# A Completeness Result for BAN Logic

Mika Cohen Mads Dam

*ACCESS Linnaeus Center*
*KTH - Royal Institute of Technology*
*Stockholm, Sweden*
{*mikac,mfd*}*@kth.se*

**Abstract**

BAN logic is a propositional logic of knowledge for the verification of cryptographic protocols. While BAN logic has been successful from a practical point of view, the semantics of the epistemic (knowledge) modality is unclear. Several Kripke semantics have been proposed, but they do not attempt at anything beyond a soundness result. Completeness is prevented by the so called logical omniscience problem: Agents in BAN can draw only feasibly computable consequences of their knowledge, whereas agents in Kripke semantics are not so constrained. To circumvent this problem, we index the epistemic possibility relation of Kripke semantics with a message correlation, relating how cipher texts at the current state correspond to cipher texts at the epistemically possible state. An agent is said to know a property of a message if corresponding messages at epistemically possible states satisfy that property. We obtain completeness with respect to message passing systems, and decidability, by transferring canonical model and filtration constructions from Kripke semantics.

Keywords: Epistemic logic, Cryptography, Logical Omniscience, BAN Logic, Completeness

## 1 Introduction

BAN logic [4] is a propositional epistemic logic for the verification of cryptographic protocols. From a practical point of view, BAN logic has turned out to be quite successful: It produces short, informative derivations that can reveal subtle protocol errors. However, the semantics of the epistemic (knowledge) modality in BAN logic has remained problematic. While a number of semantics have been proposed for BAN and BAN-like logics, none of them capture accurately the intended meaning of the epistemic modality in BAN (cf. [1,7,12,19,20,21,22,26]). This situation is unsatisfactory. Without a semantics, it is unclear what is established by a derivation in the proof system of BAN: A proof system is merely a definition, and as such it needs further

justification. Moreover, the restriction to proof system based protocol analysis is unfortunate. Indeed, elsewhere in epistemic logic, semantically based techniques for analysing security protocols, for instance model checking, are preferred (cf. [13,16,25]).

In this paper, we show that BAN logic, or a logic close to original BAN, is decidable and is sound and complete with respect to concrete, run-based models in the tradition of [9,18]. The completeness result provides strong evidence that the semantics indeed captures the intended meaning in BAN. By contrast, previous work on semantics for BAN-like logics does not go beyond soundness results.

Any interpretation of BAN's knowledge modality faces the so-called logical omniscience problem [9]. To illustrate this, under BAN's idealized treatment of cryptography, the implication:

$$\mathit{fresh}\, M \rightarrow \mathit{fresh}\, \{M\}_K \tag{1}$$

should be regarded as valid, reflecting the fact that if the message $M$ has never appeared as a component of any message exchanged in the past, then neither has $\{M\}_K$. But in Kripke semantics, the standard semantics for knowledge, if (1) is validated then so is:

$$A\, \mathit{knows}\, \mathit{fresh}\, M \rightarrow A\, \mathit{knows}\, \mathit{fresh}\, \{M\}_K \tag{2}$$

However, (2) goes against the intended meaning in BAN, since in BAN agent $A$ can know that $M$ is inside $\{M\}_K$ only when $A$ knows $K$. In general, according to the intended (informal) meaning of knowledge, agents can only perform computationally feasible cryptographic calculations, whereas in Kripke semantics agents draw arbitrary logical inferences, including cryptographic calculations that are not computationally feasible. From the point of view of modal logic, the problem is that Kripke semantics yields the rule of normality:

$$\frac{F \rightarrow F'}{A\, \mathit{knows}\, F \rightarrow A\, \mathit{knows}\, F'}$$

stating that if $F \rightarrow F'$ is valid, then so is $A\, \mathit{knows}\, F \rightarrow A\, \mathit{knows}\, F'$. But, this rule is intuitively unsound for BAN logic, as the above example illustrates.

As another counterexample to the rule of normality, consider BAN's flagship rule, the message meaning rule, according to which if agent $A$ receives a ciphertext $\{M\}_K$, which $A$ did not send, and $A$ knows that the key $K$ to it is secret between $A$ and agent $B$, then $A$ knows that $B$ sent the ciphertext $\{M\}_K$. Clearly, the message meaning rule implicitly assumes a receiving introspection validity:

$$A\, \mathit{received}\, M \rightarrow A\, \mathit{knows}\, A\, \mathit{received}\, M \tag{3}$$

Say we extend BAN, as in [12,19], with a predicate $A\, \mathit{rec}$, where $A\, \mathit{rec}\, M$ holds

if $M$ is a part of something $A$ received. Trivially,

$$A \textit{ received } \{M\}_K \rightarrow A \textit{ rec } M \tag{4}$$

is valid. However, by the rule of normality, (3) and (4) yield the following validity:

$$A \textit{ received } \{M\}_K \rightarrow A \textit{ knows } A \textit{ rec } M \tag{5}$$

which gives agent $A$ unlimited decryption power, clearly contrary to the intended meaning in BAN.

In Kripke semantics, agents $A$'s knowledge is interpreted through an epistemic possibility relation $\sim_A$ between states: At the current system state, agent $A$ knows that message $M$ has property $p$, if $M$ has property $p$ at all epistemically possible system states. Logical omniscience (the rule of normality) is inescapable, no matter how the epistemic possibility relation $\sim_A$ is defined. Therefore, as (2) above illustrates, every extension to BAN is incomplete with respect to any Kripke semantics, assuming that the extension stays faithful to the intended meaning of knowledge in BAN. Moreover, this gap between the obtained validities and the intended meaning can become even more severe as new predicates are added, as (5) shows. As it happens, all semantics for BAN and BAN-like logics, except for [6], are based on Kripke semantics (cf. [1,7,12,19,20,21,22,26]).

Outside the BAN literature, various semantics avoid logical omniscience, but at the price of a drastic break with Kripke semantics (cf. [9,16,19]). Recently, however, we showed (cf. [6]) how to avoid logical omniscience in a mild generalization of Kripke semantics, inspired by so-called counterpart semantics [15]. The idea is to modify Kripke semantics by permuting the data (i.e., cryptographic messages) as we follow the epistemic possibility relation: Agent $A$ knows that message $M$ has property $p$, if at every epistemically possible system state, the message correlated to $M$ satisfies property $p$. Due to the permutation of messages, agents are no longer logically omniscient.

In [6] we established some of the basic properties of the generalized Kripke semantics, including soundness. Here, we extend this work to show that a faithful version of BAN is decidable and complete with respect to message passing systems. We note that completeness for the original BAN logic [4] cannot be expected. The original logic, as its authors make clear, leaves out rules that are validated by any reasonable semantics, for instance generalizations to iterated modalities.

Our axiomatization uses, to begin with, some axioms specific to message passing systems, including receiving introspection (3). The axiomatization uses, in addition, standard modal axioms *K*, *T*, *4* and *5*, but excludes the rule of necessitation. The latter is weakened so that agents can only infer "'feasibly computable" theorems. Applying this weakening, we recover a substantial part of original BAN logic, including the above mentioned message meaning principle.

To obtain completeness and decidability, we transfer canonical model and filtration constructions from Kripke semantics: After lifting the semantics from concrete message passing systems to abstract counterpart models [15], we build a canonical counterpart model, and then filter it into a finite message passing system.

The rest of the paper is organized as follows. Section 2 defines our language and reviews message passing systems. Section 3 interprets the language on message passing systems using the generalized Kripke semantics. Section 4 defines a proof system which extends original BAN logic. Section 5 shows the proof system to be sound, complete and decidable. Section 6, finally, concludes.

## 2 Language and System

### *2.1 Language of Full Propositional BAN*

We assume a language of propositional epistemic logic with atomic statements specialized for message passing systems. Messages are generated by:

$$M, K ::= \ c \mid M \cdot K \mid \{M\}_K$$

where $c$ ranges over a countable set $\mathcal{C}$ of message atoms ("constants"), $\cdot$ represents pairing and $\{-\}_-$ represents symmetric encryption. Assume a finite subset $\mathcal{A} \subseteq \mathcal{C}$ of agent names $A, B, C, \ldots$ The sub-message relation $\leq$ is the smallest reflexive and transitive relation on messages such that $M \leq \{M\}_K$, $K \leq \{M\}_K$, $M \leq M \cdot M'$ and $M' \leq M \cdot M'$. A message space is a non-empty set of messages closed under $\geq$, i.e., if $M \geq M'$ then the space contains $M'$ if it contains $M$. We fix a finite message space $\mathcal{T}$; A message $M$ is, from now on, a message in the fixed space $\mathcal{T}$.[1] The proofs of completeness and decidability in section 5 depend on this restriction to a finite message space. Atomic predicates $p$ are as follows:

$$p ::= \ A \mathit{\ received} \mid A \mathit{\ rec} \mid A \mathit{\ sent} \mid A \mathit{\ sen} \mid A \mathit{\ infers} \mid \mathit{unfresh} \mid \mathit{exists}$$

The intended meaning is straightforward: $A \mathit{\ received}\, M$ if agent $A$ received message $M$ from the network, $A \mathit{\ rec}\, M$ if $M$ is a sub-message of some message $A$ received; The intended meaning of $a \mathit{\ sent}\, M$ and $a \mathit{\ sen}\, M$ are analogous; $A \mathit{\ infers}\, M$ if agent $A$ deduces ("knows") the message $M$ and can use it as decryption key; $\mathit{unfresh}\, M$ if $M$ is a sub-message of some message sent in an old session; $\mathit{exists}\, M$ if $M$ is a sub-message of some message some agent or other communicated. The set $\mathcal{F}$ of statements $F$ is generated by:

$$F ::= \ p(M) \mid \Box_A F \mid F \wedge F \mid \neg F$$

[1] We assume $\mathcal{A} \subseteq \mathcal{T}$.

where $\Box_A$ is the epistemic modality for $A$, read "Agent $A$ knows that". Define disjunction ($\vee$), implication ($\rightarrow$), equivalence ($\leftrightarrow$) and truth ($\top$) in the usual way. Write $\bigwedge_{1\leq i\leq n} F_i$ for the nested conjunction $F_1 \wedge \cdots \wedge F_n$, and let $\bigwedge_{1\leq i\leq 0} F_i$ be $\top$. For a set $\kappa$ of messages, write $A$ *infers* $\kappa$ for the conjunction $\bigwedge_{M\in\kappa} A$ *infers* $M$. For a set $\Delta$ of statements, write $\Box_A\Delta$ for the set $\{\Box_A F \mid F \in \Delta\}$.

The modality $\Box_A$ is the only "epistemic" language construct; None of the primitive predicates involve the notion of "feasible cryptographic computation" – except, of course, the predicate $A$ *infers*. But, this predicate will be eliminable in the logics we consider, and is kept for presentation purposes only. By contrast, predicates in original BAN (and its successors), for instance *sees*, *said* and *secret*, do depend on a model of "feasible decryptability". Instead, these "epistemic" predicates from original BAN are introduced as abbreviations, similar to [19]:

- $A$ *sees* $M =_{df} \Box_A A$ *rec* $M$
- $A$ *said* $M =_{df} \Box_A A$ *sen* $M$
- $M$ *secret of* $G =_{df} (\bigvee_{A\in G} A$ *infers* $M) \wedge (\bigwedge_{A\notin G} \neg A$ *infers* $M)$

where $G$ is a non-empty group of agents. As (5) in section 1 shows, the adequacy of the above abbreviations requires that the epistemic modality fails logical omniscience (the rule of normality). [2]

Our language differs in other respects from the original BAN language [4]. First, original BAN has some constructs for asymmetric cryptography. Second, there is no negation operator in original BAN, although several extensions and variations to BAN do add negation (cf. [1,12,19,21,22,26]). Third, original BAN includes messages that contain statements, so called idealized messages. (As example 4.9 will illustrate, idealized messages can be replaced by explicit protocol assumptions.) Fourth, we have dropped predicates *good* and *controls*; *good* is dropped because it is analogous to *secret*, and *controls* is dropped since it becomes superfluous when the epistemic modality is interpreted as knowledge rather than belief [19]. We refer to [23] for a comprehensive presentation of original BAN.

While our choice of basic predicates is intended to be representative of the BAN-literature, the choice is not intended to be canonical; The focus in this paper is on BAN's epistemic modality, and not on the specific choice of basic predicates. Our predicate *infers* appears (under various names, such as "deduces", "possesses", "knows", "has") in most extensions to BAN logic (cf. [1,3,10,19,21,23,26]), predicates *received* and *sent* appear, for instance, in BAN extensions in [12,19,20], and predicates *rec* and *sen* in [12,19].

[2] In [19], therefore, similar abbreviations use an epistemic modality for resource bounded, so called algorithmic knowledge, without a Kripke semantics.

### 2.2 Message Passing System

We assume a standard form of message passing system, where agents take turns to send and receive messages [9,18]. Freshness of messages will be determined along the lines of [1], using a special action $\texttt{begin epoch}$ that signals the start of a new time period ("epoch"). To aid the completeness construction, we also add a set of internal ("silent") actions; These will be used to enforce message correlations in the canonical countermodel to non-theorems.

The details are as follows. Actions $\pi$ are:

$$\pi ::= A\,\texttt{sends}\,M \mid A\,\texttt{receives}\,M \mid A\,int\,M \mid \texttt{begin epoch}$$

where $int$ ranges over a finite set of primitive internal actions. An execution history is a sequence $h$ of the form:

$$h ::= i \mid h \cdot \pi$$

where $i : \mathcal{A} \longrightarrow 2^{\mathcal{T}}$; The initialization $i$ assigns a set $i(A)$ of messages to agent $A$, the messages $A$ possesses when execution begins. A system is a non-empty set $H$ of execution histories, informally the set of executions of some underlying protocol. Since $H$ need not be closed under prefixing, $H$ may consist of only completed protocol runs.

The local history of agent $A$ in history $h$, in symbols $h|A$, is the sequence of observations that $A$ makes during $h$:

$$\begin{aligned}
(h \cdot A\,\texttt{sends}\,M)|A &= (h|A) \cdot A\,\texttt{sends}\,M \\
(h \cdot B\,\texttt{sends}\,M)|A &= (h|A),\ B \neq A \\
(h \cdot A\,\texttt{receives}\,M)|A &= (h|A) \cdot A\,\texttt{receives}\,M \\
(h \cdot B\,\texttt{receives}\,M)|A &= (h|A),\ B \neq A \\
(h \cdot A\,int\,M)|A &= (h|A) \cdot A\,int\,M \\
(h \cdot B\,int\,M)|A &= (h|A),\ B \neq A \\
(h \cdot \texttt{begin epoch})|A &= (h|A) \cdot \texttt{begin epoch} \\
i|A &= \texttt{init}\,i(A)
\end{aligned}$$

where $\texttt{init}\,\kappa$ represents a local initialization which generates the set $\kappa$ of messages. In short, agents observe the "global time" and their own communication actions and internal actions.

We introduce the auxiliary notion of action trace. An action trace is a finite, possibly empty sequence $\theta$ of initializations, local initializations and actions:

$$\theta ::= \epsilon \mid \theta \cdot i \mid \theta \cdot \texttt{init}\,\kappa \mid \theta \cdot \pi$$

where $\epsilon$ is the empty sequence and $\kappa \subseteq \mathcal{T}$. Thus, histories $h$ and local histories $h|A$ are action traces. Write $actions(\theta)$ for the set of actions occurring in action trace $\theta$:

$$
\begin{aligned}
\mathit{actions}(\epsilon) &= \emptyset \\
\mathit{actions}(\theta \cdot i) &= \mathit{actions}(\theta) \cup \{i\} \\
\mathit{actions}(\theta \cdot \texttt{init}\,\kappa) &= \mathit{actions}(\theta) \cup \{\texttt{init}\,\kappa\} \\
\mathit{actions}(\theta \cdot \pi) &= \mathit{actions}(\theta) \cup \{\pi\}
\end{aligned}
$$

Write $\mathit{messages}(\theta)$ for the set of the messages initially possessed or communicated in $\theta$:

$$
\begin{aligned}
\mathit{messages}(\epsilon) &= \emptyset \\
\mathit{messages}(\theta \cdot i) &= \mathit{messages}(\theta) \cup \bigcup \mathit{ran}(i) \\
\mathit{messages}(\theta \cdot \texttt{init}\,\kappa) &= \mathit{messages}(\theta) \cup \kappa \\
\mathit{messages}(\theta \cdot A\,\texttt{sends}\,M) &= \mathit{messages}(\theta) \cup \{M\} \\
\mathit{messages}(\theta \cdot A\,\texttt{receives}\,M) &= \mathit{messages}(\theta) \cup \{M\} \\
\mathit{messages}(\theta \cdot \texttt{begin epoch}) &= \mathit{messages}(\theta) \\
\mathit{messages}(\theta \cdot A\,\mathit{int}\,M) &= \mathit{messages}(\theta)
\end{aligned}
$$

where $\mathit{ran}(i)$ is the range of $i$.

### *2.3 Interpretation of Predicates*

A predicate interpretation $I$ on a system $H$ assigns, to each predicate $p$ and history $h \in H$, an extension $I(p,h) \subseteq \mathcal{T}$. An interpreted system based on $H$ is a pair $\mathcal{I} = \langle H, I \rangle$, where $I$ is an interpretation on $H$. The interpretation of predicate $A\,\mathit{infers}$ is left open until section 3.3. For remaining predicates, we assume the following fixed interpretation:

$$
\begin{aligned}
I(A\,\mathit{sent}, h) &= \{M \mid (A\,\texttt{sends}\,M) \in \mathit{actions}(h)\} \\
I(A\,\mathit{received}, h) &= \{M \mid (A\,\texttt{receives}\,M) \in \mathit{actions}(h)\} \\
I(A\,\mathit{rec}, h) &= \{M \mid \exists M' \geq M.\, A\,\texttt{receives}\,M' \in \mathit{actions}(h)\} \\
I(A\,\mathit{sen}, h) &= \{M \mid \exists M' \geq M.\, A\,\texttt{sends}\,M' \in \mathit{actions}(h)\} \\
I(\mathit{exists}, h) &= \{M \mid \exists M' \geq M.\, M' \in \mathit{messages}(h)\}
\end{aligned}
$$

The predicate *unfresh* is interpreted along the lines of [1], through the `begin epoch` action: $I(\mathit{unfresh}, h)$ contains sub-messages of messages sent prior to the latest epoch, i.e., $M \in I(\mathit{unfresh}, h)$, if and only if,

$$h = \theta_- \cdot \texttt{begin epoch} \cdot \theta_+ \text{ and } M \in I(A\,\mathit{sen}, \theta_-)$$

for some $A \in \mathcal{A}$ and some action traces $\theta_-$ and $\theta_+$. The interpretation of *unfresh* is not critical. Other accounts can be dealt with by routine changes. Admittedly, the interpretation of *exists* is somewhat ad hoc, since $\mathit{messages}(h)$ need not contain messages acted upon internally, i.e., $\mathit{messages}(h)$ need not include the message $M$ even if $(A\,\mathit{int}\,M) \in \mathit{actions}(h)$; The interpretation of *exists* is chosen so as to facilitate the completeness construction.

# 3 Semantics

## *3.1 Kripke Semantics*

In Kripke semantics, the epistemic modality $\Box_A$ is interpreted through an epistemic possibility relation $\sim_A$ between states, in our case histories, as follows:

$$h \models_{\mathcal{I}} \Box_A F \Leftrightarrow \forall h' \in H : h \sim_A h' \Rightarrow h' \models_{\mathcal{I}} F$$

Intuitively, $h \sim_A h'$ means that $h$ and $h'$ appear identical from the point of view of $A$. Truth conditions for Boolean operators and atomic statements are as expected:

$$\begin{aligned} h \models_{\mathcal{I}} p(M) &\Leftrightarrow M \in I(p,h) \\ h \models_{\mathcal{I}} F \wedge F' &\Leftrightarrow h \models_{\mathcal{I}} \text{ and } h \models_{\mathcal{I}} F' \\ h \models_{\mathcal{I}} \neg F &\Leftrightarrow h \not\models_{\mathcal{I}} F \end{aligned}$$

Entailment and validity are also defined as usual. For a set $\Delta$ of statements, write $h \models_{\mathcal{I}} \Delta$ if $h \models_{\mathcal{I}} F$ for all $F \in \Delta$. A set $\Delta$ entails a statement $F$ in interpreted system $\mathcal{I}$, written $\Delta \models_{\mathcal{I}} F$, if for all histories $h \in H$, if $h \models_{\mathcal{I}} \Delta$ then $h \models_{\mathcal{I}} F$. A statement $F$ is valid in $\mathcal{I}$, written $\models_{\mathcal{I}} F$, if the empty set entails $F$ in $\mathcal{I}$.

The epistemic possibility relation has a default definition for message passing systems, due to [9,18]: $h \sim_A h'$, if and only if, $h|A = h'|A$. This default definition is used in, for instance, [19,20] to interpret BAN's epistemic modality. However, the default definition does not reflect the limited decryption power of agents, as is intended in BAN logic.

**Example 3.1** Consider an interpreted system $\mathcal{I} = \langle H, I \rangle$ such that $H$ contains exactly two execution histories $h_B$ and $h_C$. In $h_B$, agent $B$ encrypts her own name and send the encryption to agent $A$, while in $h_C$, agent $C$ encrypts her own name and send the encryption to agent $A$:

$$\begin{aligned} h_B &= i \cdot B \,\mathsf{sends}\, \{B\}_K \cdot A \,\mathsf{receives}\, \{B\}_K \\ h_C &= i' \cdot C \,\mathsf{sends}\, \{C\}_{K'} \cdot A \,\mathsf{receives}\, \{C\}_{K'} \end{aligned}$$

where $i(A) = \emptyset$, $i(B) = \{K\}$, $i(C) = \emptyset$ and $i'(A) = \emptyset$, $i'(B) = \emptyset$ and $i'(C) = \{K'\}$. It is reasonable to assume that neither at $h_B$ nor at $h_C$ can agent $A$ decrypt the received cryptogram: Histories $h_B$ and $h_C$ are indistinguishable to $A$. In other words, agent $A$ does not know who (of agents $B$ and $C$) sent the cryptogram received. Contrary to this intuition, the default definition of $\sim_A$ makes agent $A$ know who sent the message: $h_B \models_{\mathcal{I}} \Box_A B \, sent \, \{B\}_K$.

To avoid unintended consequences like those in example 3.1, the AT semantics [1], and its descendants [22,26] weaken the requirement of local history identity, so as to hide cryptographically inaccessible parts of the local history. Roughly, $h \sim_A h'$ if $h|A$ and $h'|A$ are equivalent up to the structure of unopened (undecrypted) ciphertexts. However, even after thus hiding inaccessible parts of the local history, the semantics still remain unfaithful to

BAN.[3] There are two main problems: First, AT-style semantics invalidates BAN's message meaning rule, since AT-style semantics invalidates receiving introspection (3) in section 1.

**Example 3.2** Receiving introspection fails in example 3.1. Clearly, $h_B \models_{\mathcal{I}} A \mathit{\ received\ } \{B\}_K$. However, in AT-style semantics, we have that $h_B \sim_A h_C$, and therefore $h_B \not\models_{\mathcal{I}} \Box_A A \mathit{\ received\ } \{B\}_K$, since $h_C \not\models_{\mathcal{I}} A \mathit{\ received\ } \{B\}_K$.

Furthermore, no matter how $\sim_A$ is weakened, logical omniscience is unavoidable in any Kripke semantics, resulting in validities that are not intended in BAN, such as (2) in section 1.

### *3.2 Generalized Kripke Semantics*

Our departure from AT semantics, and from Kripke semantics in general, starts by making the epistemic possibility relation $\sim_A$ record message correspondences between histories.

**Example 3.3** Continuing example 3.1, cryptogram $\{B\}_K$ at $h_B$ corresponds to ("is a counterpart of") cryptogram $\{C\}_{K'}$ at $h_C$, in the sense that everything that agent $A$ observes of $\{B\}_K$ at $h_B$, agent $A$ also observes of $\{C\}_{K'}$ at $h_C$. In each case, $A$ observes that the message is received, the message cannot be opened, etc.

To make $\sim_A$ keep track of message correspondences, we relativize it to a message permutation (counterpart mapping), a bijection $\rho$ on the set of messages. Informally, $h \sim_A^{\rho} h'$ if any message $M$ at $h$ corresponds for $A$ to $\rho(M)$ at $h'$. Formally, for $h \sim_A^{\rho} h'$ to hold, we require that $\rho$ respects the observations (actions) of $A$ in $h$, i.e., we require that

- $\rho(h|A) = h'|A$

where $\rho$ is extended to local histories by point-wise application: $\rho(\mathtt{init}\,\kappa) = \mathtt{init}\,\{\rho(M) \mid M \in \kappa\}$, $\rho(h|A \cdot A\,\mathtt{receives}\,M) = \rho(h|A) \cdot A\,\mathtt{receives}\,\rho(M)$, etc. Moreover, for $h \sim_A^{\rho} h'$ to hold, we require that $\rho$ is consistent with ("respects") the keys $I(A \mathit{\ infers}, h)$ available to agent $A$ at $h$.

**Definition 3.4** [Consistent Permutation] Permutation $\rho$ is consistent with $\kappa \subseteq \mathcal{T}$, in symbols $\rho \lhd \kappa$, if and only if,

(i) $K \in \kappa \Rightarrow \rho(\{M\}_K) = \{\rho(M)\}_{\rho(K)}$

(ii) $\rho(M \cdot M') = \rho(M) \cdot \rho(M')$

(iii) $\rho(c) = c$, for $c \in \mathcal{C}$

For a set $\kappa \subseteq \mathcal{T}$, let $\rho(\kappa) = \{\rho(M) \mid M \in \kappa\}$.

**Lemma 3.5** *The following hold:*

- $\rho \lhd \kappa,\ \kappa \supseteq \kappa' \implies \rho \lhd \kappa'$ *(Monotonicity)*

[3] But we acknowledge that only [1] was so intended.

- $id \lhd \kappa$ *(Reflexivity)*
- $\rho \lhd \kappa,\ \rho' \lhd \rho(\kappa) \implies (\rho' \circ \rho) \lhd \kappa$ *(Transitivity)*
- $\rho \lhd \kappa \implies \rho^{-1} \lhd \rho(\kappa)$ *(Symmetry)*

**Proof.** Monotonicity and reflexivity: Immediate. Transitivity: Assume that $\rho \lhd \kappa$ and $\rho' \lhd \rho(\kappa)$. We show that $\rho' \circ \rho$ respects encryption with keys in $\kappa$ (i.e., condition 1 in definition 3.4), showing that $r' \circ r$ respects clear text (i.e., conditions 2 and 3 in definition 3.4) is trivial. Assume that $K \in \kappa$. By the assumptions, $\rho(\{M\}_K) = \{\rho(M)\}_{\rho(K)}$ and $\rho'(\{\rho(M)\}_{\rho(K)}) = \{\rho'(r(M))\}_{\rho'(\rho(K))}$. Thus, $(\rho' \circ \rho)(\{M\}_K) = \rho'(\rho(\{M\}_K)) = \rho'(\{\rho(M)\}_{\rho(K)}) = \{\rho'(r(M))\}_{\rho'(\rho(K))} = \{(\rho' \circ \rho)(M)\}_{(\rho' \circ \rho)(K)}$. Symmetry: Assume that $\rho \lhd \kappa$. We show that $\rho^{-1}$ respects encryption with keys in $\rho(\kappa)$ (i.e., condition 1 in definition 3.4), showing that $\rho^{-1}$ respects clear text (i.e., conditions 2 and 3 in definition 3.4) is analogous. Assume that $K \in \rho(\kappa)$, i.e., $\rho^{-1}(K) \in \kappa$. By the assumption, $\rho(\{\rho^{-1}(M)\}_{\rho^{-1}(K)}) = \{\rho \circ \rho^{-1}(M)\}_{\rho \circ \rho^{-1}(K)} = \{M\}_K$. Thus, $\rho^{-1}(\{M\}_K) = \rho^{-1} \circ \rho(\{r^{-1}(M)\}_{\rho^{-1}(K)}) = \{\rho^{-1}(M)\}_{\rho^{-1}(K)}$. □

Conjoining the two requirements on $\sim_A^\rho$, we stipulate that $h \sim_A^\rho h'$ if $\rho$ carries $h|A$ to $h'|A$ and $\rho$ is consistent with the keys available to $A$ at $h$.

**Definition 3.6** [Relativized Possibility Relation] $h \sim_A^\rho h'$ in $\mathcal{I}$, if and only if,

- $\rho(h|A) = h'|A$
- $\rho \lhd I(A\ infers, h)$

**Example 3.7** Continuing example 3.1, we may stipulate that agent $A$ infers only the messages received, i.e., $I(A\ infers, h_B) = \{\{B\}_K\}$. Let $\rho$ be the substitution on messages that swaps $\{B\}_K$ and $\{C\}_{K'}$. Then, $\rho(\{B\}_K) = \{C\}_{K'}$, so $\rho(h_B|A) = h_C|A$. Moreover, $\rho \lhd I(A\ infers, h_B)$, hence $h_B \sim_A^\rho h_C$ in $\mathcal{I}$. Thus, $\{B\}_K$ at $h_B$ corresponds for $A$ to $\{C\}_{K'}$ at $h_c$.

Given the relativized epistemic possibility relation, we say that an agent knows a statement if *corresponding* statements hold at epistemically possible histories; We lift permutations to statements in the obvious way: $\rho(p(M)) = p(\rho(M))$, $\rho(\Box_A F) = \Box_A \rho(F)$, etc.

**Definition 3.8** [Generalized Kripke]

$$h \models_{\mathcal{I}} \Box_A F \Leftrightarrow \forall \rho : \forall h' \in H : h \sim_A^\rho h' \Rightarrow h' \models_{\mathcal{I}} \rho(F)$$

Remaining truth conditions, as well as the notion of validity, are preserved from section 3.1. The break with Kripke semantics should be clear. We check a corresponding statement $\rho(F)$ at $h'$, and not the original statement $F$. As a result, agents are no longer logically omniscient, as the following example illustrates.

**Example 3.9** Consider the interpreted system $\mathcal{I}$ of example 3.7. We obtain (cf. soundness of axiom $I$ in theorem 5.1), $h_B \models_{\mathcal{I}} \Box_A A\ received\ \{B\}_K$. If we

pick the permutation $\rho$ from example 3.7, then $\rho(B) = B$ and $h_B \sim_A^\rho h_C$. Since $h_C \not\models_H A\,rec\,\rho(B)$, we have $h_B \not\models_{\mathcal{I}} \Box_A A\,rec\,B$. This contradict logical omniscience, since $A\,received\,\{B\}_K \models A\,rec\,B$.

The consistency relation $\lhd$ is related to the states of knowledge and belief of [2,24]. The definition 3.4 of $\lhd$ is not intended to be canonical: There are alternative, equally reasonable, definitions. Most obviously, requirement (iii), which reflects the assumption that atoms are "plain text", could be restricted to atoms in $\mathcal{A}$. As another example, it might, perhaps, be reasonable to restrict requirement (ii) to messages in the given set $\kappa$:

$$M \in \kappa,\ M' \in \kappa \Rightarrow \rho(M \cdot M') = \rho(M) \cdot \rho(M')$$
$$M \cdot M' \in \kappa \Rightarrow \rho(M \cdot M') = \rho(M) \cdot \rho(M')$$

However, with this restriction, soundness for classical BAN (section 4.1) would fail. (Specifically, BAN rules *R7* and *R8* in table 1 would be unsound.) As regards the requirement that $\rho$ must be a permutation, we note that symmetry of $\lhd$ in lemma 3.5 depends on this requirement.

### *3.3 Inductive Interpretation*

So far, we left the interpretation of *infers* open. However, a notion of message inference is implicit in original BAN [4]: An agent infers a key if the agent knows the key to be secret.[4] In symbols:

$$\Box_A K\ secret\ of\ G \rightarrow A\ infers\ K \tag{6}$$

Extrapolating from (6), we obtain:

$$A\ infers\ K \leftrightarrow \Box_A \bigvee_p p(K)$$

where $p$ ranges over a selected set of relevant predicates. Here, for simplicity, we shall take *exists* to be the only relevant predicate:

$$A\ infers\ K \leftrightarrow \Box_A exists\ K \tag{7}$$

However, the stipulation (7) requires a recursive definition, since the epistemic modality $\Box_A$ is defined in terms of the relativized possibility relation, which, in turn, is defined through the interpretation of $A\ infers$ (definition 3.6).

**Definition 3.10** [Fixed Point Interpretation] An interpretation function $I$ is a fixed point on a system $H$, if condition (7) holds in the interpreted system $\mathcal{I} = \langle H, I\rangle$.

An inductive, rather than a co-inductive interpretation of $A\ infers$ is appropriate, since $I(A\ infers, h)$ should assign the set of keys that agent $A$ has

[4] Cf. rules *R1*, *R4* and *R9* in table 1.

gathered some positive information about at history $h$. We introduce some terminology. Interpretation $I$ is smaller than $I'$, $I \leq I'$ if $I(A\,infers, h) \subseteq I'(A\,infers, h)$ for all $A \in \mathcal{A}$ and all $h \in H$.[5]

**Definition 3.11** [Inductive Interpretation] Interpretation $I$ is inductive on system $H$, if $I$ is a minimal fixed point on $H$. System $\mathcal{I} = \langle H, I\rangle$ is inductive if $I$ is inductive on $H$.

**Theorem 3.12** *There is a unique inductive interpretation on every system.*

**Proof.** From monotonicity of $\triangleleft$ (lemma 3.5). Let $f$ be a function in the set of interpretations on system $H$ such that:

$$f(I)(A\,infers, h) = \{K \mid\ h \models_{\langle H,I\rangle} \Box_A\, exists\, K\}$$

Assume that $I$ is smaller than $I'$, i.e., $I(A\,infers, h) \subseteq I'(A\,infers, h)$ for all $A \in \mathcal{A}$ and $h \in H$. Assume that $K \in f(I)(A\,infers, h)$, i.e., $h \models_{\langle H,I\rangle} \Box_A\, exists\, K$. We proceed to show that $h \models_{\langle H,I'\rangle} \Box_A\, exists\, K$. Pick any $h' \in H$ and permutation $\rho$ such that $h \sim_A^{\rho} h'$ in $\langle H, I'\rangle$, i.e., such that $\rho(h|A) = h'|A$ and $\rho \triangleleft I'(A\,infers, h)$. By monotonicity of $\triangleleft$ (lemma 3.5), $\rho \triangleleft I(A\,infers, h)$. Thus, $h \sim_A^{\rho} h'$ in $\langle H, I\rangle$. By assumption, $h' \models_{\langle H,I\rangle} exists\,\rho(K)$, i.e., $h' \models_{\langle H,I'\rangle} exists\,\rho(K)$. Since $h'$ and $\rho$ were chosen arbitrary, it follows that $h \models_{\langle H,I'\rangle} \Box_A K$, i.e., $K \in f(I')(A\,infers, h)$. This establishes that $f$ is monotone, and therefore has a unique least fixed point. □

**Lemma 3.13** *In inductive systems $\mathcal{I}$:*

(i) $h \sim_A^{id} h$

(ii) $h \sim_A^{\rho} h'$, $h' \sim_A^{\rho'} h'' \implies h \sim_A^{\rho' \circ \rho} h''$

(iii) $h \sim_A^{\rho} h' \implies h' \sim_A^{\rho^{-1}} h$

**Proof.** (i): From reflexivity of $\triangleleft$ (lemma 3.5). (ii): From transitivity of $\triangleleft$ (lemma 3.5) and fixed point induction. (iii): From symmetry of $\triangleleft$ (lemma 3.5) and fixed point induction. The fixed point induction is rather involved in each case. For details, we refer to [5,6]. □

According to (iii) in lemma 3.13, the apparent asymmetry in the definition of the epistemic possibility relation disappears in inductive models. As a non-inductive countermodel to (iii), consider the system $H$ in example 3.1 with an interpretation $I$ such that $I(A\,infers, h_B) = \{K\}$ and $I(A\,infers, h_C) = \emptyset$. Logical omniscience fails in inductive interpreted systems; The model in example 3.9 is an example.

From now on, if no interpretation $I$ is given, we implicitly assume the inductive interpretation: $h \models_H F$, if and only if, $h \models_{\mathcal{I}} F$ for the inductive interpreted system $\mathcal{I}$ based on $H$; Statement $F$ is valid in system $H$ if $h \models_H F$ for all $h \in H$.

[5] Recall that the interpretation of predicates other than *infers* is fixed.

Many semantics proposed for BAN and BAN-like logics uses a customary Dolev-Yao style, operational definition of inferred messages [8]: Roughly, a message is inferred if it is an initial possession, or if it is received, or if it is the first or second pairing component of an inferred message, or if it is the body of an inferred symmetric encryption locked with an inferred key. In [5], it is shown that the inductive interpretation (definition 3.11) is at least as inclusive as a Dolev-Yao style interpretation, and that the two interpretations agree on *atomic* messages under certain reasonable requirements on message passing systems. For *composite* messages, it is shown that the inductive interpretation withstands the well-known Duck-Duck-Goose counter example [11] to Dolev-Yao style interpretations.

# 4 Logic

## *4.1 Classical BAN Logic*

We introduce rules of original BAN logic [4] as requirements on theories. A *theory* is a set $L$ of statements such that $L$ contains all Boolean tautologies and $L$ is closed under modus ponens, i.e., if $F \to F' \in L$ and $F \in L$ then $F' \in L$. A statement $F$ is derivable from a set $\Delta$ of statements in theory $L$, $\Delta \vdash_L F$, if there is a finite number of statements $F_1, ..., F_n \in \Delta$ such that $(\bigwedge_{1 \le i \le n} F_i) \to F \in L$. As usual, we write $\vdash_L F$ for $\emptyset \vdash_L F$, and we omit the subscript $L$ whenever $L$ is clear from the context. Let $\mathit{from}\, B : M$ abbreviate, say, $B \cdot M$.

**Definition 4.1** [Classical BAN] A theory is a classical BAN logic if it satisfies all conditions in table 1.

Note that rule *R1*, the well-known *message meaning rule*, assumes that agents are honest, in the sense that the first component inside a cipher text, if locked with a secret key, is a reliable sender field.

In definition 4.1, we define a class of logics, rather than a single logic, since the original BAN logic is open ended and leaves out rules that are intuitively valid. For instance, *seeing introspection*:

$$A \mathit{\ sees\ } M \vdash \Box_A A \mathit{\ sees\ } M \tag{8}$$

is not part of the original BAN logic, even though it is clearly implicit in requirement *R1*.[6] As another illustration, all requirements may be generalized to iterated modalities. For instance, requirement *R2* may be generalized to $\Box_A \Box_B C \mathit{\ sees\ } M \cdot M' \vdash \Box_A \Box_B C \mathit{\ sees\ } M$.

While the definition 4.1 keeps close to the original definition of BAN logic in [4], it nonetheless simplifies the original definition. As explained in section

[6] Some BAN extensions add the seeing introspection rule, cf. [3].

*R1* $A \text{ sees } \{\text{from } B : M\}_K, \Box_A K \text{ secret of } G \vdash \Box_A B \text{ said } M,\ B \in G$

*R2* $A \text{ sees } M \cdot M' \vdash A \text{ sees } M$

*R3* $A \text{ sees } M \cdot M' \vdash A \text{ sees } M'$

*R4* $A \text{ sees } \{M\}_K,\ \Box_A K \text{ secret of } G \vdash A \text{ sees } M$

*R5* $\Box_A B \text{ said } M \cdot M' \vdash \Box_A B \text{ said } M$

*R6* $\Box_A B \text{ said } M \cdot M' \vdash \Box_A B \text{ said } M'$

*R7* $\Box_A \text{fresh } M \vdash \Box_A \text{fresh } M \cdot M'$

*R8* $\Box_A \text{fresh } M' \vdash \Box_A \text{fresh } M \cdot M'$

*R9* $\Box_A \text{fresh } M,\ \Box_A K \text{ secret of } G \vdash \Box_A \text{fresh } \{M\}_K$

*R10* $\Box_A F \vdash F$

Table 1
Classical BAN

2.1, original BAN logic includes idealized messages, language constructs for public key as well as some further predicates.

### *4.2 BAN Theories*

Since the definition 4.1 of classical BAN logics leaves out intuitively valid rules (as does original BAN logic itself), we should not expect completeness for an arbitrary classical BAN logic; We need stronger proof rules. Write $\exists M' \geq M.F(M)$ for the finite disjunction $\bigvee_{M' \geq M} F(M')$.[7]

**Definition 4.2** [BAN Theory] A theory $L$ is a BAN theory, if and only if, $L$ contains the axioms and is closed under the rules in table 2.

[7] Since the message space is finite, there are finitely many $M'$.

| | |
|---|---|
| *Weakening of S5* | |
| *PNec* | $\dfrac{\rho(F),\ \ \forall \rho \lhd \kappa}{A\ infers\ \kappa \rightarrow \Box_A F}$ |
| *K* | $\Box_A(F \rightarrow F') \rightarrow \Box_A F \rightarrow \Box_A F'$ |
| *T* | $\Box_A F \rightarrow F$ |
| *4* | $\Box_A F \rightarrow \Box_A \Box_A F$ |
| *5* | $\neg\Box_A F \rightarrow \Box_A \neg\Box_A F$ |
| *Introspection* | |
| *I* | $p_A(M) \rightarrow \Box_A p_A(M),\ p_A \in \{A\ received,\ A\ sent\}$ |
| *Infers Reduction* | |
| *Red* | $A\ infers\ K \leftrightarrow \Box_A exists\ K$ |
| *Global Clock* | |
| *GC* | $unfresh\ M \rightarrow \exists M' \geq M. \bigvee\limits_{A \in \mathcal{A}} (A\ sent\ M' \wedge \Box_A unfresh\ M')$ |
| *Monotonicity* | |
| *Mono* | $p(M) \rightarrow p(M'),\ M \geq M',\ p \in \{exists, A\ rec, A\ sen, unfresh\}$ |
| *Predicates Mix* | |
| *M1* | $A\ received\ M \rightarrow A\ rec\ M$ |
| *M2* | $A\ sent\ M \rightarrow A\ sen\ M$ |
| *M3* | $A\ received\ M \rightarrow exists\ M$ |
| *M4* | $A\ sent\ M \rightarrow exists\ M$ |
| *M5* | $A\ rec\ M \rightarrow \exists M' \geq M. A\ received\ M'$ |
| *M6* | $A\ sen\ M \rightarrow \exists M' \geq M. A\ sent\ M'$ |
| *M7* | $exists\ M \rightarrow \exists M' \geq M. \bigvee\limits_{A \in \mathcal{A}} A\ infers\ M'$ |

Table 2
BAN Theory

The *permutation necessitation rule PNec*, which weakens the standard rule of necessitation, formalizes the intuition that an agent knows all "feasibly

computable" theorems. To illustrate, from the set of statements

$$\{exists\,\{M\}_K \rightarrow exists\,M \mid M, K \in \mathcal{T}\}$$

rule *PNec* yields the statement $A\ infers\ K \rightarrow \Box_A(exists\,\{M\}_K \rightarrow exists\,M)$. The rule *PNec* is quasi-semantic in that it uses the consistency relation $\lhd$. But, since there are finitely many permutations, rule *PNec* is finitary, i.e., involves a finite set of premises. When combined with axiom $K$, *PNec* yields a weakening of normality, according to which an agent knows "feasibly computable" logical implications of what the agent knows. Extend permutations to sets $\Delta$ of statements in the obvious way: $\rho(\Delta) = \{\rho(F) \mid F \in \Delta\}$.

**Lemma 4.3 (Permutation Normality)** *Assume that $L$ is a BAN theory and assume that $\rho(\Delta) \vdash_L \rho(F)$ for all $\rho \lhd \kappa$. Then, $A\ infers \kappa$, $\Box_A\Delta \vdash_L \Box_A F$.*

**Proof.** Assume that $\rho(\Delta) \vdash_L \rho(F)$, $\forall \rho \lhd \kappa$. Since the message space is finite, there are only finitely many permutations. Let $\rho_1, ..., \rho_n$ be all permutations $\rho$ such that $\rho \lhd \kappa$. For each $i \in \{1, ..., n\}$ there is a finite $\Delta_i \subseteq \Delta$ such that $\rho_i(\Delta_i) \vdash_L \rho_i(F)$. Thus for each $i \in \{1, ..., n\}$: $\rho_i(\Delta_1, ..., \Delta_n) \vdash_L \rho_i(F)$. Since $\Delta_1, ..., \Delta_n$ is finite, by rule *PNec* and axiom $K$: $A\ infers\ \kappa$, $\Box_A(\Delta_1, ..., \Delta_n) \vdash_L \Box_A F$. Since $\Delta_i \subseteq \Delta$: $A\ infers\ \kappa$, $\Box_A\Delta \vdash_L \Box_A F$. □

As its proof shows, lemma 4.3 depends on the restriction to a finite message space.

Axioms *K*, *T*, *4* and *5* are standard for introspective knowledge. The introspection axiom *I* says that an agent knows if it sent or received a message. Axiom *Red* states that an agent infers a message precisely if the agent knows it exists. According to axiom *GC*, any unfresh message $M$ is part of some message $M'$ some agent $A$ sent long ago. The axiom reflects the assumption that the time is, to some extent, common knowledge: If agent $A$ sent message $M'$ long ago, then agent $A$ knows it sent $M'$ long ago, and so knows that $M'$ is unfresh. In a temporal logic extension, axiom *GC* would reduce to sending introspection (axiom *I*), general epistemic-temporal interaction axioms and non-epistemic axioms for predicates. The remaining axioms are non-epistemic and straightforward. In particular, axiom *Mono* says that *A rec*, *A sen*, *exists* and *unfresh* are monotone with respect to the sub-message relation $\geq$.

At first sight, it might appear as if predicates *A rec* and *A sen* are superfluous: By axioms *Mono*, *M1*, *M2*, *M5* and *M6* it follows that every BAN theory contains:

$$A\ rec\ M \leftrightarrow \exists M' \geq M.A\ received\ M'$$
$$A\ sen\ M \leftrightarrow \exists M' \geq M.A\ sent\ M'$$

Nonetheless, the predicates are not eliminable. For instance, BAN theories need not contain any of the following: [8]

[8] Soundness theorem 5.1 can be used to show this.

$$\Box_A \exists M' \geq M.A \; received \; M' \rightarrow \Box_A A \; rec \; M$$
$$\Box_A \exists M' \geq M.A \; sent \; M' \rightarrow \Box_A A \; sen \; M$$

In the above implications, recall that $\exists M' \geq M.F(M')$ is just an abbreviation of the disjunction $\bigvee_{M' \geq M} F(M')$.

### *4.3 Embedding of Classical BAN Logic*

By way of the definitions in section 2.1 of classical BAN predicates *sees*, *said* and *secret*, as well as the obvious abbreviation $fresh\, M =_{df} \neg unfresh\, M$, the conditions of classical BAN can be derived using the following lemma.

**Lemma 4.4** *Assume that $L$ is a BAN theory. Assume that $\rho(\Delta) \vdash_L \rho(F)$ for all $\rho \lhd \{K\}$.*

(i) $\Box_A\, K\, secret\, of\, G,\ \Box_A \Delta \vdash_L \Box_A F.$

(ii) $A\, sees\, K,\ \Box_A \Delta \vdash_L \Box_A F.$

**Proof.** (1): From axiom *Red* and axiom *T*, $K\, secret\, of\, G \vdash exists\, K$, i.e., by lemma 4.3, $\Box_A K\, secret\, of\, G \vdash \Box_A exists\, K$, i.e., by axiom *Red*, $\Box_A K\, secret\, of\, G \vdash A\, infers\, K$. By assumption and lemma 4.3, we reach (1). (2): From axioms *Mono*, *M3* and *M5*, $A\, rec\, K \vdash exists\, K$, i.e., by lemma 4.3, $\Box_A A\, rec\, K \vdash \Box_A exists\, K$, i.e., by axiom *Red*, $A\, sees\, K \vdash A\, infers\, K$. By assumption and lemma 4.3, we reach (2). □

**Theorem 4.5** *BAN theories satisfy classical BAN conditions R2 - R10.*

**Proof.** From axiom *Mono* and lemma 4.4. □

In fact, through successive application of lemma 4.4, theorem 4.5 can be generalized to classical BAN conditions with iterated modalities. For instance, BAN theories satisfy the following generalization of condition *R9*:

$$\Box_A \Box_B fresh\, M,\ \Box_A \Box_B K\, secret\, of\, G \vdash \Box_A \Box_B fresh\, \{M\}_K$$

To obtain classical BAN condition *R1*, we add an origination axiom:

$$K\, secret\, of\, G \rightarrow A\, rec\, \{from\, B : M\}_K \rightarrow \quad (9)$$
$$B\, said\ \{from\, B : M\}_K \wedge B\, sees\, K$$

**Theorem 4.6** *Any BAN theory that contains the origination axiom (9) satisfies classical BAN condition* R1.

**Proof.** From axiom *Mono*, $B\, sen\ \{from\, B : M\}_K \vdash B\, sen\ M$. By lemma 4.4.2, we obtain $\Box_B B\, sen\ \{from\, B : M\}_K,\ B\, sees\ K \vdash \Box_B B\, sen\ M$, i.e., $B\, said\ \{from\, B : M\}_K,\ B\, sees\ K \vdash B\, said\ M$. By lemma 4.4.1, we get $\Box_A B\, said\ \{from\, B : M\}_K,\ \Box_A B\, sees\ K,\ \Box_A K\ secret\ of\ G \vdash \Box_A B\, said\ M$. Condition *R1* follows by lemma 4.4.1 applied to (9). □

Of course, axiom (9) is only applicable to a group $G$ of honest agents who supply sender fields inside their ciphertexts. But, a weaker form of origination axiom is more generally applicable:

$$K \, secret \, of G \rightarrow (A \, rec \, \{M\}_K \rightarrow \bigvee_{B \in G} (B \; said \; \{M\}_K \wedge B \, sees \, K) \qquad (10)$$

**Proposition 4.7** *Any BAN theory that contains the weaker origination axiom (10) satisfies the condition:*

$$A \, sees \, \{M\}_K, \, \Box_A K \, secret \, of G \vdash \Box_A \bigvee_{B \in G} B \, said \, M$$

**Proof.** From axiom *Mono*, $B \, sen \, \{M\}_K \vdash B \, sen \, M$. By lemma 4.4.2, we get $B \, said \, \{M\}_K$, $B \; sees \; K \vdash B \, said \; M$, i.e., we obtain $\bigvee_{B \in G} (B \, said \; \{M\}_K \wedge B \; sees \; K) \vdash \bigvee_{B \in G} B \, said \; M$. Applying lemma 4.4.1, we obtain $\Box_A K \; secret \; of \; G$, $\Box_A \bigvee_{B \in G} (B \, said \; \{M\}_K \wedge B \; sees \; K) \vdash \Box_A \bigvee_{B \in G} B \, said \; M$. The proposition follows by lemma 4.4.1 applied to (10). □

Theorems 4.5 and 4.6 and proposition 4.7 provide some justification to our definition of *sees* and *said*. The following proposition lends some further support.

**Corollary 4.8** *Any BAN theory contains:*

(i) $A \, sees \, M \rightarrow \Box_A A \, sees \, M$

(ii) $\neg A \, sees \, M \rightarrow \Box_A \neg A \, sees \, M$

(iii) $A \, said \, M \rightarrow \Box_A A \, said \, M$

(iv) $\neg A \, said \, M \rightarrow \Box_A \neg A \, said \, M$

(v) $A \; received \, M \rightarrow A \; sees \, M$

(vi) $A \; sent \, M \rightarrow A \; said \, M$

**Proof.** (1): Axiom *4*. (2): Axiom *5*. (3): Axiom *4*. (4): Axiom *5*. (5): From axiom *M1* and lemma 4.3, $\Box_A A \, received \, M \rightarrow \Box_A A \, rec \, M$, i.e., by axiom *I*, $A \, received \, M \rightarrow A \, sees \, M$. (6): From axiom *M2* and lemma 4.3, $\Box_A A \, sent \, M \rightarrow \Box_A A \, sen \, M$, i.e., by axiom *I*, $A \, sent \, M \rightarrow A \, said \, M$. □

### *4.4 Theory Base*

Theorem 4.6 and proposition 4.7 suggest that we might be interested in BAN theories generated from a base of "extra axioms". In fact, BAN-style protocol analysis normally add protocol specific rules. [9]

[9] Either explicitly (cf. [14,22,26]) or implicitly by substituting "idealized" messages for messages in the protocol description.

**Example 4.9** Consider the Needham-Schröder Shared Key Protocol [17] between principals $A$ and $B$ and with key server $S$. If the server sends the cipher text $\{N \cdot B \cdot K \cdot M\}_{K_A}$, and $K_A$ is $A$:s server key, then the server generated $K$ for $A$ and $B$:

$$S\,said\{N \cdot B \cdot K \cdot M\}_{K_A},\ K_A\ secret\ of\{A, S\},\ fresh\,N \rightarrow K\ secret\ of\{A, B, S\} \tag{11}$$

Furthermore, agent $A$ does not send the kind of cipher texts sent by the key server $S$:

$$K_A\ secret\ of\{A, S\} \rightarrow \neg A\,said\{N \cdot B \cdot K \cdot M\}_{K_A} \tag{12}$$

Assume a BAN theory that contains protocol specific axioms (11) and (12), for all keys $N$, $K$ and $K_a$ and all messages $M$, and contains the weaker origination axiom (10) for $G = \{A, S\}$. Then, the BAN theory also contains the following authentication specification:

$$A\,received\{N \cdot B \cdot K \cdot \{K \cdot A\}_{K_B}\}_{K_A},\ \Box_A K_A secret\ of\ \{A, S\},\ \Box_A fresh\,N \rightarrow \Box_A K\ secret\ of\ \{A, B, S\}$$

stating that if $A$ receives the message $\{N \cdot B \cdot K \cdot \{K \cdot A\}_{K_B}\}_{K_A}$ from the server, knows the key $K_A$ to this message, and knows that the nonce $N$ inside is fresh, then $A$ knows that the key $K$ provided inside is secret between $A$, $B$ and $S$. The derivation proceeds as follows. From (12), we get $K_A\ secret\ of\{A, S\},\ \bigvee_{A' \in \{A,S\}} A'\,said\{N \cdot B \cdot K \cdot M\}_{K_A} \vdash S\,said\{N \cdot B \cdot K \cdot M\}_{K_A}$. By lemma 4.4,

$$\Box_A K_A\ secret\ of\{A, S\},\ \Box_A \bigvee_{A' \in \{A,S\}} A'\,said\{N \cdot B \cdot K \cdot M\}_{K_A} \vdash \Box_A S\,said\{N \cdot B \cdot K \cdot M\}_{K_A} \tag{13}$$

From weak origination axiom (10) and lemma 4.4, we get $\Box_A K_A\ secret\ of\{A, S\}$, $A\,sees\{N \cdot B \cdot K \cdot M\}_{K_A} \vdash \Box_A \bigvee_{A' \in \{A,S\}} A'\,said\{N \cdot B \cdot K \cdot M\}_{K_A}$. By corollary 4.8.5,

$$\Box_A K_A\ secret\ of\{A, S\},\ A\,received\{N \cdot B \cdot K \cdot M\}_{K_A} \vdash \Box_A \bigvee_{A' \in \{A,S\}} A'\,said\{N \cdot B \cdot K \cdot M\}_{K_A} \tag{14}$$

Combining (13) and (14),

$$\Box_A K_A\ secret\ of\{A, S\},\ A\,received\{N \cdot B \cdot K \cdot M\}_{K_A} \vdash \Box_A S\,said\{N \cdot B \cdot K \cdot M\}_{K_A}$$

The specification follows from this and the application of lemma 4.4 on (11).

We define the BAN theory induced by a finite set $\boldsymbol{A}$ of statements, in symbols $L\boldsymbol{A}$, as the smallest BAN theory containing the finite set $\boldsymbol{A}$; We shall

refer to $\boldsymbol{A}$ as the theory base of $L\boldsymbol{A}$. Note that the origination schemata (9) and (10), as well as the protocol specific schemata (11) and (12) in example 4.9, are finite, since the message space is finite.

## 5 Soundness, Completeness and Decidability

Recall that a statement is valid in a message passing system $H$, if it is valid in the inductive interpreted system $\mathcal{I}$ based on $H$. Write $\|\Delta\|$ for the set of all systems $H$ validating all statements in $\Delta$. The set $\Delta$ is sound with respect to a class $C$ of systems, if $C \subseteq \|\Delta\|$. The set $\Delta$ is complete with respect to $C$, if $\Delta$ contains all statements valid in all systems in $C$.

**Theorem 5.1 (Soundness)** *$L\boldsymbol{A}$ is sound with respect to $\|\boldsymbol{A}\|$.*

**Proof.** Boolean tautologies and modus ponens: Routine. Rule *PNec*: Assume $\models_{\mathcal{I}} \rho(F)$, $\forall \rho \triangleleft \kappa$. Pick any $h \in H$ such that $h \models_{\mathcal{I}} A \mathit{infers} \kappa$. Then, $\kappa \subseteq I(A \mathit{infers}, h)$. Pick any $\rho$ and $h' \in H$ such that $h \sim_A^{\rho} h'$. Then, $\rho \triangleleft I(A \mathit{infers}, h)$. By monotonicity of $\triangleleft$ (lemma 3.5), $\rho \triangleleft \kappa$. By assumption, $\models_{\mathcal{I}} \rho(F)$, and so $h' \models_{\mathcal{I}} \rho(F)$. Since $\rho$ and $h'$ were chosen arbitrarily, $h \models_{\mathcal{I}} \Box_A F$. Axiom $K$: Routine. Axioms $T$, *4* and *5*: Lemma 3.13. Axiom $I$: Assume that $h \models_{\mathcal{I}} A \mathit{received} M$ and $h \sim_A^{\rho} h'$ in $\mathcal{I}$. From the first assumption, $A \,\mathtt{receives}\, M \in \mathit{Actions}(h|A)$, so by the second assumption, $A \,\mathtt{receives}\, \rho(M) \in \mathit{Actions}(h'|A)$, i.e., $h' \models_{\mathcal{I}} A \mathit{received} \rho(M)$. Since $h'$ and $\rho$ are arbitrary, $h \models_{\mathcal{I}} \Box_A A \mathit{received} M$. Axiom $I$ for $A \mathit{sent} M$ is analogous. Axiom *Red*: Induction property (7). Axiom $GC$: Since agent $A$ observes action $\mathtt{begin\,epoch}$ and action $A \,\mathtt{sends}$, i.e., $(h \cdot \mathtt{begin\,epoch})|A = (h|A) \cdot \mathtt{begin\,epoch}$ and $(h \cdot A \,\mathtt{sends}\, M)|A = (h|A) \cdot A \,\mathtt{sends}\, M$. Non-epistemic axioms: Routine. □

We obtain a strong form of completeness by showing that, for any given protocol base $\boldsymbol{A}$, any statement valid in systems defined by $\boldsymbol{A}$ is provable using the rules and axioms of table 2, augmented by axioms taken from $\boldsymbol{A}$. The proof of completeness is deferred to section 5.1 below.

**Theorem 5.2 (Completeness)** *$L\boldsymbol{A}$ is complete with respect to $\|\boldsymbol{A}\|$.*

Thus, the protocol base $\boldsymbol{A}$ semantically guarantees a specification only if the specification is a theorem of $L\boldsymbol{A}$. Contrast this with the usual verification practice in BAN, based on an open ended proof system: If the specification is unprovable, it can be concluded that either the protocol assumptions do not ensure the specification or the base logic needs to be extended (cf. [4,23]).

Completeness theorem 5.2 is evidence that our notion of validity is faithful to BAN. In fact, since the protocol base is freely chosen, the theorem suggests not only that validity with respect to all systems is faithful to BAN, but also that validity with respect to selected classes of systems is faithful. Clearly, applications such as model checking require the latter and stronger form of faithfulness.

**Theorem 5.3 (Decidability)** *$L\boldsymbol{A}$ is decidable.*

### *5.1 Proof of Completeness and Decidability*

We shall reach completeness and decidability by way of a finite model property: If $F$ is not a theorem of $L\boldsymbol{A}$, then there is a finite system $H_F \in \|A\|$ such that $H_F$ invalidates $F$. To construct the countersystem $H_F$, we first lift the semantics from systems to a more general class of structures, counterpart models (section 5.1.1). We then build a canonical counterpart model $\mathcal{C}_{L\boldsymbol{A}}$ that validates precisely the theorems of $L\boldsymbol{A}$ (section 5.1.2). Finally, we transform $\mathcal{C}_{L\boldsymbol{A}}$, while preserving validity of $\mathbf{A}$ and non-validity of $F$, into a finite system $H_F$ (section 5.1.4).

#### *5.1.1 Counterpart Model*

We abstract from our semantics on systems to a semantics on abstract counterpart models [15]. A counterpart model is a triple $\mathcal{C} = \langle W, \longrightarrow, Int\rangle$, where $W$ is a set of worlds (states), $\longrightarrow^{\rho}_{A} \subseteq W \times W$ for each agent $A \in \mathcal{A}$ and each message permutation $\rho$, and $Int(p, w)$ is a set of messages, intuitively the set of messages satisfying predicate $p$ at $w$. Intuitively, $w \longrightarrow^{\rho}_{A} w'$ says that any $M$ at $w$, could, for all $A$ knows, be $\rho(M)$ at $w'$. The semantics of section 3.2 is generalized in the obvious way:

$$w \models_{\mathcal{C}} \Box_A F \Leftrightarrow \forall \rho : \forall w' \in W : w \longrightarrow^{\rho}_{A} w' \Rightarrow w' \models_{\mathcal{C}} \rho(F)$$
$$w \models_{\mathcal{C}} p(M) \Leftrightarrow M \in Int(p, w)$$

Truth conditions for boolean operators are standard.

Counterpart models are used in counterpart semantics [15], a semantics for first order modal logic. However, in counterpart semantics, one updates the assignment to logical variables as one moves along the possibility relation from one state to another, rather than, as we do here, update the terms inside the evaluated statement $F$.

#### *5.1.2 Canonical Counterpart Model*

Next, we build a canonical counterpart model that validates precisely the theorems of a given BAN theory. Assume a BAN theory $L$. A set $\Delta$ of statements is consistent if there is no statement $\neg F$ such that $\Delta \vdash \neg F$ and $\Delta \vdash F$.[10] $\Delta$ is maximal consistent if there is no consistent set $\Delta'$ such that $\Delta' \supset \Delta$. Using the standard Lindenbaum construction we obtain:

**Lemma 5.4 (Extension Lemma)** *If $\Delta \nvdash F$, there is a maximal consistent set $\Delta' \supseteq \Delta$ such that $F \notin \Delta'$.*

The canonical counterpart model for BAN theory $L$ is $\mathcal{C}_L = \langle W_L, \underset{L}{\longrightarrow}, Int_L\rangle$, where

[10] Since the BAN theory $L$ is clear from the context, we drop the subscripted $L$ from $\vdash_L$.

- $W_L$ is the set of all maximal consistent sets
- $Int_L(w,p) = \{M \mid p(M) \in w\}$
- $w \underset{L}{\longrightarrow}^{\rho}_{A} w' \Leftrightarrow \rho \triangleleft Int_L(A\ infers, w)$ and $\forall F : \Box_A F \in w \Rightarrow \rho(F) \in w'$

**Lemma 5.5 (Truth lemma)** $w \models_{\mathcal{C}_L} F \Leftrightarrow F \in w$.

**Proof.** By induction in (the number of statement operators in) $F$, using permutation normality (Lemma 4.3). The base case, for atomic $F$, is immediate. The induction step, for boolean operators, uses standard properties of maximal consistent sets. For the epistemic modality let $w|A$ be the set $\{F \mid \Box_A F \in w\}$. For the only-if direction first:

$\Box_A F \notin w$

| | | |
|---|---|---|
| $\Rightarrow \rho(w\|a) \not\vdash \rho(F)\ \&\ \rho \triangleleft Int_L(a\ uses, w),\ \exists \rho$ | (By rule *PNec*) | (15) |
| $\Rightarrow \rho(w\|a) \subseteq w'\ \&\ \rho(F) \notin w',\ \exists w' \in W_L$ | (By lemma 5.4) | (16) |
| $\Rightarrow w' \not\models_{\mathcal{C}_L} \rho(F)$ | (By the ind. hyp.) | (17) |
| $\Rightarrow \forall F : \Box_A F \in w \Rightarrow \rho(F) \in w'$ | (By (16)) | (18) |
| $\Rightarrow w \underset{L}{\longrightarrow}^{\rho}_{A} w'$ | (By (15) and (18)) | (19) |
| $\Rightarrow w \not\models_{\mathcal{C}_L} \Box_A F$ | (By (17) and (19)) | |

For the if-direction:

$\Box_A F \in w\ \&\ w \underset{L}{\longrightarrow}^{\rho}_{A} w'\ \&\ w' \in W_L$

| | |
|---|---|
| $\Rightarrow \rho(F) \in w'$ | |
| $\Rightarrow w' \models_{\mathcal{C}_L} \rho(F)$ | (By the ind. ass.) |
| $\Rightarrow w \models_{\mathcal{C}_L} \Box_A F$ | (By the assumptions) |

□

The canonical counterpart model validates precisely all theorems.

**Corollary 5.6 (Canonical Model Corollary)** $\models_{\mathcal{C}_L} F \Leftrightarrow \vdash_L F$.

**Proof.** From extension lemma 5.4 and truth lemma 5.5. □

If $w$ is related to $w'$ under permutation $\rho$, then $\rho$ transforms what the agent knows in $w$ to what the agent knows in $w'$.

**Lemma 5.7** *If* $w \underset{L}{\longrightarrow}^{\rho}_{A} w'$, *then* $\Box_A F \in w \Leftrightarrow \Box_A \rho(F) \in w'$.

**Proof.** From axioms 4 and 5. Assume that $w \underset{L}{\longrightarrow}^{\rho}_{A} w'$.

$\Box_A F \in w$

| | |
|---|---|
| $\Rightarrow \Box_A \Box_A F \in w$ | (Axiom 4) |
| $\Rightarrow \Box_A \rho(F) \in w'$ | (Since $w \underset{L}{\longrightarrow}^{\rho}_{A} w'$) |

For the converse:

$\Box_A F \notin w$
$\Rightarrow \neg\Box_A F \in w$
$\Rightarrow \Box_A \neg\Box_A F \in w$ (Axiom 5)
$\Rightarrow \neg\Box_A \rho(F) \in w'$ (Since $w \underset{L}{\longrightarrow}{}^{\rho}_{A} w'$)
$\Rightarrow \Box_A \rho(F) \notin w'$

□

*5.1.3 Filtration*

In the section following this one, we transform the canonical model into a system, while preserving validity of theorems and non-validity of a given non-theorem $F$. In this section, we lay down conditions that assure that such a transformation succeeds: We define a notion of filtration from a counterpart model to an interpreted system, such that the filtration preserves truth values in a set $\Gamma$ of statements.

Assume a set $\Gamma$ of statements, a counterpart model $\mathcal{C} = \langle W, \longrightarrow, Int\rangle$ and an interpreted system $\mathcal{I} = \langle H, I\rangle$. A relation $\rightsquigarrow \subseteq W \times H$ is a $\Gamma$-filtration from $\mathcal{C}$ to $\mathcal{I}$ if whenever $w \rightsquigarrow h$ then

(i) $Int(p, w) = I(p, h)$

(ii) $w \longrightarrow^{\rho}_{A} w' \Rightarrow \exists h' \in H : w' \rightsquigarrow h',\ h \sim^{\rho}_{A} h'$

(iii) $h \sim^{\rho}_{A} h' \Rightarrow \exists w' \in W : w' \rightsquigarrow h',\ w \models_{\mathcal{C}} \Box_A F \Rightarrow w' \models_{\mathcal{C}} \rho(F),$ if $\Box_A F \in \Gamma$

From now on, we assume that $\Gamma$ is closed in two respects: $\Gamma$ is closed under sub-statements, i.e., if $F \in \Gamma$ and $F'$ is a sub-statement of $F$ then $F' \in \Gamma$, and $\Gamma$ is closed under message permutations, i.e., if $F \in \Gamma$ and $\rho$ is any permutation of messages then $\rho(F) \in \Gamma$. [11]

**Lemma 5.8 (Filtration Lemma)** *Assume that $\rightsquigarrow$ is a $\Gamma$-filtration from $\mathcal{C}$ to $\mathcal{I}$, $w \rightsquigarrow h$ and $F \in \Gamma$. Then, $w \models_{\mathcal{C}} F \Leftrightarrow h \models_{\mathcal{I}} F$.*

**Proof.** By induction on $F$. The base case, for atomic $F$, is filtration condition (i). The induction step, for boolean operators, is immediate. The induction step, for the epistemic modality: Assume, first, $h \models_{\mathcal{I}} \Box_A F$.

$w \longrightarrow^{\rho}_{A} w'$
$\Rightarrow w' \rightsquigarrow h' \wedge h \sim^{\rho}_{A} h', \exists h' \in H$ (Filt.cond. (ii))
$\Rightarrow h' \models_{\mathcal{I}} \rho(F)$ (Since $h \models_{\mathcal{I}} \Box_A F$)
$\Rightarrow w' \models_{\mathcal{C}} \rho(F)$ (Induct. assum., $\Gamma$ is closed)
$\Rightarrow w \models_{\mathcal{C}} \Box_A F$ ($w'$ and $r$ are arbitrary)

For the converse, assume that $w \models_{\mathcal{C}} \Box_A F$.

$h \sim^{\rho}_{A} h'$
$\Rightarrow w' \rightsquigarrow h' \wedge (w \models_{\mathcal{C}} \Box_A F \Rightarrow w' \models_{\mathcal{C}} \rho(F)), \exists w'$ (Filt.cond. (iii))

[11] Since the message space is finite, there are finitely many permutations.

$\Rightarrow w' \models_{\mathcal{C}} \rho(F)$ (Since $w \models_{\mathcal{C}} \Box_A F$)
$\Rightarrow h' \models_{\mathcal{I}} r(F)$ (Induct. assum., $\Gamma$ is closed)
$\Rightarrow h \models_{\mathcal{I}} \Box_A F$ ($h'$ and $\rho$ are arbitrary)

□

*5.1.4 Canonical System*

We build a filtration from the canonical counterpart model $\mathcal{C}_L = \langle W_L, \underset{L}{\longrightarrow}, Int_L \rangle$ into an interpreted system, transforming each maximal consistent set $w$ into one or more histories $h$. To this end, we first transform an arbitrary set $\Delta$ of statements into two actions sets, a set $Actions^-(\Delta)$ of "old" actions and a set $Actions^+(\Delta)$ of "recent" actions:

$$Actions^-(\Delta) = \bigcup_{A \in \mathcal{A}} Actions^-(\Delta, A)$$
$$Actions^+(\Delta) = \bigcup_{A \in \mathcal{A}} Actions^+(\Delta, A)$$

where $Actions^-(\Delta, A)$ is the set:

- $\{A \,\mathsf{sends}\, M : (A\ sent\ M) \in \Delta \wedge (\Box_A\, unfresh\, M) \in \Delta\}$

and $Actions^+(\Delta, A)$ is the union of the following three sets:

(i) $\{A \,\mathsf{receives}\, M : (A\ received\ M) \in \Delta\}$

(ii) $\{A \,\mathsf{sends}\, M : (A\ sent\ M) \in \Delta \wedge (\Box_A\, unfresh\, M) \notin \Delta\}$

(iii) $\{A \,\mathsf{int}\, F : (\Box_A F) \in \Delta\}$

In (iii), we assume that internal actions are of the form $a\,\mathtt{int}\,F$, where $F$ is any statement. [12]

Assume a set $\Gamma$ of statements. We relate a state $w$ in the canonical counterpart model to a history $h$, in symbols $w \rightsquigarrow h$, if and only if, for some initialization $i$ and some action traces $\theta^-$ and $\theta^+$:

- $h = i \cdot \theta^- \cdot \mathsf{begin\ epoch} \cdot \theta^+$
- $i(A) = \{M \mid (A\ infers\ M) \in w \cap \Gamma\}$, $A \in \mathcal{A}$
- $Actions(\theta^-) = Actions^-(w \cap \Gamma)$
- $Actions(\theta^+) = Actions^+(w \cap \Gamma)$

In order to obtain a finite system, we exclude any history that repeats actions, i.e., contains at least two occurrences of the same action $\pi(M)$. Thus, we define the canonical system – the system that we filter the canonical counterpart model into – as the set $H_L$ of all repetition-free histories obtained from states

[12] This assumes a slightly different definition of internal action than that of Section 2.2. Alternatively, we could introduce $a\,\mathtt{int}\,F$ as an abbreviation for an internal action of the form $a\ int\ M$.

in $W_L$:

$$H_L = \{h : \exists w \in W_L \text{ s.t. } w \rightsquigarrow h \text{ and } h \text{ is repetition-free}\}$$

Let the canonical interpretation $I_L$ interpret predicates $A\,sent$, $A\,received$, $A\,rec$, $A\,sen$ and *exists* according to the requirements in section 2.3:

$$I_L(A\,sent, h) = \{M \mid (A\,\mathtt{sends}\,M) \in actions(h)\},$$

and so on for the other predicates. For the remaining predicate, $A\,infers$, let:

$$I_L(A\,infers, i \cdot \theta) = i(A) \tag{20}$$

Finally, set the canonical interpreted system to $\mathcal{I}_L = \langle H_L, I_L \rangle$. We proceed to show that $\rightsquigarrow$ is a $\Gamma$-filtration from $\mathcal{C}_L$ to $\mathcal{I}_L$, under certain assumptions on $\Gamma$: We assume, from now on, that $\Gamma$ is finite and contains all atomic statements and contains $\Box_A A\ received\ M$, $\Box_A A\ sent\ M$, $\Box_A A\ infers\ M$, $\Box_A exists\ M$ and $\Box_A unfresh\ M$ for all $A \in \mathcal{A}$ and messages $M$.[13] As before, we also assume that $\Gamma$ is closed under sub-statements and message permutations $\rho$.

**Lemma 5.9 (Filtration Condition 1)** *If $w \rightsquigarrow h$, then $Int_L(p, w) = I_L(p, h)$.*

**Proof.** Assume that $w \rightsquigarrow h$. Case $p = A\,received$:

$M \in Int_L(A\,received, w)$
$\Leftrightarrow A\ received\ M \in w$
$\Leftrightarrow A\ received\ M \in w \cap \Gamma$ (Since $\Gamma$ contains atomic statements)
$\Leftrightarrow A\,\mathtt{receives}\,M \in Actions^+(w \cap \Gamma)$
$\Leftrightarrow A\,\mathtt{receives}\,M \in Actions(h)$ (Since $w \rightsquigarrow h$)
$\Leftrightarrow M \in I_L(A\,received, h)$

Case $p = A\,rec$:

$M \in Int_L(A\,rec, w)$
$\Leftrightarrow A\ rec\ M \in w$
$\Leftrightarrow A\ received\ M' \in w,\ \exists M' \geq M$ (By *M1*, *M5*, *Mono*)
$\Leftrightarrow M' \in Int_L(A\,received, w),\ \exists M' \geq M$
$\Leftrightarrow M' \in I_L(A\,received, h),\ \exists M' \geq M$ (By case $p = A\,received$)
$\Leftrightarrow M \in I_L(A\,rec, h)$

Cases $p = A\,sent$ and $p = A\,sen$ are analogous. Case $p = unfresh$:

$M \in Int_L(unfresh, w)$
$\Leftrightarrow unfresh\ M \in w$
$\Leftrightarrow A\ sent\ M', \Box_A unfresh\ M' \in w,\ \exists A.\exists M' \geq M$ (By *GC*, *T*, *Mono*)
$\Leftrightarrow A\ sent\ M', \Box_A unfresh\ M' \in w \cap \Gamma,\ \exists A.\exists M' \geq M$ (By conditions on $\Gamma$)
$\Leftrightarrow A\,\mathtt{sends}\,M' \in Actions^-(w \cap \Gamma),\ \exists A.\exists M' \geq M$
$\Leftrightarrow M \in I_L(unfresh, h)$ (Since $w \rightsquigarrow h$)

[13] Recall that the message space is finite.

Case $p = \mathit{exists}$: Let $\mathit{Actions}(\Delta) = \mathit{Actions}^-(\Delta) \cup \mathit{Actions}^+(\Delta)$.

$M \in \mathit{Int}_L(\mathit{exists}, w)$
- $\Leftrightarrow \mathit{exists}\, M \in w$
- $\Leftrightarrow (A\ \mathit{sent}\, M' \vee A\ \mathit{received}\, M' \vee A\, \mathit{infers}\, M') \in w$, $\exists A.\exists M' \geq M$ (By *M7*, *M3*, *M4*, and *Mono*,*Red*, *T*)
- $\Leftrightarrow A\ \mathit{sent}\, M' \in w \cap \Gamma$ or $A\ \mathit{received}\, M' \in w \cap \Gamma$ or $A\, \mathit{infers}\, M' \in w \cap \Gamma$, $\exists A.\exists M' \geq M$ (By conditions on $\Gamma$)
- $\Leftrightarrow A\, \mathsf{sends}\, M' \in \mathit{Actions}(w \cap \Gamma)$ or $A\, \mathsf{receives}\, M' \in \mathit{Actions}(w \cap \Gamma)$ or $A\, \mathit{infers}\, M' \in w \cap \Gamma$, $\exists A.\exists M' \geq M$
- $\Leftrightarrow M' \in \mathit{messages}(h)$, $\exists M' \geq M$ (Since $w \rightsquigarrow h$)
- $\Leftrightarrow M \in I_L(\mathit{exists}, h)$

Case $p = A\ \mathit{infers}$:

$M \in \mathit{Int}_L(A\ \mathit{infers}, w)$
- $\Leftrightarrow A\ \mathit{infers}\, M \in w$
- $\Leftrightarrow A\ \mathit{infers}\, M \in w \cap \Gamma$ (By conditions on $\Gamma$)
- $\Leftrightarrow M \in I_L(A\ \mathit{infers}, h)$ (Since $w \rightsquigarrow h$)

□

**Lemma 5.10 (Filtration Condition ii)** *If $w \rightsquigarrow h$ and $w \underset{L}{\longrightarrow}{}^{\rho}_{A} w_1$, there is $h_1 \in H_L$ such that $w_1 \rightsquigarrow h_1$ and $h \sim^{\rho}_{A} h_1$ in $\mathcal{I}_L$.*

**Proof.** Assume that $w \rightsquigarrow h$ and $w \underset{L}{\longrightarrow}{}^{\rho}_{A} w_1$. From the latter assumption, $\rho \lhd \mathit{Int}_L(A\, \mathit{infers}, w)$, i.e., by lemma 5.9 and the first assumption, $\rho \lhd I_L(A\, \mathit{infers}, h)$. Pick some $h_1 \in H_L$ such that $w_1 \rightsquigarrow h_1$. Let:

$$h|A = (\mathtt{init}\, \kappa) \cdot \theta^- \cdot \mathsf{begin\ epoch} \cdot \theta^+$$
$$h_1|A = (\mathtt{init}\, \kappa_1) \cdot \theta_1^- \cdot \mathsf{begin\ epoch} \cdot \theta_1^+$$

for some action traces $\theta^-$, $\theta^+$, $\theta_1^-$, $\theta_1^+$ and sets $\kappa, \kappa_1 \subseteq \mathcal{T}$. We shall show that:

$$\rho(\kappa) = \kappa_1 \tag{21}$$
$$\rho(\mathit{Actions}(\theta^-)) = \mathit{Actions}(\theta_1^-) \tag{22}$$
$$\rho(\mathit{Actions}(\theta^+)) = \mathit{Actions}(\theta_1^+) \tag{23}$$

The lemma then follows by shuffling the inside of $\theta_1^-$ and the inside of $\theta_1^+$: After shuffling, we obtain $\rho(h|A) = h_1|A$, and so $h \sim^{\rho}_{A} h_1$, but still $h_1 \in H_L$ and $w_1 \rightsquigarrow h_1$. For (21):

$M \in \kappa$
- $\Leftrightarrow (A\, \mathit{infers}\, M) \in w \cap \Gamma$ (Since $w \rightsquigarrow h$)
- $\Leftrightarrow (A\, \mathit{infers}\, M) \in w$ (By conditions on $\Gamma$)
- $\Leftrightarrow (\Box_A \mathit{exists}\, M) \in w$ (By *Red*)

$\Leftrightarrow (\Box_A \mathit{exists}\, \rho(M)) \in w_1$ (By lemma 5.7, $w \underset{L}{\longrightarrow}^{\rho}_{A} w_1$)

$\Leftrightarrow (A\ \mathit{infers}\, \rho(M)) \in w_1$ (By *Red*)

$\Leftrightarrow (A\ \mathit{infers}\, \rho(M)) \in w_1 \cap \Gamma$ (By conditions on $\Gamma$)

$\Leftrightarrow \rho(M) \in \kappa_1$ (Since $w_1 \rightsquigarrow h_1$)

For (22):

$A\ \mathsf{sends}\ M \in \mathit{Actions}(\theta^-)$

$\Leftrightarrow A\ \mathsf{sends}\ M \in \mathit{Actions}^-(w \cap \Gamma)$ (Since $w \rightsquigarrow h$)

$\Leftrightarrow (A\ \mathit{sent}\ M) \in w \cap \Gamma$
and $(\Box_A \mathit{unfresh}\, M) \in w \cap \Gamma$

$\Leftrightarrow (\Box_A A\ \mathit{sent}\ M) \in w \cap \Gamma$
and $(\Box_A \mathit{unfresh}\, M) \in w \cap \Gamma$ (By $I$, $T$, conditions on $\Gamma$)

$\Leftrightarrow (\Box_A A\ \mathit{sent}\ \rho(M)) \in w_1 \cap \Gamma$
and $(\Box_A \mathit{unfresh}\, \rho(M)) \in w_1 \cap \Gamma$ (By lemma 5.7, $w \underset{L}{\longrightarrow}^{\rho}_{A} w_1$)

$\Leftrightarrow (A\ \mathit{sent}\ \rho(M)) \in w_1 \cap \Gamma$
and $(\Box_A \mathit{unfresh}\, \rho(M)) \in w_1 \cap \Gamma$ (By $I$, $T$)

$\Leftrightarrow A\ \mathsf{sends}\ \rho(M) \in \mathit{Actions}^-(w_1 \cap \Gamma)$

$\Leftrightarrow A\ \mathsf{sends}\ \rho(M) \in \mathit{Actions}(\theta_1^-)$ (Since $w_1 \rightsquigarrow h_1$)

To establish (23), we show that $A\ \mathsf{receives}\ M \in \mathit{Actions}(\theta^+)$ if and only if $A\ \mathsf{receives}\ \rho(M) \in \mathit{Actions}(\theta_1^+)$, and similarly for internal and send actions. For receive actions:

$A\ \mathsf{receives}\ M \in \mathit{Actions}(\theta^+)$

$\Leftrightarrow A\ \mathsf{receives}\ M \in \mathit{Actions}(h)$

$\Leftrightarrow A\ \mathsf{receives}\ M \in \mathit{Actions}^+(w \cap \Gamma)$ (Since $w \rightsquigarrow h$)

$\Leftrightarrow A\ \mathit{received}\ M \in w \cap \Gamma$

$\Leftrightarrow \Box_A A\ \mathit{received}\ M \in w \cap \Gamma$ (By $I$, $T$, conditions on $\Gamma$)

$\Leftrightarrow \Box_A A\ \mathit{received}\ \rho(M) \in w_1 \cap \Gamma$ (By lemma 5.7 and $w \underset{L}{\longrightarrow}^{\rho}_{A} w_1$ and conditions on $\Gamma$)

$\Leftrightarrow A\ \mathit{received}\ \rho(M) \in w_1 \cap \Gamma$ (By $I$, $T$, conditions on $\Gamma$)

$\Leftrightarrow A\ \mathsf{receives}\ \rho(M) \in \mathit{Actions}^+(w_1 \cap \Gamma)$

$\Leftrightarrow A\ \mathsf{receives}\ \rho(M) \in \mathit{Actions}(h_1)$ (Since $w_1 \rightsquigarrow h_1$)

$\Leftrightarrow A\ \mathsf{receives}\ \rho(M) \in \mathit{Actions}(\theta_1^+)$

The proof for internal actions is similar and left to the reader. For send actions:

$A\ \mathsf{sends}\ M \in \mathit{Actions}(\theta^+)$

$\Leftrightarrow A\ \mathsf{sends}\ M \in \mathit{Actions}^+(w \cap \Gamma)$ (Since $w \rightsquigarrow h$)

$\Leftrightarrow (A\ \mathit{sent}\ M) \in w \cap \Gamma$
and $(\Box_A \mathit{unfresh}\, M) \notin w \cap \Gamma$

$\Leftrightarrow (\Box_A A \, sent \, M) \in w \cap \Gamma$
and $(\Box_A unfresh \, M) \notin w \cap \Gamma$ (By $I$, $T$, conditions on $\Gamma$)
$\Leftrightarrow (\Box_A A \, sent \, \rho(M)) \in w_1 \cap \Gamma$
and $(\Box_A unfresh \, \rho(M)) \notin w_1 \cap \Gamma$ (By lemma 5.7, $w \underset{L}{\longrightarrow}^{\rho}_{A} w_1$)
$\Leftrightarrow (A \, sent \, \rho(M)) \in w_1 \cap \Gamma$
and $(\Box_A unfresh \, \rho(M)) \notin w_1 \cap \Gamma$ (By $I$, $T$)
$\Leftrightarrow A \, \mathsf{sends} \, \rho(M) \in Actions^+(w_1 \cap \Gamma)$
$\Leftrightarrow A \, \mathsf{sends} \, \rho(M) \in Actions(\theta_1^+)$ (Since $w_1 \rightsquigarrow h_1$)

□

**Lemma 5.11 (Filtration Condition iii)** *Assume that $h \sim^{\rho}_{A} h'$ in $\mathcal{I}_L$ and $w \rightsquigarrow h$. Then, there is $w' \in W_L$ such that $w' \rightsquigarrow h'$, and for all $(\Box_A F) \in \Gamma$: $w \models_{\mathcal{C}_L} \Box_A F \Rightarrow w' \models_{\mathcal{C}_L} \rho(F)$.*

**Proof.** Assume that $w \rightsquigarrow h$ and $h \sim^{\rho}_{A} h'$ in $\mathcal{I}_L$. Then, $h' \in H_L$, i.e., $w' \rightsquigarrow h'$ for some $w' \in W_L$. Assume $(\Box_A F) \in \Gamma$. Then,

$w \models_{\mathcal{C}_L} \Box_A F$
$\Rightarrow (\Box_A F) \in w \cap \Gamma$ (By lemma 5.5)
$\Rightarrow A \, \mathsf{int} \, F \in Actions^+(w \cap \Gamma)$
$\Rightarrow A \, \mathsf{int} \, F \in Actions(h)$ (By $w \rightsquigarrow h$)
$\Rightarrow A \, \mathsf{int} \, \rho(F) \in Actions(h')$ (By $h \sim^{\rho}_{A} h'$)
$\Rightarrow A \, \mathsf{int} \, \rho(F) \in Actions^+(w' \cap \Gamma)$ (By $w' \rightsquigarrow h'$)
$\Rightarrow \Box_A \rho(F) \in w'$
$\Rightarrow \rho(F) \in w'$ (By axiom $T$)
$\Rightarrow w' \models_{\mathcal{C}_L} \rho(F)$ (By lemma 5.5)

□

Having thus established all three filtration conditions, we know that $\rightsquigarrow$ is a filtration.

**Corollary 5.12** *$\rightsquigarrow$ is a $\Gamma$-filtration from the canonical counterpart model to the canonical interpreted system.*

**Proof.** From lemmas 5.9, 5.10 and 5.11. □

To reach completeness theorem 5.2, it remains to be shown that $\mathcal{I}_L$ is inductive.

**Lemma 5.13** *The canonical interpreted system is inductive.*

**Proof.** We show first that the canonical interpretation function $I_L$ is fixed point. Assume that $w \rightsquigarrow h$.

$h \models_{\mathcal{I}_L} A \, infers \, K$
$\Leftrightarrow A infers \, K \in w$ (Lemma 5.9)
$\Leftrightarrow \Box_A exists \, K \in w$ (Axiom *Red*)

$\Leftrightarrow h \models_{\mathcal{I}_L} \Box_A exists\, K$ (Lemmas 5.5 + 5.8, corollary 5.12 and $\Box_A exists\, K \in \Gamma$)

To show that $I_L$ is minimal, we show that if $K \in I_L(A\ infers, h)$ then $h \models_{\langle H_L, I' \rangle} \Box_A exists\ K$ for any interpretation function $I'$ on $H_L$.[14]

$K \in I_L(A\ infers, h)$ and $h \sim_A^\rho h'$ in $\langle H_L, I' \rangle$ (24)
$\Rightarrow K \in messages(h|A)$ (From (20) and (24)) (25)
$\Rightarrow \rho(h|A) = h'|A$ (From (24)) (26)
$\Rightarrow \rho(K) \in messages(h'|A)$ (From (25) + (26))
$\Rightarrow \rho(K) \in I'(exists, h')$
$\Rightarrow h' \models_{\langle H_L, I' \rangle} exists\, \rho(K)$
$\Rightarrow h \models_{\langle H_L, I' \rangle} \Box_A exists K$ (Since $h'$ and $\rho$ are arbitrary)

□

**Lemma 5.14 (Finite Model Property)** *If $\not\vdash_{L\boldsymbol{A}} F$, there is a finite system $H \in \|\boldsymbol{A}\|$ such that $\not\models_H F$.*

**Proof.** From canonical model corollary 5.6, filtration lemma 5.8, lemma 5.12 and lemma 5.13. Assume that $\not\vdash_{L\boldsymbol{A}} F$. From canonical model corollary 5.6, $\not\models_{\mathcal{C}_{L\boldsymbol{A}}} F$ and $\models_{\mathcal{C}_{L\boldsymbol{A}}} \boldsymbol{A}$. Let $\Gamma$ be the smallest set closed under message permutations and sub-statements, and containing $F$ and $\boldsymbol{A}$, and containing all atomic statements, containing $\Box_A A\ received\ M$, $\Box_A A\ sent\ M$, $\Box_A exists\ M$, $\Box_A A\ infers\ M$ and $\Box_A unfresh\, M$, for all $A \in \mathcal{A}$ and messages $M$. $\Gamma$ is finite, since $\boldsymbol{A}$ is finite. By filtration lemma 5.8, lemma 5.12 and lemma 5.13, $\not\models_{H_{L\boldsymbol{A}}} F$ and $\models_{H_{L\boldsymbol{A}}} \boldsymbol{A}$, where $H_{L\boldsymbol{A}}$ is the canonical system for theory $L\boldsymbol{A}$ and filtration set $\Gamma$. By construction, $H_{L\boldsymbol{A}}$ is finite, as $\Gamma$ is finite. □

From Finite Model Property 5.14, we immediately get completeness theorem 5.2. By soundness and the proof of completeness it is not difficult to find a bound $n$ such that $F \in L\boldsymbol{A}$, if and only if, $F$ is valid in all systems in $\|A\|$ with at most $n$ histories, each of size less than $n$. This is sufficient to establish Decidability Theorem 5.3.

## 6 Conclusion

Several Kripke semantics for BAN have been proposed in the literature. However, no logic faithful to BAN is complete with respect to Kripke semantics, due to the logical omniscience problem. Indeed, there have been no completeness results so far for BAN and BAN-like logics.

Adopting a recently proposed generalization of Kripke semantics that avoids logical omniscience, we have shown that a logic faithful to BAN, with full boolean operators, is decidable, and that it is sound and complete with respect to message passing systems. Completeness and decidability generalize

[14] The interpretation of predicates other than *infers* is fixed.

to logics induced by an arbitrary theory base. The theory base may express how participants in a specific protocol are expected to behave, or state general assumptions about the network, such as origination assumptions. Since the theory base is arbitrary, the completeness result helps to bring out that validity is faithful to BAN, not only validity with respect to all systems, but also validity with respect to selected classes of systems. Clearly, applications such as model checking require this stronger form of faithfulness.

In the future, we intend to explore model checking of BAN logic specifications, transferring techniques [13] from standard Kripke semantics.

*Acknowledgments*

Work was partially supported by the Swedish Research Council project 621-2003-2597. Also, the second author was supported by a personal grant from the Swedish Research Council.

## References

[1] Abadi, M. and M. Tuttle, *A semantics for a logic of authentication*, in: *PODC'91*, 1991, pp. 201–216.

[2] Bieber, P., *A logic of communication in hostile environments.*, in: *Third IEEE Computer Security Foundations Workshop (CSFW'90)* (1990), pp. 14–22.

[3] Bleeker, A. and L. Meertens, *A semantics for ban logic*, in: *Proceedings DIMACS Workshop on Design and Formal Verification of Protocols* (1997).

[4] Burrows, M., M. Abadi and R. M. Needham, *A logic of authentication.*, ACM Trans. Comput. Syst. **8** (1990), pp. 18–36.

[5] Cohen, M., "Logics of knowledge and cryptography: Completeness and Expressiveness," Ph.D. thesis, KTH Royal Institute of Technology (2007).

[6] Cohen, M. and M. Dam, *Logical omniscience in the semantics of BAN logic*, in: *Foundations of Computer Security (FCS'05)*, 2005, pp. 121–132.

[7] Dekker, A. H., *C3P0: A tool for automatic sound cryptographic protocol analysis.*, in: *Proceedings of the 13th IEEE Computer Security Foundations Workshop (CSFW'00)* (2000), pp. 77–87.

[8] Dolev, D. and A. C.-C. Yao, *On the security of public key protocols.*, IEEE Transactions on Information Theory **29** (1983), pp. 198–207.

[9] Fagin, R., J. Y. Halpern, Y. Moses and M. Y. Vardi, "Reasoning About Knowledge," MIT Press, 1995.

[10] Gong, L., R. M. Needham and R. Yahalom, *Reasoning about belief in cryptographic protocols.*, in: *IEEE Symposium on Security and Privacy* (1990), pp. 234–248.

[11] Halpern, J. Y. and R. Pucella, *Modeling adversaries in a logic for security protocol analysis.*, in: A. E. Abdallah, P. Ryan and S. Schneider, editors, *Formal Aspects of Security, First International Conference (FASec 2002)*, Lecture Notes in Computer Science **2629** (2002), pp. 115–132.

[12] Halpern, J. Y., R. Pucella and R. van der Meyden, *Revisiting the foundations of authentication logics*, *Manuscript* (2003).

[13] Kacprzak, M., A. Lomuscio, A. Niewiadomski, W. Penczek, F. Raimondi and M. Szreter, *Comparing BDD and SAT based techniques for model checking Chaum's Dining cryptography protocol*, Fundamenta Informaticae **72** (2006), pp. 215–234.

[14] Kindred, D. and J. Wing, *Losing the idealization gap with theory generation*, in: *Proceedings of the DIMACS Workshop on Cryptographic Protocol Design and Verification* (1997), pp. 3–5.

[15] Lewis, D., *Counterpart theory and quantified modal logic*, Journal of Philosophy **65** (1968), pp. 113–126.

[16] Lomuscio, A., F. Raimondi and B. Wozna, *Verification of the Tesla protocol in MCMAS-X*, Fundamenta Informaticae **79 (3-4)** (2007), pp. 473–486.

[17] Needham, R. M. and M. D. Schroeder, *Using encryption for authentication in large networks of computers*, Commun. ACM **21** (1978), pp. 993–999.

[18] Parikh, R. and R. Ramanujam, *Distributed processes and the logic of knowledge.*, in: R. Parikh, editor, *Logics of Programs*, Lecture Notes in Computer Science **193** (1985), pp. 256–268.

[19] Pucella, R., "Reasoning about Resource-Bounded Knowledge: Theory and Application to Security Protocol Analysis," Ph.D. thesis, Cornell University (2004).

[20] Syverson, P. F., *Towards a strand semantics for authentication logics*, in: *Electronic Notes in Theoretical Computer Science*, 20,2000.

[21] Syverson, P. F. and P. C. van Oorschot, *On unifying some cryptographic protocol logics*, in: *Proc. IEEE Symposium on Research in Security and Privacy* (1994), pp. 14–28.

[22] Syverson, P. F. and P. C. van Oorschot, *A unified cryptographic protocol logic*, NRL Publication 5540-227, Naval Research Lab (1996).

[23] Teepe, W., "Reconciling Information Exchange and Confidentiality — A Formal Approach," Ph.D. thesis, Rijksuniversiteit Groningen (2006).

[24] Toussaint, M.-J. and P. Wolper, *Reasoning about cryptographic protocols*, in: J. Feigenbaum and M. Merritt, editors, *Distributed Computing and Cryptography*, DIMACS Series in Discrete Mathematics and Theoretical Computer Science **2**, American Mathematical Society, 1989 pp. 245–262.

[25] van der Meyden, R. and K. Su, *Symbolic model checking the knowledge of the dining cryptographers*, in: *17th IEEE workshop on Computer Security Foundations (CSFW '04)* (2004), p. 280.

[26] Wedel, G. and V. Kessler, *Formal semantics for authentication logics.*, in: E. Bertino, H. Kurth, G. Martella and E. Montolivo, editors, *Computer Security - ESORICS 96, 4th European Symposium on Research in Computer Security*, Lecture Notes in Computer Science **1146** (1996), pp. 219–241.