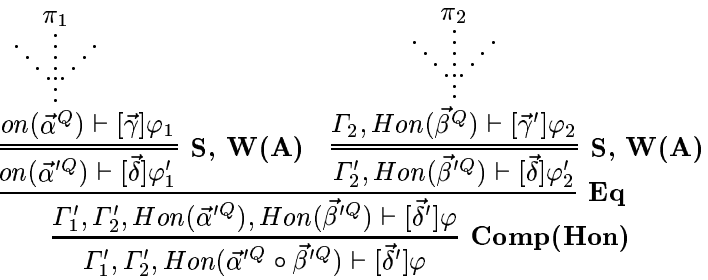
Composing steps in our system:

By using the contraction rule for commutative conjunction (",") in (I) and weakening rules in (IV), operations for composition of honesty assumptions are interpreted by the following derived rule (called **Comp(Hon)**).

$$\cfrac{\cfrac{\Gamma, Hon(\vec{\alpha}^Q), Hon(\vec{\beta}^Q) \vdash [\vec{\gamma}]\varphi}{\Gamma, Hon(\vec{\alpha}^Q \circ \vec{\beta}^Q), Hon(\vec{\alpha}^Q \circ \vec{\beta}^Q) \vdash [\vec{\gamma}]\varphi}\ \mathbf{Weak(\ ;\ )}}{\Gamma, Hon(\vec{\alpha}^Q \circ \vec{\beta}^Q) \vdash [\vec{\gamma}]\varphi}\ \mathbf{Cont(\ ,\ )}$$

Here the notation $\vec{\alpha}^Q \circ \vec{\beta}^Q$ is a result of *order preserving merge* of sequence $\vec{\alpha}^Q$ and $\vec{\beta}^Q$. That is, $\vec{\alpha}^Q \circ \vec{\beta}^Q$ is a sequence of actions which includes all actions both in $\vec{\alpha}^Q$ and $\vec{\beta}^Q$, and preserving the order. (For example, $\alpha_3; \alpha_1; \alpha_2; \alpha_4; \alpha_3$ and $\alpha_1; \alpha_2; \alpha_3; \alpha_4$ are order preserving merges of two lists $\alpha_1; \alpha_2; \alpha_3$ and $\alpha_3; \alpha_4$.)

This derived rule is useful to prove properties of a composed protocol by reusing proofs of its components as follows. Assume that there are two proofs π_1 and π_2, whose end sequents are $\Gamma_1, Hon(\vec{\alpha}^Q) \vdash [\vec{\gamma}]\varphi_1$ and $\Gamma_2, Hon(\vec{\beta}^Q) \vdash [\vec{\gamma}']\varphi_2$, respectively. From these proofs, in our inference system we can get a composed proof by adding some inferences as follows.



Step 1 (Substitutions): For the end sequents of π_1 and π_2, we apply some substitution rules and weakening rules so that each $\vec{\gamma}$ and $\vec{\gamma}'$ becomes the same action $\vec{\delta}$, where $\vec{\delta} = \vec{\gamma} \circ \vec{\gamma}'$. Here Γ_i', $\vec{\alpha}'$ ($\vec{\beta}'$, resp.) and φ_i' (for each $i = 1, 2$) are results of the substitutions, respectively.
Then, we apply an equality inference or cut rule (the above derivation is a case of equality inference). Here $[\vec{\delta}']\varphi$ is a result of $[\vec{\delta}']\varphi_1'$ and $[\vec{\delta}']\varphi_2'$ by equality inference.

Step 2 (Order preserving merge): We apply the composition rule for honesty assumptions (**Comp(Hon)**) to get the proof of a property φ about a composed protocol $\vec{\alpha}' \circ \vec{\beta}'$ which is an order preserving merge of $\vec{\alpha}$ and $\vec{\beta}$.

In the next section, we show a concrete example of this process.

3 An Example of Correctness Proof

In this section, we provide a case study of our compositional treatment of honesty assumptions. As an example we show a proof of the agreement property (in the sense of Woo-Lam [19]) of the *ISO-9798-3 protocol* [16]. This property is proved by the composition of freshness proof for *Diffie-Hellman protocol* [8] and authentication proof for *Challenge Response protocol*, which is already proved in [6, 7].

First, we show our interpretation of composing steps of the ISO 9798-3 protocol by using an informal description. (The notations are also used in the formal proof shown below.)

An informal description of composition of the protocols:

The following two protocols are informal descriptions of *the Diffie-Hellman Protocol* (denoted by Π) and *the Challenge Response Protocol* (denoted by Π'). Here we omit principals' names appearing in each message for readability. In this example, we suppose that in the Challenge Response protocol principals P and Q do not generate m and n as fresh values, respectively (cf. [6, 7]).

The Diffie-Hellman protocol: Π	The challenge response protocol Π'
1 $(\alpha_1^P; \alpha_2^P, \beta_1^Q)$. $P \to Q$: g^P	1′ $(\alpha_1'^P, \beta_1'^Q)$. $P \to Q$: m
2 $(\beta_2^Q; \beta_3^Q, \alpha_3^P)$. $Q \to P$: g^Q	2′ $(\beta_2'^Q, \alpha_2'^P)$. $Q \to P$: $n, \{n, m\}_{K_Q^{-1}}$
	3′ $(\alpha_3'^P, \beta_3'^Q)$. $P \to Q$: $\{m, n\}_{K_P^{-1}}$

In our interpretation, these protocols are composed by the following two steps. (These steps correspond to Composing steps in Section 2.2.)

Step 1. Substitutions: by replacing g^Q with $\langle g^Q, \{g^Q, g^P\}_{K_Q^{-1}}\rangle$ in the Diffie-Hellman protocol, and by replacing g^P with m and g^Q with n in the Challenge Response protocol, we get new protocols Π'' and Π''' as follows.

$$\begin{array}{l|l}
\Pi'' = \Pi[\langle g^Q, \{g^Q, g^P\}_{K_Q^{-1}}\rangle / g^Q] & \Pi''' = \Pi'[g^P/m, g^Q/n] \\
\hline
1'' \ (\alpha_1''^P; \alpha_2''^P, \beta_1''^Q).\ P \to Q\colon g^P & 1''' \ (\alpha_1'''^P, \beta_1'''^Q).\ P \to Q\colon g^P \\
2'' \ (\beta_2''^Q; \beta_3''^Q, \alpha_3''^P). & 2''' \ (\beta_2'''^Q, \alpha_2'''^P).\ Q \to P\colon g^Q, \{g^Q, g^P\}_{K_Q^{-1}} \\
\quad Q \to P\colon g^Q, \{g^Q, g^P\}_{K_Q^{-1}} & 3''' \ (\alpha_3'''^P, \beta_3'''^Q).\ P \to Q\colon \{g^P, g^Q\}_{K_P^{-1}}
\end{array}$$

Here $\alpha_2''^P = \alpha_1'''^P$, $\alpha_3''^P = \alpha_2'''^P$, $\beta_1''^Q = \beta_1'''^Q$ and $\beta_3''^Q = \beta_2'''^Q$.

Step 2. Order preserving merge: by the composition of protocols Π'' and Π''', we get the ISO-9798-3 protocol as follows.

$$\begin{array}{l}
\underline{\text{protocol } (\Pi'' \circ \Pi''')} \\
1'' \ (\alpha_1''^P; \alpha_1'''^P, \beta_1''^Q).\ P \to Q\colon g^P \\
2'' \ (\beta_2''^Q; \beta_3''^Q, \alpha_2'''^P).\ Q \to P\colon g^Q, \{g^Q, g^P\}_{K_Q^{-1}} \\
3''' \ (\alpha_3'''^P, \beta_3'''^Q).\qquad P \to Q\colon \{g^P, g^Q\}_{K_P^{-1}}
\end{array}$$

The notation $\Pi \circ \Pi'$ denotes a result of an *order-preserving merge* of lists Π and Π'.

From now, we give a formal proof of the agreement property for the ISO 9798-3 protocol. This property is stated informally as follows.

Agreement property from A's view: Assume that a principal A follows the initiator's role of the protocol communicating with B, and that the responder, say Q, honestly follows his/her role. If A completes a run of the protocol using values N_1 and N_2, then A knows that B actually performs as the responder Q's role communicating with A using the same values N_1 and N_2.

In the following example, we omit the subscriptions of names P and Q from each meta-symbols $\alpha_i^P, \alpha_i'^P, \ldots$ and $\beta_j^Q, \beta_j'^Q, \ldots$, respectively.

Proving process of the agreement property from initiator's view for the ISO 9798-3 protocol:

First for the Diffie-Hellman protocol, the following sequent is provable by using Axiom about primitive actions.

$$\vdash [\alpha_1; \alpha_2]_A fresh(g^A) \tag{1}$$

On the other hand, for the Challenge Response protocol, the following sequents are also provable. (The proving process of these sequent are shown in [15].)

$$fresh(N_1), Honest((\beta_1'; \beta_2'; \beta_3')) \vdash [\alpha_1'; \alpha_2'; \alpha_3']_A B \textit{ receives } \langle a, b, N_1 \rangle \quad (2)$$

$$fresh(N_1), Honest((\beta_1'; \beta_2'; \beta_3')) \vdash [\alpha_1'; \alpha_2'; \alpha_3']_A B \textit{ sends } \langle b, a, N_2, \{N_2, N_1, a\}_{K_B^{-1}} \rangle \quad (3)$$

From (2) and (3) we prove the agreement property of the Challenge Response protocol. However, in our logic, a non-commutative conjunct appears only in the left hand side of a sequent, then we cannot express directly the agreement property. That is, we cannot state that "B performs the following actions in order: receiving $\langle a, b, N_1 \rangle$ and then sending $\langle b, a, N_2, \{N_2, N_1, a\}_{K_B^{-1}} \rangle$" from A's view. Nevertheless, if we assume Q honestly follows his/her role (i.e., Q follows the sequence of parameterized actions in order: he/she first receives $\langle p, q, m \rangle$ and then sends $\langle q, p, n, \{n, m, p\}_{K_Q^{-1}} \rangle$), and if A knows B actually performs the actions corresponding his/her role, then A can know the order of B's actual actions by matching. In other words, information about ordering of actions performed by an honest principal is implicitly contained in the honesty assumptions. Therefore, if we must formalize a derivation of the agreement property, we can formalize it by introducing the following inference rule.

$$\frac{\Gamma, Hon(\vec{\alpha}^Q) \vdash [\vec{\beta}]_A \ B \ act_1 \ \sigma m_1 \quad \Gamma, Hon(\vec{\alpha}^Q) \vdash [\vec{\beta}]_A \ B \ act_2 \ \sigma m_2 \qquad \Gamma, Hon(\vec{\alpha}^Q) \vdash [\vec{\beta}]_A \ \vec{x} = \vec{t}}{\Gamma, Hon(\vec{\alpha}^Q) \vdash [\vec{\beta}]_A \ (B \ act_1 \ \sigma m_1; B \ act_2 \ \sigma m_2)}$$

where each act_1 and act_2 is a primitive action of receiving, sending, or generating, and σ is $[\vec{t}/\vec{x}]$, and these satisfy the following conditions:

- $\vec{\alpha}^Q$ includes primitive actions α_1^Q and α_2^Q, where α_1^Q precedes α_2^Q.
- If $act_i \ \sigma m_i$ (for each $i = 1, 2$) is a sending action, then α_i^Q is also "Q *sends* m_i". (The case of receiving is the same as sending.)
- If $act_i \ \sigma m_i$ is a generating action, then α_i^Q is also "P *generates* x" with $\sigma x = m_i$.

Therefore, from the above results of (2) and (3), it is clear that the agreement property from A's view is provable in the extended system. Then, the following sequent is provable.

$$fresh(N_1), Honest((\alpha_1'; \alpha_2'; \alpha_3')) \vdash [\beta_1'; \beta_2'; \beta_3']_A \ Agree_B \quad (4)$$

(Here the statement $Agree_B$ is the abbreviation of "B *receives* $\langle a, b, N_1 \rangle$; B *sends* $\langle b, a, N_2, \{N_2, N_1, a\}_{K_B^{-1}} \rangle$", which represents B's actions guaranteeing the agreement for B.)

From now, by composing proofs of (1) and (4), we prove our aimed property.

First, following the procedure of Step 1, we substitute g^P for m and g^Q for n, respectively, in the proofs of (1), and also substitute $\langle g^Q, \{g^Q, g^P\}_{K_Q^{-1}} \rangle$ for g^Q in the proofs of (4) to get the following sequents.

$$\vdash [\beta_1''; \beta_2'']_A \; fresh(g^A) \tag{5}$$

$$fresh(g^A), Honest((\alpha_1'''; \alpha_2'''; \alpha_3''')) \vdash [\beta_1'''; \beta_2'''; \beta_3''']_A \; Agree_B[g^A/N_1, g^B/N_2] \tag{6}$$

Then, by applying weakening rules for actions to (5) and (6), respectively, we get the following sequents.

$$\vdash [\beta_1''; \beta_2''; \beta_3''; \beta_3''']fresh(g^A) \tag{7}$$

$$fresh(g^A), Honest((\alpha_1'''; \alpha_2'''; \alpha_3''')) \vdash [\beta_1''; \beta_1'''; \beta_2'''; \beta_3''']_A \; Agree_B[g^A/N_1, g^B/N_2] \tag{8}$$

Since $\beta_2'' = \beta_1'''$ and $\beta_3'' = \beta_2'''$, $\beta_1''; \beta_2''; \beta_3''; \beta_3'''$ in (7) and $\beta_1''; \beta_1'''; \beta_2'''; \beta_3'''$ in (8) are the same action. Then by applying the cut rule to (7) and (8), we get a new proof of the following sequent.

$$Honest((\alpha_1'''; \alpha_2'''; \alpha_3''')) \vdash [\beta_1''; \beta_1'''; \beta_2'''; \beta_3''']_A \; Agree_B[g^A/N_1, g^B/N_2] \tag{9}$$

This is a proof of agreement property for the ISO-9798-3 protocol from P's view.

4 Trace Semantics and Soundness of the System

In this section we give a semantics for our inference system. We give the definition of our semantics (in Section 4.1) and a sketch of soundness proof for our system (in Section 4.2).

4.1 Trace Semantics

The basic notion of our semantics is *primitive state* of the form "principal P has information m", and denoted by $P(m), Q(m), \ldots$. We also introduce a special kind of primitive state "message m sent by P is currently transmitted through the network", and denoted by $Net(m, P)$. A *state* is a multiset of primitive states and a *trace* is a finite sequence of states. We use the following notations. The letters $\mathtt{s}, \mathtt{s}', \ldots$ are used to denote traces, and $s_i, s_i', \ldots$ to denote the i-th elements of $\mathtt{s}, \mathtt{s}', \ldots$, respectively. The number i is called the *position* of s_i in $\mathtt{s}$. We also introduce some notions related to traces. We say $s_i \in \mathtt{s}'$ (where $\mathtt{s}' = s_1', \ldots, s_n'$) if $s_i = s_j'$ for some $j = 1, \ldots, n$. For a sequence $\mathtt{s} = s_1, \ldots, s_n$ and for $s_i, s_j \in \mathtt{s}$, we denote $s_i \leq_{\mathtt{s}} s_j$ if $i \leq j$. For traces $\mathtt{s}$ and $\mathtt{s}'$, if $s_i \in \mathtt{s}'$ for all $s_i \in \mathtt{s}$ and if $\forall s_i, s_j \in \mathtt{s}.(s_i \leq_{\mathtt{s}} s_j \Rightarrow s_i \leq_{\mathtt{s}'} s_j)$, we say $\mathtt{s}'$ is an *extension* of $\mathtt{s}$ and denote it by $\mathtt{s} \subseteq \mathtt{s}'$.

Here we only consider the traces satisfying the following condition: for any $s_i, s_j \in \mathtt{s}$, if $s_i <_{\mathtt{s}} s_j$ and $P(m) \in s_i$ then $P(m) \in s_j$. In other words, we consider only traces where, once information is possessed by a principal, it does not disappear in his/her memory.

We denote the number of occurrence of primitive state $P(m)$ in a state s_i by $\| s_i \|_{P(m)}$ (e.g. if $s_i = \{P(m), P(m), Q(m)\}$, then $\| s_i \|_{P(m)} = 2$). $Key(P, s_i)$ is

used to denote the set of key possessed by principal P at position s_i. For messages m, m' and a set of keys $\{k_1, \ldots, k_l\}$, "m is *accessible* in m' with keys $\{k_1, \ldots, k_l\}$" (denoted by $m \in_{\{k_1,\ldots,k_l\}} m'$) is the reflexive-transitive closure satisfying the following conditions: (i) $m_i \in_{\{k_1,\ldots,k_l\}} \langle m_1, \ldots, m_n \rangle$ for some $i = 1, \ldots, n$, (ii) $m \in_{\{k_1,\ldots,k_l\}} \{m\}_{k_j}$ for some $j = 1, \ldots, l$.

By means of the notion of trace, truth conditions for predicates of our syntax are defined as follows. We denote the basic semantic relation "φ is true at state s_i in $\mathtt{s}$" by "$\models_{\langle \mathtt{s},i \rangle} \varphi$".

Truth condition for predicates:

- $\models_{\langle \mathtt{s},i \rangle} PK(P,k)$ iff $P(k'), KeyPair(k,k') \in s_i$ and $\forall X \neq P.(X(k') \notin s_i)$.
- $\models_{\langle \mathtt{s},i \rangle} P \overset{k}{\leftrightarrow} Q$ iff $P(k), Q(k) \in s_i$ and $\forall X \neq P, Q.(X(k) \notin s_i)$.
- $\models_{\langle \mathtt{s},i \rangle} t = t'$ (for any terms t and t') iff $s_i[t/x] = s_i[t'/x]$.
- $\models_{\langle \mathtt{s},i \rangle} P \textit{ sends } m$ iff $P(m) \in s_{i-1}$, $Net(m,P) \notin s_{i-1}$ and $Net(m,P) \in s_i$.
- $\models_{\langle \mathtt{s},i \rangle} P \textit{ receives } m(\{m_1\}^*_{k_1}, \ldots, \{m_n\}^*_{k_n})$ iff $\exists X.\ (Net(m,X) \in s_{i-1}$ and $Net(m,X) \notin s_i)$ and $\| s_{i-1} \|_{P(m)} + 1 = \| s_i \|_{P(m)}$, and $\{m_j\}_{k_j} \in_{Key(P,s_i)} m$ and $\| s_{i-1} \|_{P(m_j)} + 1 = \| s_i \|_{P(m_j)}$ for each $j = 1, \ldots, n$.
- $\models_{\langle \mathtt{s},i \rangle} P \textit{ generates } m$ iff $P(m) \notin s_{i-1}$ and $P(m) \in s_i$.
- $\models_{\langle \mathtt{s},i \rangle} fresh(m)$ iff $\exists X \exists n.(X(n) \notin s_{i-1}$ and $X(n) \in s_i)$ and $n \sqsubseteq m$.
- $\models_{\langle \mathtt{s},i \rangle} \alpha_1; \cdots; \alpha_n$ iff $\models_{\langle \mathtt{s},i_1 \rangle} \alpha_1$ and $\cdots$ and $\models_{\langle \mathtt{s},i_n \rangle} \alpha_n$, and $i_1 \leq \cdots \leq i_n \leq s_i$.

Next, the definition "φ is true for trace $\mathtt{s}$" (denoted by $\models_{\mathtt{s}} \varphi$) is as follows.

- $\models_{\mathtt{s}} \beta$ iff $\forall s_i \in \mathtt{s}.(\models_{\langle \mathtt{s},i \rangle} \beta)$
  (where $\beta = PK(P,k)$ or $P \overset{k}{\leftrightarrow} Q$, or $t = t'$.)
- $\models_{\mathtt{s}} fresh(m)$ iff $\exists s_i \in \mathtt{s}.(\models_{\langle \mathtt{s},i \rangle} fresh(m))$.
- $\models_{\mathtt{s}} \alpha_1; \cdots; \alpha_n$ iff $\exists s_i \in \mathtt{s}.(\models_{\langle \mathtt{s},i \rangle} \alpha_1; \cdots; \alpha_n)$
  (where each α_i is an action predicate.)

We define that $\models_{\mathtt{s}} \Gamma$ iff "$\models_{\mathtt{s}} \vec{\alpha}$ and ... and $\models_{\mathtt{s}} \vec{\beta}$, and $\models_{\mathtt{s}} \theta_i$ for each $i = 1, \ldots, n$" (where $\Gamma = \vec{\alpha}, \ldots, \vec{\beta}, \theta_1, \ldots, \theta_n$). By the above definition, it is clear that for any φ if $\models_{\mathtt{s}} \varphi$ then $\models_{\mathtt{s}'} \varphi$ for any $\mathtt{s} \subseteq \mathtt{s}'$.

In terms of the above definitions, we define the basic form of assertion as true under $\mathtt{s}$, that is to say:

$$Honest(\alpha_1^P); \cdots; Honest(\alpha_n^P), \ldots Honest(\alpha_1^Q); \cdots; Honest(\alpha_k^Q), \ldots, \Gamma \models_{\mathtt{s}} [\vec{\alpha}]\varphi$$

if and only if the following is satisfied (where φ is a single action or non-action predicate).

If C1 $\forall i \leq n.\forall i' < i.(\models_{\mathtt{s}} \alpha_i^P \Rightarrow \models_{\mathtt{s}} \alpha_{i'}^P)$, and
$\forall j \leq k.\forall j' < j.(\models_{\mathtt{s}} \alpha_j^Q \Rightarrow \models_{\mathtt{s}} \alpha_{j'}^Q)$,
C2 $\exists \mathtt{s}'.(\mathtt{s} \subseteq \mathtt{s}' \wedge \forall i \leq n.(\models_{\mathtt{s}'} \alpha_i) \wedge \forall j \leq k.(\models_{\mathtt{s}'} \alpha_j))$,
C3 $\models_{\mathtt{s}} \Gamma$,
C4 $\models_{\mathtt{s}} \vec{\alpha}$,
then $\models_{\mathtt{s}} \varphi$.

Here for each predicate $Honest(\alpha_i^X)$, if it is of the form $Honest(\alpha_i^X, m_i^X)$ for $X = P, Q$ and for $i = 1, \ldots, n$ or $1, \ldots, k$ (i.e., m_i^X is not empty), then the following condition is also satisfied:

C5 $\forall m'.((m' \sqsupseteq m_i^X) \wedge (m' \neq m'') \wedge (\alpha_i^X = X \; sends \; m'')$
$\Rightarrow \forall \mathtt{s}' \sqsupseteq \mathtt{s}.(\not\models_{\mathtt{s}'} X \; sends \; m'))$.

We need this additional condition for the following reason: first recall that $Honest(\alpha_i^X, m_i^X)$ (where m_i^X is not empty term) means "X honestly follows the sending action α_i^X (say, $X \; sends \; m''$) and he/she does not follow any other sending actions of the message m' including m_i^X". Therefore, to satisfy this restriction, we assume $X \; sends \; m''$ is false for any extension $\mathtt{s}'$ of $\mathtt{s}$.

If the above form of assertion is true for any trace $\mathtt{s}$, then this assertion is called *valid* and we omit the subscription $\mathtt{s}$.

Finally, to prove the soundness of our system, we introduce the notion of *duplication of atomic actions in trace* $\mathtt{s}$ as follows. We say "two atomic action formulas α and β are duplicated in trace $\mathtt{s}$", when the following condition is satisfied: "for some $s_i, s_j \in \mathtt{s}$ with $i \neq j$, there exists a substitution σ such that $\sigma\alpha = \sigma\beta$ and that $\models_{\langle \mathtt{s}, i \rangle} \alpha$ and $\models_{\langle \mathtt{s}, j \rangle} \beta$". As we mentioned in Section 2, our inference system is sound under the assumption that no trace includes atomic actions which are duplicated.

Therefore, our soundness theorem proved in the next subsection is stated as follows.

Theorem (Soundness). If a sequent (i.e., a basic form of assertion) S is provable in our inference system, then S is true for any trace $\mathtt{s}$ which includes no duplicated atomic actions.

4.2 Soundness of the System

In this subsection we sketch out a proof of the soundness.

(I) Logical inference rules

Here we give a soundness proof only for **Cut** rule as follows. Proofs for the other rules in this class are similar.

$$\frac{\Gamma \vdash [\vec{\alpha}]\varphi \quad \varphi, \Delta \vdash [\vec{\alpha}]\psi}{\Gamma, \Delta \vdash [\vec{\alpha}]\psi} \; \mathbf{Cut}$$

Assume that the upper sequents are both valid. That is, for any $\mathtt{s}$ and $\mathtt{s}'$, (i) if $\models_{\mathtt{s}} \Gamma$ and $\models_{\mathtt{s}} \vec{\alpha}$, then $\models_{\mathtt{s}} \varphi$, and (ii) if $\models_{\mathtt{s}'} \varphi$ and $\models_{\mathtt{s}'} \Delta$ and $\models_{\mathtt{s}'} \vec{\alpha}$, then $\models_{\mathtt{s}'} \psi$

hold. Assume that for any $\mathtt{s}''$, $\models_{\mathtt{s}''} \Gamma$ and $\models_{\mathtt{s}''} \Delta$ and $\models_{\mathtt{s}''} \vec{\alpha}$. Then by (i), $\models_{\mathtt{s}''} \varphi$ holds. Then by (ii), $\models_{\mathtt{s}''} \psi$ holds. Therefore the lower sequent is also valid.

(II-1) Axioms about primitive actions:

$$\vdash [\alpha_1^P; \cdots; \alpha_n^P]\alpha_i^P \qquad (\text{for } i = 1, \ldots, n.)$$

This sequent is valid if, for any $\mathtt{s}$, if $\models_{\mathtt{s}} \alpha_1^P$, ..., $\models_{\mathtt{s}} \alpha_n^P$ then $\models_{\mathtt{s}} \alpha_i^P$ for any $i = 1, \ldots, n$. This condition immediately holds by the definition.

(II-2) Axioms for relationship between properties:
Here we show only the case of Freshness 1 and 2, and Nonce Verification. Proofs for the other axioms are similar.

Freshness 1:

$$P \textit{ generates } m \vdash fresh(m)$$

Assume that $\models_{\mathtt{s}} P \textit{ generates } m$ for any $\mathtt{s}$. That is, $\exists s_i \in \mathtt{s}.((P(m) \notin s_{i-1}) \wedge (P(m) \in s_i))$ holds. Then, $\exists X \exists n.((X(n) \notin s_{i-1}) \wedge (X(n) \in s_i))$ with $n \sqsubseteq m$ holds. This is the truth condition for $fresh(m)$.

Freshness 2:

$$fresh(m) \vdash fresh(m') \qquad (\text{where } m \sqsubseteq m')$$

Assume that $\models_{\mathtt{s}} fresh(m)$ for any $\mathtt{s}$. That is, $\exists s_i \in \mathtt{s} \exists X \exists m''.((X(m'') \notin s_{i-1}) \wedge (X(m'') \in s_i))$ with $m'' \sqsubseteq m$. By assumption of $m \sqsubseteq m'$, $m'' \sqsubseteq m'$ also holds. Therefore is the truth condition for $fresh(m')$ is satisfied.

Nonce Verification:

$$(PK(k, Q)), (fresh(m)), (P \textit{ receives } m'(\{m\}^*_{k^{-1}})) \vdash Q \textit{ sends } m''$$
$$(\text{where } \{m\}_{k^{-1}} \sqsubseteq m', m''.)$$

Assume that all atoms in the left hand side of this axiom are valid. That is, for any $\mathtt{s}$, (i) $\forall s_i \in \mathtt{s}.((Q(k^{-1}) \in s_i) \wedge \forall X \neq Q.(X(k^{-1}) \notin s_i))$, (ii) $\exists s_i \in \mathtt{s} \exists X \exists n.((X(n) \notin s_{i-1}) \wedge (X(n) \in s_i))$, and (iii) $\exists s_i \in \mathtt{s} \exists X.((Net(m', X) \in s_{i-1}) \wedge (\|s_{i-1}\|_{P(m')} + 1 = \|s_i\|_{P(m')}) \wedge (\|s_{i-1}\|_{P(m)} + 1 = \|s_i\|_{P(m)}))$. Informally, by (i) and (iii), $\exists s_i \in \mathtt{s}.(Net(m'', Q) \in s_{i-1})$ with $\{m\}_{k^{-1}} \sqsubseteq m''$ holds. That is, $\exists s_j <_{\mathtt{s}} s_i.((Net(m', Q) \notin s_j) \wedge (Q(m') \in s_j))$. Then, by (ii) $\exists s_k \in \mathtt{s}.((s_k <_{\mathtt{s}} s_i) \wedge (Net(m', Q)) \wedge (Q(m') \in s_k))$. This is the truth condition for $Q \textit{ sends } m''$.

(III) Honesty Inferences:

(1) Substitution:

$$\frac{\Gamma \vdash [\vec{\alpha}]Q \textit{ sends } m[t/x]}{\Gamma, Honest(Q \textit{ sends } m) \vdash [\vec{\alpha}]x = t}$$

(where t is a constant and x is a variable which has the same sort as t.)

Assume that the upper sequent is valid. That is, for any $\mathtt{s}$, "if $\models_{\mathtt{s}} \Gamma$ and if $\models_{\mathtt{s}} \vec{\alpha}$, then $\models_{\mathtt{s}} Q\ sends\ m[t/x]$" holds. Here we also assume that, for any $\mathtt{s}'$, (i) $\models_{\mathtt{s}} \Gamma$ and $\models_{\mathtt{s}} \vec{\alpha}$, and (ii) conditions C1 and C2 for $Honest(Q\ sends\ m)$ hold. By assumption (i), $\models_{\mathtt{s}'} Q\ sends\ m[t/x]$ holds. By assumption (ii), because the condition C2 for the honesty assumption holds, there exists a trace $\mathtt{s}'' \supseteq \mathtt{s}'$ such that $\models_{\mathtt{s}''} Q\ sends\ m$ holds, and under such $\mathtt{s}''$, $\models_{\mathtt{s}''} Q\ sends\ m[t/x]$ also holds. Therefore for some $s_i, s_j \in \mathtt{s}$, $\models_{\langle \mathtt{s}'', i\rangle} Q\ sends\ m$ and $\models_{\langle \mathtt{s}'', j\rangle} Q\ sends\ m[t/x]$. Here by the assumption such that $\mathtt{s}''$ does not include any duplicated atomic actions, for some $s_i \in \mathtt{s}''$, $s_i = s_i[t/x]$ and $\models_{\langle \mathtt{s}'', i\rangle} Q\ sends\ m$ and $\models_{\langle \mathtt{s}'', i\rangle} Q\ sends\ m[t/x]$ hold. Here, it is easy to show that $\forall s_j \in \mathtt{s}''.(s_j = s_j[t/x])$ by the definition of traces. (Remind that each trace satisfies the condition that for any primitive state of the form $P(m)$, $\forall s_i, s_j \in \mathtt{s}.(s_i < s_j$ and $P(m) \in s_i$ then $P(m) \in s_j).)$ That is, $\models_{\mathtt{s}''} x = t$ holds, and then by $\mathtt{s}' \subseteq \mathtt{s}''$, $\models_{\mathtt{s}'} x = t$ holds. This is the truth condition for the lower sequent.

(2) Matching:

$$\frac{\Gamma \vdash [\vec{\alpha}]Q\ sends\ m}{\Gamma, Honest(Q\ sends\ m', m) \vdash [\vec{\alpha}]Q\ sends\ m'}$$

Assume that the upper sequent is valid. That is, for any $\mathtt{s}$, "if $\models_{\mathtt{s}} \Gamma$ and if $\models_{\mathtt{s}} \vec{\alpha}$, then $\models_{\mathtt{s}} Q\ sends\ m$". Here we also assume that, for any $\mathtt{s}'$, (i) $\models_{\mathtt{s}'} \Gamma$ and $\models_{\mathtt{s}'} \vec{\alpha}$ hold, and (ii) conditions C1, C2 and C5 for $Honest(Q\ sends\ m', m)$ hold. By assumption (i) and the validity of the upper sequent, $\models_{\mathtt{s}} Q\ sends\ m$ holds. By condition C2 of (ii), $\exists s'' \supseteq s'.(\models_{\mathtt{s}''} Q\ sends\ m')$ holds. Moreover, by C5 of (ii), $\forall m''.((m'' \sqsupseteq m) \wedge (m'' \neq m') \Rightarrow \forall \mathtt{s}'' \supseteq \mathtt{s}.(\not\models_{\mathtt{s}''} Q\ sends\ m''))$. That is, $\forall m''.((m'' \sqsupseteq m) \wedge (m'' \neq m') \Rightarrow \neg\exists \mathtt{s}'' \supseteq \mathtt{s}'.(\not\models_{\mathtt{s}''} Q\ sends\ m''))$. Therefore, $\models_{\mathtt{s}'} Q\ sends\ m'$. This is the truth condition for the lower sequent.

(3) Deriving another actions:

$$\frac{\Gamma \vdash [\vec{\alpha}]Q\ sends\ m}{\Gamma, Honest(Q\ sends\ m'; Q\ sends\ m), \vdash [\vec{\alpha}]Q\ sends\ m'}$$

Assume that the upper sequent is valid. That is, for any $\mathtt{s}$, $\models_{\mathtt{s}} \Gamma$ and $\models_{\mathtt{s}} \vec{\alpha}$, then $\models_{\mathtt{s}} Q\ sends\ m$ holds. Here we also assume that, for any $\mathtt{s}'$, (i) $\models_{\mathtt{s}'} \Gamma$ and $\models_{\mathtt{s}'} \vec{\alpha}$, and (ii) conditions C1 and C2 for $Honest(Q\ sends\ m'; Q\ sends\ m)$ hold. By assumption (i) and the validity of upper sequent, $\models_{\mathtt{s}'} Q\ sends\ m$ holds. By condition C1 of (ii), $\models_{\mathtt{s}'} Q\ sends\ m'$ also holds. This is the truth condition for the lower sequent.

(IV) Weakening rules:

$$\frac{\Gamma, Honest(\vec{\alpha}^P; \vec{\alpha}'^P) \vdash [\vec{\beta}]\varphi}{\Gamma, Honest(\vec{\alpha}^P; \alpha''^P; \vec{\alpha}'^P) \vdash [\vec{\beta}]\varphi}\ \mathbf{W(Hon)} \qquad \frac{\Gamma \vdash [\vec{\alpha}^P; \vec{\alpha}'^P]\varphi}{\Gamma \vdash [\vec{\alpha}^P; \alpha''^P; \vec{\alpha}'^P]\varphi}\ \mathbf{W(Act)}$$

(1) Weakening (Honesty): We should only show that, for any $\mathtt{s}$, if $\mathtt{s}$ satisfies the conditions C1 and C2 for $Honest(\vec{\alpha}^P; \alpha''^P; \vec{\alpha}'^P)$, $\mathtt{s}$ also satisfies the conditions C1 and C2 for $Honest(\vec{\alpha}^P; \vec{\alpha}'^P)$. C1 is satisfied, because for any sequence

$\vec{\beta}$, if $\forall \alpha_i, \alpha_j \in \vec{\beta}.((j \leq i) \Rightarrow (\models_{\mathtt{s}} \alpha_i \Rightarrow \models_{\mathtt{s}} \alpha_j))$, then this property also holds for any $\vec{\beta}'$ such that $\vec{\beta}' \subseteq \vec{\beta}$. C2 is also satisfied, because for any $\mathtt{s}' \supseteq \mathtt{s}$ and for any $\vec{\beta}$, $\forall \alpha_i \in \vec{\beta}(\models_{s'} \alpha_i)$ holds, then, for the same $\mathtt{s}'$ at least, this condition also holds for any $\vec{\beta}'$ such that $\vec{\beta}' \subseteq \vec{\beta}$.

(2) Weakening (Actions): We should only show that for any $\mathtt{s}$, if $\models_{\mathtt{s}} \vec{\alpha}; \alpha''; \vec{\alpha}'$ then $\models_{\mathtt{s}} \vec{\alpha}; \vec{\alpha}'$. This immediately follows from the definition of $\models_{\mathtt{s}} \vec{\alpha}; \alpha''; \vec{\alpha}'$.

5 Conclusions

We presented an inference system based on a framework of compositional logic originally introduced by [11, 6, 7]. The main difference between the compositional logic of [11, 6, 7] and ours was the way to formalize inferences on a principal's honesty: while in [11, 6, 7] assumptions on a principal's honesty were represented by the implication of the form $Honest(P) \supset \varphi$, in our framework we divided each honest principal's role into its components (i.e., his/her primitive actions) and introduced some special kinds of inference rules, called *honesty inferences*, to derive a minimal requirement on principal's honesty to conclude a property. Such honesty assumptions were composed during a proving process by using *weakening rules* analogous to the structural rules of traditional logic. For this formalization, the language of our system is restricted to Horn-clauses, in other words we do not use logical negations nor nested implications (nor disjunctions appearing in the right hand side of a sequent) which were used in [11, 6, 7].

We also introduced the distinction between the *monotonic* properties and *non-monotonic* ones. In this paper, by restricting our attention to the monotonic properties, we gave a core inference system and showed a proof of the *agreement property* of the ISO 9798-3 protocol. Such restriction leads to a simplification of the system, because we do not need any restriction on a free application of weakening rules and honesty inferences. However, the use of non-monotonic properties provides us more powerful derivations. In the subsequent work [15] of ours, we show the way to extend our system by introducing non-monotonic properties. As an example, in [15] we introduce the non-monotonic property "P $firstly\_sends$ (m, n)" (which means "P sends a message m containing n as a subterm, and P does not send any other message m' containing n before the sending of m"). This property is useful to derive information about ordering of actions performed by different principals, which cannot be proved in the system of this paper, and by this information we prove *matching conversation* of the *Challenge Response protocol* (cf. [9]), which was originally proved in [6, 7].

Acknowledgments

We would like to express our sincere thanks to Drs. Andre Scedrov and Iliano Cervesato for their invaluable comments and discussions. We also would like to express our sincere thanks to Mrs. Lam Ta-Minh and Pierre Grialou for their helpful comments. Finally, helpful comments from the anonymous reviewers results in improvements to this paper.

References

1. M. Burrows, M. Abadi and R. Needham. A Logic of Authentication. *Technical Report 39*, Digital System Research Center, 1989.
2. I. Cervesato, N.A. Durgin, P.D. Lincoln, J.C. Mitchell and A. Scedrov. A meta-notation for protocol analysis. *12th IEEE Computer Security Foundations Workshop*, 1999.
3. I. Cervesato, N.A. Durgin, P.D. Lincoln, J.C. Mitchell and A. Scedrov. A Comparison between Strand Spaces and Multiset Rewriting for Security Protocol Analysis. M. Okada, B. Pierce, A. Scedrov, H. Tokuda and A. Yonezawa (eds.), *Software Security — Theories and Systems*, Lecture Notes in Computer Science, Hot Topics, vol.2609, Springer-Verlag, pp.356-382, 2003.
4. I. Cervesato, N.A. Durgin, P.D. Lincoln, J.C. Mitchell and A. Scedrov. Multiset rewriting and the complexity of bounded security protocols. *Journal of Computer Security*, vol.12, no.1, pp.677-722, 2004.
5. J. Clark and J. Jacob. A Survey of Authentication Protocol Literature: Version 1.0 (web draft), 1997.
6. A. Datta, A. Derek, J. C. Mitchell and D. Pavlovic. A Derivation System for Security Protocols and its Logical Formalization. *Journal of Computer Security, Special Issue of Selected Papers from CSFW-16*, 2004.
7. A. Datta, A. Derek, J. C. Mitchell and D. Pavlovic. Secure Protocol Composition. *Proceedings of 19th Annual Conference on Mathematical Foundations of Programming Semantics, ENTCS Vol. 83*, 2004.
8. W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, IT-22(6), pp.644-654, 1976.
9. W. Diffie, P. C. van Oorschot and M. J. Wiener. Authentication and authenticated key exchange *Designs, Codes and Cryptography*, vol.2, pp.107-125, 1992.
10. N.A. Durgin, P.D. Lincoln, J.C. Mitchell and A. Scedrov. Undecidability of bounded security protocol. *The 1999 Federated Logic Conference (FLoC '99)*, 11 pages, 1999.
11. N. Durgin, J. Mitchell, and D. Pavlovic. A compositional logic for proving security properties of protocols. *Journal of Computer Security*, vol.11, no.4, pp.677-721, 2003.
12. F. J. T. Fábrega, J. C. Herzog and J. D. Guttman. Strand spaces: Why is a security protocol correct? *Proceedings of the 1998 IEEE Symposium on Security and Privacy*, pp.160-171, 1998.
13. J. D. Guttman and F. J. T. Fábrega. Authentication tests and the structure of bundles. *Theoretical Computer Science*, vol. 283(2), pp.333-380, 2002.
14. K. Hasebe and M. Okada. A Logical Verification Method for Security Protocols Based on Linear Logic and BAN Logic. M. Okada, B. Pierce, A. Scedrov, H. Tokuda and A. Yonezawa (eds.), *Software Security — Theories and Systems*, Lecture Notes in Computer Science, Hot Topics, vol.2609, Springer-Verlag, pp.417-440, 2003.
15. K. Hasebe and M. Okada. Non-monotonic Properties for Proving Correctness in a Framework of Compositional Logic. to appear in the *proceedings of the workshop on Foundations of Computer Security '04 (LICS and ICALP affiliated workshop)*, Turku, Finland, 12 pages, 2004.
16. IEEE. Entity Authentication Mechanisms - part 3: Entity Authentication Using Asymmetric Techniques. Technical report ISO/IEC IS 9798-3, ISO/IEC, 1993.
17. A. J. Menezes, P. C. van Oorschot and S. A. Vanstone. *Handbook of Applied Cryptography*. CRS press, 1996 (fifth printing, 2001).

18. P. Syverson and I. Cervesato. The Logic of Authentication Protocols. *Lecture notes in Computer Science*, Vol. 2171, pp. 63-136, 2001.
19. T. Y. C. Woo and S. S. Lam. Verifying authentication protocols: Methodology and example. *Proceedings of the International Conference on Network Protocols*, 1993.

Appendix

A Inference system

A.1 The language

(I) Sorts and Terms

The language is many sorted. (However sorts are not explicitly indicated in the language.) `Name`, `PublicKey`, `SecretKey`, `SharedKey` and `Nonce` are primitive sorts. (`Key` is used to denote `PublicKey` or `SecretKey` or `SharedKey`.) `Message` is also sort defined below.

The letters A, B, C,... are constants of sort `Name` (i.e., specific principal's names), while the letters P, Q, R,... are variables of sort `Name` (i.e., parameterized principal's names). The capital letters $K, K', \ldots, K_1, K_2, \ldots$ and $N, N', \ldots, N_1, N_2, \ldots$ are constants of sort `Key` and of sort `Nonce`, respectively, while the small letters $k, k', \ldots, k_1, k_2, \ldots$ and $n, n', \ldots, n_1, n_2, \ldots$ are variables of the same sorts as above. All constants and variables of sort `Name` or `Key` or `Nonce` are terms of sort `Message`, and the letters $m, m', \ldots, m_1, m_2, \ldots$ are used to denote terms of the sort `Message`. $\{m\}_K$ (the encryption of m with key K) and $\langle m_1, \ldots, m_n \rangle$ (the concatenation of messages $m_1, \ldots, m_n$) are also terms of sort `Message`, where $\{*\}_K$ and $\langle *, \ldots, * \rangle$ are functions of sort $\texttt{Message} \times \texttt{Key} \to \texttt{Message}$ and of sort $\texttt{Message}^n \to \texttt{Message}$, respectively.

We use the following binary relations as meta-symbols. $m \sqsubseteq m'$ represents that m is subterm of m'.

(II) Basic form of assertion

$$Honest(\alpha_{1_1}^{Q_1}); \cdots; Honest(\alpha_{1_m}^{Q_1}), \ldots,$$
$$Honest(\alpha_{n_1}^{Q_n}); \ldots; Honest(\alpha_{n_m}^{Q_n}), \Gamma \vdash [\vec{\beta}]_P \; \varphi$$

(where Q_i may be the same as Q_j for some $i, j = 1, \ldots, n$.)

- *Action predicates* (performed by P) are as follows.
  - P *generates* m: P generates a nonce or session key m.
  - P *receives* m: P receives a message m.
  - P *sends* m: P sends a message m.
- *Non-action predicates* are as follows.
  - $fresh(n)$: n is a fresh value.
  - $PK(P, k)$: k is a public key of P. (Here k^{-1} denotes the secret key of k.)

- $P \overset{K}{\leftrightarrow} Q$: k is a shared key for P and Q.
- $t = t'$: (usual equality)

- Each $\alpha_{i_j}^{Q_i}$ (for $i = 1, \ldots, n$) is an atomic formula made of an action predicate.
- $\vec{\beta}$ is a sequence of action predicates performed by P.
- φ is a single atomic formula (made of an action or non-action predicate).
- $Honest(\alpha_{i_j}^{Q_i})$: a principal Q_i honestly follows a primitive action $\alpha_{i_j}^{Q_i}$.
- $Honest(\alpha_{i_1}^{Q_i}); \cdots; Honest(\alpha_{i_m}^{Q_i})$: a principal Q_i honestly follows a sequence of primitive actions $\alpha_{i_1}^{Q_i}; \cdots; \alpha_{i_m}^{Q_i}$. (We also use the abbreviation $Honest(\alpha_{i_1}^{Q_i}; \cdots; \alpha_{i_m}^{Q_i})$.)

A.2 Axioms and inference rules

Here each Γ, Δ represents a set of atoms or a sequence of atomic formulas, which may includes honesty assumptions.

(I) Logical inference rules

(1) Structural rules: weakening, contraction and exchange rules in the left hand side, and cut rule (**Cut**) (2) Inference rules for equality (**Eq**) (a typical rule which we often use is presented below), (3) Substitution rule (**Subst**).

$$\frac{\Gamma \vdash [\vec{\alpha}]\varphi \quad \varphi, \Delta \vdash [\vec{\alpha}]\psi}{\Gamma, \Delta \vdash [\vec{\alpha}]\psi}\ \textbf{Cut} \qquad \frac{\Gamma \vdash [\vec{\alpha}]x = t \quad \Delta \vdash [\vec{\alpha}]\varphi}{\Gamma, \Delta \vdash [\vec{\alpha}]\varphi[t/x]}\ \textbf{Eq}$$

$$\frac{\Gamma \vdash [\vec{\alpha}]\varphi}{\Gamma[t/x] \vdash [\vec{\alpha}[t/x]]\varphi[t/x]}\ \textbf{Subst}$$

(II-1) Axioms about primitive actions

$\vdash [\alpha_1^P; \cdots; \alpha_n^P]\alpha_i^P$ (for any $i = 1, \ldots, n$ and for any principal P.)

(II-2) Axioms for relationships between properties

Freshness 1:
$P\ generates\ n \vdash fresh(n)$

Freshness 2: (where $m \sqsubseteq m'$.)
$fresh(m) \vdash fresh(m')$

Nonce Verification: (where $\{m\}_{k^{-1}} \sqsubseteq m', m''$.)
$(PK(k, Q)), (fresh(m)), (P\ receives\ m'(\{m\}_{k^{-1}}^*)) \vdash (Q\ sends\ m'')$

We also admit the axiom obtained by replacing $PK(k, Q)$ with $P \overset{k}{\leftrightarrow} Q$.

Shared secret: (where $K' \sqsubseteq m_1, m_2$.)
$(P\ sends\ \{m_1\}_{K_1}), (P\ sends\ \{m_2\}_{K_2}), (P\ generates\ K'),$
$(P \overset{K_1}{\leftrightarrow} Q), (P \overset{K_2}{\leftrightarrow} R) \vdash (Q \overset{K'}{\leftrightarrow} R)$

(III) Honesty inferences

For (1) Substitution and for (3) Deriving another action, we also admit the inference rules obtained by replacing "*receives*" with "*generates*" or "*sends*", respectively. These rules satisfy the (♯) condition. (See Section 2.2.)

(1) Substitution:

$$\frac{\Gamma \vdash [\vec{\alpha}](Q \; receives \; m[t/x])}{\Gamma, Honest(Q \; receives \; m) \vdash [\vec{\alpha}]x = t} \; \textbf{Hon(Subst)}$$

(where t is a constant and x is a variable which has the same sort of t.)

(2) Matching:

$$\frac{\Gamma \vdash [\vec{\alpha}](Q \; sends \; m)}{\Gamma, Honest(Q \; sends \; m', m) \vdash [\vec{\alpha}](Q \; sends \; m')} \; \textbf{Hon(Match)}$$

(3) Deriving another action in a role:

$$\frac{\Gamma \vdash [\vec{\alpha}](Q \; sends \; m)}{\Gamma, Honest(Q \; receives \; m'; Q \; sends \; m) \vdash [\vec{\alpha}](Q \; receives \; m')} \; \textbf{Hon(Role)}$$

(IV) Weakening rules for actions and honesty assumptions

Weakening rule for honesty assumptions (left below) satisfies (♯) condition.

$$\frac{\Gamma, Honest(\vec{\alpha}^P; \vec{\alpha}'^P) \vdash [\vec{\beta}]\varphi}{\Gamma, Honest(\vec{\alpha}^P; \alpha''^P; \vec{\alpha}'^P) \vdash [\vec{\beta}]\varphi} \; \textbf{W(Hon)} \qquad \frac{\Gamma \vdash [\vec{\alpha}^P; \vec{\alpha}'^P]\varphi}{\Gamma \vdash [\vec{\alpha}^P; \alpha''^P; \vec{\alpha}'^P]\varphi} \; \textbf{W(Act)}$$