A Completeness Result for BAN Logic

Mika Cohen Mads Dam

KTH Royal Institute of Technology, Stockholm, Sweden
{*mikac,mfd*}*@imit.kth.se*

Abstract

BAN logic is an epistemic logic for verifying cryptographic protocols. While BAN has been quite successful from a practical point of view, the semantics of the epistemic modality is controversial. 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 can draw all logical consequences of their knowledge. To avoid logical omniscience, we index the epistemic possibility relation of Kripke semantics with a message renaming, relating how cipher texts at the current state correspond to cipher texts at the epistemically possible state. An agent is said to know a statement if corresponding statements hold at epistemically possible states. We obtain completeness with respect to message passing systems and decidability by transferring canonical model and filtration constructions from Kripke semantics.

Keywords: BAN Logic, Completeness, Decidability, Logical Omniscience

1 Introduction

BAN logic [4] is an epistemic logic proof system for reasoning about cryptographic protocols. Since BAN was introduced in the late eighties, a substantial amount of work has been done applying, varying and clarifying BAN (cf. [1,2,5,6,8,10,11,12,13,15]). However, BAN's central language construct, the epistemic modality, has no agreed upon semantics. The confusion around the semantics hampers the application of semantically based methods, and makes it difficult to evaluate variations to the proof system.

Any interpretation of cryptographic knowledge faces the so-called logical omniscience problem [7]: According to the intended, informal meaning of knowledge, agents can only perform computationally feasible cryptographic

⋆ Work supported by the Swedish Research Council grants 621-2003-2597 and 622-2003-6108

calculations, whereas in the standard semantics for knowledge, Kripke semantics, agents draw arbitrary logical inferences, including computationally unjustified cryptographic calculations. To illustrate, under BAN's idealized cryptography we get the validity $\mathit{fresh}\, M \models \mathit{fresh}\, \{M\}_K$, which, in Kripke semantics, yields the entailment $a\ \mathit{knows}\ \mathit{fresh}\, M \models a\ \mathit{knows}\ \mathit{fresh}\, \{M\}_K$. However, the latter entailment 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. From the point of view of modal logic, the example shows the failure of the rule of normality that allows inference of an entailment $a, \mathit{knows}\, F \models a\, \mathit{knows}\, F'$ from the entailment $F \models F'$. We refer to [5] for additional counterexamples to the rule of normality.

In Kripke semantics, the knowledge of an agent a at a state s is determined by the data $s|a$ available to a at s. An agent knows a statement if her available data entail the statement. Thus, logical omniscience (rule of normality) is inescapable, no matter how $s|a$ is defined. As it happens, all semantics for BAN-like logics, except for [5], are based on Kripke semantics [1,6,10,11,12,13,15]. Therefore, as the above example illustrates, every extension to BAN is incomplete with respect to these semantics, assuming the extension is faithful to the intended meaning in BAN. Indeed, existing work have so far been limited to soundness results.

Recently, we proposed a generalized Kripke semantics that avoids logical omniscience [5]. There, we established some of the basic properties of the semantics, including soundness. Here we extend this work to show that a faithful version of BAN is complete with respect to message passing systems [7], and that it is decidable. We emphasize that completeness for original BAN [4] cannot be expected, since original BAN, as its authors make clear, leaves out rules that are validated by any reasonable semantics.

The key intuition is that two different cipher texts can be indistinguishable to an agent, due to her limited decryption power. Thus, a cipher text $\{M\}_K$ which the agent cannot decrypt might as well, for all the agent knows, be some other cipher text $\{M'\}_{K'}$. In this sense, $\{M'\}_{K'}$ is an epistemically possible interpretation of $\{M\}_K$. More generally, we can think of a 1-1 mapping r between messages as a joint interpretation of all messages. For each state and agent we identify, based on the keys available to the agent, a set of epistemically possible joint interpretations. We say that agent a knows a statement $F(\{M\}_K)$ at state s, if for every possible joint interpretation r, the reinterpreted data $r(s|a)$ entails the reinterpreted statement $F(r(\{M\}_K))$. This semantics departs from Kripke semantics, in that we check the renamed cipher text $r(\{M\}_K)$ instead of the predicated cipher text $\{M\}_K$. As a result, logical omniscience is avoided.

We present an axiomatization of validity with respect to our semantics. The axiomatization uses standard modal axioms *K*, *T*, *S4* and *S5*, but excludes the rule of necessitation. The latter is weakened so that agents can only infer "feasibly computable" theorems. The axiomatization employs, in addition,

some axioms specific to message passing systems, including an epistemic axiom stating that an agent knows if she sent or received a message. We obtain completeness and decidability by transferring canonical model and filtration constructions from Kripke semantics.

Our semantics is a variation on counterpart semantics, a semantics for first order modal logic due to [9]. Epistemically possible mappings between messages are related to the message congruences of [1], and to the states of knowledge and belief of [3,14].

2 Message Passing Systems

In a message passing system agents take turns to send messages, receive messages or perform unspecified internal actions [7]. For the sake of brevity, we omit the customary initialization action, i.e., a special action that establishes initial shared or private secrets. We also use a simple, perhaps simplistic, notion of session along the lines of [1].

Assume a non-empty set of keys $K, K', ...$, a non-empty set of plain-texts $T, T', ...$, including a finite set A of agent names $a, b, ...$ Messages are generated by:

$$M ::= \ K \mid T \mid M \cdot M \mid \{M\}_K$$

where $\cdot$ represents pairing and $\{\ \}$ represents symmetric encryption. The submessage relation $\geq$ is the smallest binary relation on messages such that $M \geq M$, $\{M\}_K \geq M$, $\{M\}_K \geq K$, $M \cdot M' \geq M$ and $M \cdot M' \geq M'$. 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: A message M is, from now on, a message in this fixed space.

Actions are:

$$\sigma ::= \ a\,\texttt{sends}\,M \mid a\,\texttt{receives}\,M \mid a\,\mathit{int}\,M \mid \texttt{begin}\,\texttt{session}$$

where agent a is in A or is the special agent `env`, the environment, and *int* ranges over a finite set of internal action types. Write $\sigma(M)$ for an action in the message term M. A history, or action trace, is a finite sequence h of actions. Write $\mathit{Actions}(h)$ for the set of all actions in h: $\mathit{Actions}(\epsilon) = \emptyset$ and $\mathit{Actions}(h \cdot \sigma) = \mathit{Actions}(h) \cup \{\sigma\}$. A message passing system, or *system* for short, is a non-empty set H of histories.

The local history of agent a in history h, in symbols $h|a$, is the sequence of actions performed by a in h: $\epsilon|a = \epsilon$, if $\sigma \in \{a\,\texttt{sends}\,M,\ a\,\texttt{receives}\,M,\ a\,\mathit{int}\,M\}$ then $(h \cdot \sigma)|a = h|a \cdot \sigma$ else $(h \cdot \sigma)|a = h|a$.

A key assignment κ on H assigns a set $\kappa(a, h)$ of keys, the keys used by a at h for encryption and decryption, to each agent $a \in A$ and history $h \in H$. A model on H is a pair $\mathcal{M} = \langle H, \kappa \rangle$, where κ is a key assignment on H. We leave κ undefined until Section 5.

3 Language of Full Propositional BAN

An atomic statement is a predicate p applied to a message M:

$$p(M) ::= \ a\ received\ M \mid a\ rec\ M \mid a\ sent\ M \mid a\ sen\ M \mid old\ M$$

The meaning of atomic statements is straightforward: $a\ received\ M$ holds if agent a received message M from the network, $a\ rec\ M$ holds if M is a sub-message of some message a received. [1] The intended meaning of $a\ sent\ M$ and $a\ sen\ M$ are analogous. The statement $old\ M$ holds if M is a sub-message of some message sent in an old session, i.e., prior to a `begin session` event. We note that, unlike BAN like languages in the literature, atomic statements do not involve any notion of "feasible cryptographic computation". In particular, atomic statements do not depend on the keys used by agents. Statements are generated by:

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

where $\Box_a$ is the epistemic modality for a, read "agent a knows that". Define disjunction ($\vee$) and implication ($\rightarrow$) in the usual way. Let $G \subseteq A$. We introduce BAN predicates as abbreviations, similar to [10]:

- $a\ sees\ M = \Box_a a\ rec\ M$
- $a\ said\ M = \Box_a a\ sen\ M$
- $M\ secret\ of\ G = \bigwedge_{a \notin G} \neg\, a\ sees\ M$
- $fresh\ M = \neg\ old\ M$

The language defined above differs somewhat from the original BAN [4]. Firstly, original BAN has some constructs for asymmetric cryptography. Secondly, there is no negation operator in original BAN. Thirdly, original BAN includes messages that contain statements, so called idealized messages. 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 [10].

4 Semantics

In Kripke semantics, the epistemic modality $\Box_a$ is interpreted through an epistemic possibility relation $\longrightarrow_a$ between states, in our case histories. Intuitively, $h \longrightarrow_a h'$ means that at history h agent a could, for all she knows, be at h'. The epistemic possibility relation has a default definition in computer science, due to [7]: $h \longrightarrow_a h'$, if and only if, $h|a = h'|a$. However, because of the the limited decryption power of agents, there may be more than one way for the agent to interpret the cipher texts she has sent, received

[1] If we include initialization actions in histories, $a\ rec\ M$ also holds if M is a sub-message of some "initial secret" of a.

or otherwise acted upon. Consider, for example, a model $\mathcal{M}_0 = \langle H_0, \kappa_0 \rangle$ where H_0 has three execution histories, $h_0 = b\,\mathsf{sends}\,\{M\}_K \cdot a\,\mathsf{receives}\,\{M\}_K$, $h_1 = b\,\mathsf{sends}\,\{M'\}_{K'} \cdot a\,\mathsf{receives}\,\{M'\}_{K'}$ and $h_2 = b\,\mathsf{sends}\,\{M\}_K$, and agent a does not use any keys, i.e., $\kappa_0(a, h_0) = \kappa_0(a, h_1) = \kappa_0(a, h_2) = \emptyset$. Even though $h_0|a \neq h_1|a$, it may still be reasonable to say that at h_0, agent a could, for all she knows, be at h_1. Based on such intuitions, the AT semantics [1] and its descendants [13,15] drop the requirement of local history identity, in effect hiding cryptographically inaccessible parts of the local history from the agent herself.

We depart from AT semantics, and from Kripke semantics in general, by extending the epistemic uncertainty to predicated cipher texts. To illustrate, the cipher text $\{M\}_K$ at h_0 in the above model $\mathcal{M}_0$, could, for all agent a knows, be the cipher text $\{M'\}_{K'}$ at h_1. Everything a observes of $\{M\}_K$ at h_0, a also observes of $\{M'\}_{K'}$ at h_1. In this sense, $\{M'\}_{K'}$ at h_1 corresponds for a to $\{M\}_K$ at h_0. In general, a message sequence $M'_0, M'_1, \cdots$ at h_1 may correspond for a to another message sequence $M_0, M_1, \cdots$ at h_0. In order to keep track of message correspondences, we therefore relativize the epistemic possibility relation to a message renaming, a $1-1$ function r on the set of messages. Informally, $h \longrightarrow_a^r h'$ if any message sequence $M_0, M_1, \cdots$ at h could, for all a knows, be the sequence $r(M_0), r(M_1), \cdots$ at h'. We extend a renaming to statements by renaming the message terms inside a statement: $r(p(M)) = p(r(M))$, $r(\Box_a F) = \Box_a r(F)$, etc. Then renamings are extended to sets of statements by renaming each statement in a set: $r(\Delta) = \{r(F) \mid F \in \Delta\}$ for any set Δ of statements, and, finally, to sets of messages by renaming each message in a set: $r(\Pi) = \{r(M) \mid M \in \Pi\}$ for any set Π of messages.

Assuming the the relativized epistemic possibility relation, we say that an agent knows a statement if corresponding statements hold at epistemically possible histories:

$$h \models_{\mathcal{M}} \Box_a F \Leftrightarrow \forall r : \forall h' \in H : h \longrightarrow_a^r h' \Rightarrow h' \models_{\mathcal{M}} r(F)$$

The break with Kripke semantics should be clear. We check a renamed statement $r(F)$ at h', and not the original statement F.

For $h \longrightarrow_a^r h'$ to hold, we require that r respects the observations (actions) of a in h as well as the message structure accessible through a:s keys at h. The former requirement means that

- $r(h|a) = h'|a$

where r is extended to histories by point-wise renaming each message acted upon in the history: $r(\epsilon) = \epsilon$ and $r(h \cdot \sigma(M)) = r(h) \cdot \sigma(r(M)))$. For the latter requirement, we simply assume a *transparency relation* $\lhd$, which determines if a renaming r respects structure accessible with a set Π of keys: $r \lhd \Pi$, if Π cannot distinguish a message, a history or a statement from its renaming under r. We leave the definition of $\lhd$ open, merely insisting on four requirements:

- $r \lhd \Pi,\ \Pi \supseteq \Pi' \Rightarrow r \lhd \Pi'$ (Monotonicity)

- $\iota \lhd \Pi$, where ι is identity of messages (Reflexivity)
- $r \lhd \Pi,\ r' \lhd r(\Pi) \Rightarrow (r' \circ r) \lhd \Pi$ (Transitivity)
- $r \lhd \Pi \Rightarrow r^{-1} \lhd r(\Pi)$ (Symmetry)

For example, we may stipulate that $r \lhd \Pi$, if and only if, r respects encryption with keys in Π:

(i) $k \in \Pi \Rightarrow r(\{M\}_k) = \{r(M)\}_{r(k)}$ (Encryption)

and r respects clear text constructions:

(ii) $r(M \cdot M') = r(M) \cdot r(M')$ (Pairing)

(iii) $r(T) = T$, plain text T (Plain text)

So defined, $\lhd$ is monotone, reflexive, transitive and symmetric [5]. We say that $\lhd$ respects encryption, if, for all r and Π, $r \lhd \Pi$ implies that r respects encryption with keys in Π. Similarly, we say that $\lhd$ respects pairing/plain text, if, for all r and Π, $r \lhd \Pi$ implies that r respects paring/ plain text. Note that any $\lhd$ is finite. (Since the message space is finite, there are finitely many sets Π of keys and finitely many renamings r.) Putting the two requirements on $\longrightarrow_a^r$ together, we stipulate:

$$h \longrightarrow_a^r h' \text{ in } \mathcal{M} \Leftrightarrow r(h|a) = h'|a \ \&\ r \lhd \kappa(a, h)$$

Truth conditions for Boolean operators and atomic statements are as expected: $h \models_{\mathcal{M}} \neg F$, if and only if, $h \not\models_{\mathcal{M}} F$; $h \models_{\mathcal{M}} F \wedge F'$, if and only if, $h \models_{\mathcal{M}} F$ and $h \models_{\mathcal{M}} F'$; $h \models_{\mathcal{M}} a \mathit{\ received\ } M$, if and only if, $a \,\texttt{receives}\, M \in \mathit{Actions}(h)$; $h \models_{\mathcal{M}} a \mathit{\ sent\ } M$, if and only if, $a \,\texttt{sends}\, M \in \mathit{Actions}(h)$; $h \models_{\mathcal{M}} a \mathit{\ rec\ } M$, if and only if, M is a sub-message of some M' such that $a \,\texttt{receives}\, M' \in \mathit{Actions}(h)$; $h \models_{\mathcal{M}} a \mathit{\ sen\ } M$, if and only if, M is a sub-message of some M' such that $a \,\texttt{sends}\, M' \in \mathit{Actions}(h)$; $h \models_{\mathcal{M}} \mathit{old\ } M$, if and only if, for some h' and h'', $h = h' \cdot \texttt{begin session} \cdot h''$ and $h' \models_{\mathcal{M}} a \mathit{\ rec\ } M \vee a \mathit{\ sen\ } M$ for some $a \in A \cup \{\texttt{env}\}$. Finally, statement F is valid in model $\mathcal{M}$ if $h \models_{\mathcal{M}} F$, for all $h \in H$.

Returning to the example $\mathcal{M}_0$ above, $h_0 \models_{\mathcal{M}_0} \Box_a a \mathit{\ received\ } \{M\}_K$, since if $h_0 \longrightarrow_a^r h_0$ then $r(\{M\}_K) = \{M\}_K$ and if $h_0 \longrightarrow_a^r h_1$ then $r(\{M\}_K) = \{M'\}_{K'}$. On the other hand, $h_0 \not\models_{\mathcal{M}_0} \Box_a a \mathit{\ rec\ } M$, since there is some r such that $h_0 \longrightarrow_a^r h_1$ and $r(M) = M$, assuming that $\lhd$ is non-degenerate. As the implication $a \mathit{\ received\ } \{M\}_K \rightarrow a \mathit{\ rec\ } M$ is valid, the example illustrates that agents need not be logically omniscient.

The relativized possibility relation implicitly contains an AT-like possibility relation: $h \longrightarrow_a h'$, if and only if, there exists a renaming r such that $h \longrightarrow_a^r h'$. Thus, $h \longrightarrow_a h'$ if $h'|a$ is a possible interpretation of $h|a$. With the existential quantification over renamings r we lose the information how cipher texts at h may correspond for a to cipher texts at h'.

5 Inductive Key Assignment

We left the key assignment κ open. We now stipulate that the keys used are the keys seen. This requires a recursive definition, since *a sees* is defined in terms of $\Box_a$, which in turn is interpreted through κ itself. An inductive, rather than a coinductive definition is appropriate, since κ should assign the set of keys that the agent has gathered some positive information about. We call a key assignment κ inductive on system H, if κ is a minimal (with respect to point-wise subset inclusion) key assignment such that

$$K \in \kappa(a,h) \Leftrightarrow h \models_{\langle H,\kappa\rangle} \Box_a a \, rec \, K$$

for all $a \in A$, $h \in H$ and keys K. A model $\langle H, \kappa\rangle$ is inductive if κ is inductive on H.

Theorem 5.1 (Existence of Inductive Key Assignment) *There exists a unique inductive key assignment on every message passing system.*

Proof. An inductive key assignment on H is, by definition, a least fixed point of the following function f assigning a key assignment $f(\kappa)$ to every key assignment κ: $f(\kappa)(a,h) = \{K \mid h \models_{\langle H,\kappa\rangle} \Box_a \, a \, rec \, K\}$. Function f is monotone, as $\lhd$ is monotone and the extension of *a rec* is independent of the key assignment. [2] Therefore, f has a unique least fixed point. □

In inductive models, the relativized epistemic possibility relation generalizes an equivalence relation on histories.

Lemma 5.2 *In inductive models:*

(i) $h \longrightarrow_a^{\iota} h$

(ii) $h \longrightarrow_a^{r} h'$, $h' \longrightarrow_a^{r'} h'' \Rightarrow h \longrightarrow_a^{r' \circ r} h''$

(iii) $h \longrightarrow_a^{r} h' \Rightarrow h' \longrightarrow_a^{r^{-1}} h$

Proof. (1): From reflexivity of $\lhd$. (2): From transitivity of $\lhd$ and fixed point induction. (3): From symmetry of $\lhd$ and fixed point induction. For more detail, we refer to [5]. □

As Lemma 5.2.iii shows, the apparent asymmetry in the definition of the epistemic possibility relation disappears in inductive models. From now on, if no key assignment is given, we assume the inductive key assignment: $h \models_H F$, if and only if, $h \models_{\mathcal{M}} F$ for the inductive model $\mathcal{M}$ based on H; F is valid in H if $h \models_H F$, for all $h \in H$.

Many semantics proposed for BAN logics give a more straightforward, operational definition of seen messages and used keys. Roughly, a message is seen if it was received, or if it is the first or second pairing component of a

[2] This independence is preserved if we include initialization actions in histories, and make *a rec* apply also to sub-messages of "initial secrets" of a.

seen message, or if it is the body of a seen cipher text locked with a seen key. A key is used if it is seen. To illustrate, at a history $h_0 = b \,\mathsf{sends}\, K \cdot \{K' \cdot \{K''\}_{K''}\}_K \cdot a \,\mathsf{receives}\, K \cdot \{K' \cdot \{K''\}_{K''}\}_K$ agent a uses the keys K and K'. In fact, the inductive key assignment is at least as inclusive as this operational key assignment, assuming that $\lhd$ respects pairing and encryption. For instance, key K is in the second iteration of the fixed point definition of $\kappa(a, h_0)$, and K' is in the third. A forthcoming full version of [5] shows the inclusion and under what conditions the inductive and the operational key assignments coincide. We refer to [5] for examples of when the operational key assignment might be inappropriately weak.

6 BAN Theories

A BAN theory is a set L of statements containing all axioms and closed under all rules in Table 1, where axiom *Taut* consists of all tautologies from classical propositional logic, and a *sees* $\Pi = \bigwedge_{K \in \Pi} a$ *sees* K, with the empty conjunction abbreviating some tautology. When $F \in L$, we write $\vdash_L F$ and say that F is a theorem of L. The axioms and rules in Table 1 isolate "feasible cryptographic computation" to one point, namely renaming necessitation (*RNec*). According to *RNec*, an agent knows all theorems that are preserved under renamings transparent to seen keys. Since there are finitely many renamings, *RNec* is finitary, i.e., involves a finite set of premisses. The introspection axiom I says that an agent knows if she sent or received a message. Axioms K, T, *4* and *5* are standard. The remaining axioms and rule are non-epistemic. Axiom *Mono* says that *a rec*, *a sen* and *old* are monotone with respect to $\geq$. The disjunctions in axioms *R2* and *S2* are finite, since there are only finitely many messages.

Let Δ be a set of statements, possibly infinite. Write $\Delta \vdash_L F$, if there is a finite subset $\{F_1, ..., F_n\} \subseteq \Delta$ such that $\vdash_L F_1 \to (F_2 \to (\cdots \to (F_n \to F) \cdots))$. Write $\Box_a \Delta$ for $\{\Box_a F \mid F \in \Delta\}$. We have the following weakening of normality.

Lemma 6.1 (Renaming Normality) *If* $r(\Delta) \vdash_L r(F)$ *for all* $r \lhd \Pi$*, then* a *sees* Π, $\Box_a \Delta \vdash_L \Box_a F$.

Proof. Assume $r(\Delta) \vdash_L r(F)$, $\forall r \lhd \Pi$. Since the message space is finite, there are only finitely many renamings. Let $r_1, ..., r_n$ be all renamings r such that $r \lhd \Pi$. For each $i \in \{1, ..., n\}$ there is a finite $\Delta_i \subseteq \Delta$ such that $r_i(\Delta_i) \vdash_L r_i(F)$. Thus for each $i \in \{1, ..., n\}$: $r_i(\Delta_1, ..., \Delta_n) \vdash_L r_i(F)$. Since $\Delta_1, ..., \Delta_n$ is finite, by rule *RNec* and axiom K: a *sees* Π, $\Box_a \Delta_1, ..., \Box_a \Delta_1 \vdash_L \Box_a F$. Since $\Delta_i \subseteq \Delta$: a *sees* Π, $\Box_a \Delta \vdash_L \Box_a F$. □

Since the renaming normality rule only closes knowledge under "feasibly computable" logical implications, BAN theories can avoid the absurdities of

K	$\Box_a(F \to F') \to \Box_a F \to \Box_a F'$
T	$\Box_a F \to F$
4	$\Box_a F \to \Box_a \Box_a F$
5	$\neg\Box_a F \to \Box_a \neg\Box_a F$
RNec	$\dfrac{r(F),\ \ \forall r \lhd \Pi}{a\ sees\ \Pi \to \Box_a F}$
I	$\pi_a \to \Box_a \pi_a,\ \ \pi_a \in \{a\ received\ M, a\ sent\ M\}$
Mono	$p(M) \to p(M'),\ M \geq M',\ p \in \{a\ rec, a\ sen, old\}$
R	$a\ received\ M \to a\ rec\ M$
S	$a\ sent\ M \to a\ sen\ M$
R2	$a\ rec\ M \to \bigvee_{M' \geq M} a\ received\ M'$
S2	$a\ sen\ M \to \bigvee_{M' \geq M} a\ sent\ M'$
Taut	F, F tautology from propositional logic
MP	$\dfrac{F \quad F \to F'}{F'}$

Table 1
Axioms and Rules

logical omniscience. For instance, a BAN theory need *not* contain:

$$a\ rec\ M \to \Box_a a\ rec\ M \tag{1}$$
$$\Box_a fresh\ M \to \Box_a fresh\ \{M\}_K \tag{2}$$

This follows from Soundness Theorem 7.1. In contrast, if a BAN theory L satisfies the rule of normality, i.e., if $\Delta \vdash_L F$ implies that $\Box_a \Delta \vdash_L \Box_a F$, then L contains (1) and (2); Normality and axioms I, R, $R2$ and *Mono* give (1), while normality and axiom *Mono* yield (2). As the following fact illustrates, BAN theories contain a significant part of original BAN [4].

Corollary 6.2 *Assume $\lhd$ respects pairing and encryption. Then every BAN theory contains the following, where $s_a \in \{a\ sees, a\ said\}$*

(i) $\Box_a fresh\ M \to \Box_a fresh\ (M \cdot M')$

(ii) $\Box_a fresh\ M \to (a\ sees\ K \to \Box_a fresh\ \{M\}_K)$

(iii) $\Box_b s_a\ (M \cdot M') \to \Box_b s_a\ M$

(iv) $\Box_b s_a\ (M \cdot M') \to \Box_b s_a\ M'$

(v) $s_a\,\{M\}_K \rightarrow (a\ sees\, K \rightarrow s_a\, M)$

(vi) $s_a\, M \rightarrow \Box_a s_a\, M$

(vii) $\neg s_a\, M \rightarrow \Box_a \neg s_a\, M$

(viii) $a\ received\, M \rightarrow a\ sees\, M$

Proof. (1), (3) and (4): Axiom *Mono*, renaming normality (Lemma 6.1) and $\triangleleft$ respects pairing. (2) and (5): Axiom *Mono*, renaming normality and $\triangleleft$ respects encryption. (6): Axiom *4*. (7): Axiom *5*. (8): Axioms I and R and renaming normality. □

The well-known message meaning rule (in our setting: axiom) of BAN is conspicuously absent in Corollary 6.2. To obtain this axiom for a group G of agents , we need to assume an origination axiom for G:

$$K\ secret\ of\ G \rightarrow (b\ rec\ \{M\}_K \rightarrow \bigvee_{a \in G} (a\ said\ \{M\}_K \wedge a\ sees\ K) \qquad (3)$$

as well as an honesty axiom for G, where *from* is some special plain text atom:

$$\neg a\ said\ from \cdot b \cdot M, \text{ whenever } a \neq b, a \in G \qquad (4)$$

Corollary 6.3 (Message Meaning Axiom) *Assume $\triangleleft$ respects pairing, encryption and plain texts. Every BAN theory containing the origination axiom (3) and honesty axiom (4) for agent group G also contains:*

$$a\ sees \{from \cdot b \cdot M\}_K,\ a\ sees\, K,\ \Box_a K\, secret\ of\ G \rightarrow \Box_a\, b\, said\, M,\ b \in G$$

Proof. Immediate from renaming normality (Lemma 6.1) and that $\triangleleft$ respects plain texts, pairing and encryption. □

The message meaning axiom in Corollary 6.3 weakens the original in [4] by adding to the antecedent that agent a uses (sees) the key K, as in, for instance, [1,6,8]. We briefly illustrate BAN theories with protocol specific axioms.

Example 6.4 Consider the Needham-Schröder Shared Key Protocol 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:

$$s\ sen\, \{N \cdot b \cdot K \cdot M\}_{K_a},\ K_a\ secret\ of\ a \cdot s,\ fresh\, N \rightarrow K\ secret\ of\ a \cdot b \cdot s$$

If a BAN theory contains this protocol specific axiom, for all keys N, K and K_a and all messages M, contains the origination axiom 3 for agent group $\{a, s\}$, and assuming $\triangleleft$ respects pairing, encryption and plain texts, the BAN theory also contains the authentication specification:

$$a \textit{ sees } \{N \cdot b \cdot K \cdot \{K \cdot a\}_{K_b}\}_{K_a},\ \neg a \textit{ said } \{N \cdot b \cdot K \cdot \{K \cdot a\}_{K_b}\}_{K_a},$$
$$a \textit{ sees } K_a,\ \Box_a K_a \textit{secret of } a \cdot s,\ \Box_a \textit{fresh } N$$
$$\rightarrow \Box_a K \textit{ secret of } a \cdot b \cdot s$$

stating that if a sees the message from the server, did not send the same message herself, knows the key to this message, and knows that the nonce inside is fresh, then a knows that the key provided inside is secret between a, b and s. The derivation is by way of renaming normality (Lemma 6.1) and Corollary 6.2.

Corollary 6.3 and Example 6.4 suggest that we might be interested in BAN theories generated by adding various theory bases, *finite* sets $\boldsymbol{A}$ of statements. Note that the origination and honesty schemata in Corollary 6.3, as well as the protocol specific axiom schemata in Example 6.4, are indeed finite, since there are only finitely many messages. We define the BAN theory induced by $\boldsymbol{A}$, in symbols $L\boldsymbol{A}$, as the smallest BAN theory containing the finite set $\boldsymbol{A}$.

7 Main Results

Write $\|\Delta\|$ for the set of all message passing systems validating all statements in Δ. BAN theory L is sound with respect to a class $\mathcal{C}$ of message passing systems, if $\mathcal{C} \subseteq \|L\|$. BAN theory L is complete with respect to $\mathcal{C}$, if L contains all statements valid in all systems in $\mathcal{C}$.

Theorem 7.1 (Soundness) *$L\boldsymbol{A}$ is sound with respect to $\|\boldsymbol{A}\|$.*

Proof. Rule *RNec*: Since $\triangleleft$ is monotone. Axioms T, 4 and 5: From Lemma 5.2. Axiom I: Assume $h \models a \textit{ received } M$, i.e., $a\,\texttt{receives}\,M \in \textit{Actions}(h|a)$. Pick any $h' \in H$ and renaming r such that $h \longrightarrow_a^r h'$. Then $r(h|a) = h'|a$. Therefore, $a\,\texttt{receives}\,r(M) \in \textit{Actions}(h'|a)$, i.e., $h' \models a \textit{ received } r(M)$. Since h' and r were chosen at random, $h \models \Box_a a \textit{ received } M$. Analogously for $a \textit{ sent } M$. Remaining axioms and rule MP are immediate. □

Theorem 7.2 (Completeness) *$L\boldsymbol{A}$ is complete with respect to $\|\boldsymbol{A}\|$.*

Proof. Section 8. □

Thus, the protocol base semantically guarantees a specification only if the specification is a theorem. Contrast this with the usual verification practice in BAN, based on an open ended proof system: If your specification is unprovable, you conclude that either the base logic or your protocol assumptions are too weak [4].

Theorem 7.3 (Decidability) *$L\boldsymbol{A}$ is decidable.*

Proof. Section 8. □

8 Proof of Completeness and Decidability

We show completeness and decidability by transferring canonical model and filtration techniques from Kripke semantics. As a first step, we lift the semantics from message passing models to a more general class of structures, counterpart models. Next, we build a canonical counterpart model $\mathcal{C}_L$ that validates precisely the theorems of a given BAN theory L. For any finite set Γ of statements, $\mathcal{C}_L$ is transformed, while preserving truth values in Γ, into a finite message passing system $H_{L,\Gamma}$.

8.1 Canonical Counterpart Model

A counterpart model is a triple $\mathcal{C} = \langle W, \longrightarrow, I\rangle$, where W is a non-empty set of worlds (states), $\longrightarrow_a^r \subseteq W \times W$ for each agent $a \in A$ and renaming r, and $I(p, w)$ is a set of messages, the messages satisfying predicate p at w. Intuitively, $w \longrightarrow_a^r w'$ says that any M at w, could, for all a knows, be $r(M)$ at w'. The semantics of Section 4 is generalized in the obvious way: $w \models_{\mathcal{C}} p(M) \Leftrightarrow M \in I(p, w)$ and $w \models_{\mathcal{C}} \Box_a F \Leftrightarrow \forall r \forall w \in W : w \longrightarrow_a^r w' \Rightarrow w' \models_{\mathcal{C}} r(F)$. Truth conditions for boolean operators are unchanged.

Counterpart models are used in counterpart semantics for first order modal logic due to [9]. The truth condition above for knowledge is unorthodox, treating message terms the way counterpart semantics treats free variables.

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

Lemma 8.1 (Extension Lemma) *If $\Delta \nvdash F$, there is a maximal consistent set $\Delta' \supseteq \Delta$ such that $F \notin \Delta'$.*

Write $Keys(a, \Delta)$ for the set $\{K \mid a \text{ sees } K \in \Delta\}$. The canonical counterpart model for BAN theory L is $\mathcal{C}_L = \langle W_L, \underset{L}{\longrightarrow}, I_L\rangle$, where

- W_L is the set of all maximal L-consistent sets
- $w \underset{L}{\longrightarrow}_a^r w' \Leftrightarrow r \triangleleft Keys(a, w) \wedge \forall F : \Box_a F \in w \Rightarrow r(F) \in w'$
- $I_L(w, p) = \{M \mid p(M) \in w\}$

Lemma 8.2 (Truth lemma) $w \models_{\mathcal{C}_L} F \Leftrightarrow F \in w$.

Proof. By induction in (the number of statement operators in) F, using renaming normality (Lemma 6.1). 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:

$\Box_a F \notin w$

$\Rightarrow r(w\|a) \not\vdash r(F)$ & $r \triangleleft Keys(a,w)$, $\exists r$	(By renaming normality)	(5)
$\Rightarrow r(w\|a) \subseteq w'$ & $r(F) \notin w'$, $\exists w' \in W_L$	(By lemma 8.1)	(6)
$\Rightarrow w' \not\models_{\mathcal{C}_L} r(F)$	(By the ind. hyp.)	(7)
$\Rightarrow \forall F : \Box_a F \in w \Rightarrow r(F) \in w'$	(By (6))	(8)
$\Rightarrow w \underset{L}{\longrightarrow}{}^{r}_{a} w'$	(By (5) and (8))	(9)
$\Rightarrow w \not\models_{\mathcal{C}_L} \Box_a F$	(By (7) and (9))	

For the if-direction:

$\Box_a F \in w$ & $w \underset{L}{\longrightarrow}{}^{r}_{a} w'$ & $w' \in W_L$

$\Rightarrow r(F) \in w'$		
$\Rightarrow w' \models_{\mathcal{C}_L} r(F)$	(By the ind. ass.)	
$\Rightarrow w \models_{\mathcal{C}_L} \Box_a F$	(By the assumptions)	

□

8.2 Canonical Message Passing System

Given a finite set Γ of statements, we transform the canonical model into a finite inductive message passing model, while preserving truth values in Γ. Each $w \in W_L$ is transformed, in three steps, into a collection of histories that satisfy $w \cap \Gamma$. In the first step, w is collapsed into the finite set $w \cap \Gamma$. Secondly, this finite set is sequenced in different ways, yielding a collection of statement sequences. Thirdly, statements (in the sequences) are replaced by actions that "ground" them.

The first transformation step is trivial. For the second step, we consider various enumerations of statements. An enumeration of all statements in the language is *admissible* if it makes all atomic statements of the form *old M* appear prior to other kind of statements. In what follows, whenever we talk about *an enumeration e* we mean an admissible enumeration *e*. Any *e* induces a sequence $e(\Delta)$ from a set Δ of statements, obtained by removing all non-members of Δ from the enumeration *e*. For the third transformation step, we define an internal action to be of the form $a\,\texttt{int}\,F$, where F is any statement and $a \in A \cup \{\texttt{env}\}$.[3] We then take sequences s of statements to histories under a mapping *hist* as follows:

(i) $hist(\epsilon) = \epsilon$

(ii) $hist(s \cdot old\ M) = hist(s) \cdot \texttt{env sends}\ M \cdot \texttt{begin session}$

(iii) $hist(s \cdot a\ received\ M) = hist(s) \cdot a\ \texttt{receives}\ M$

(iv) $hist(s \cdot a\ sent\ M) = hist(s) \cdot a\ \texttt{sends}\ M$

[3] This assumes a slightly more general definition of internal action than that of Section 2. Alternatively, we could introduce $a\,\texttt{int}\,F$ as an abbreviation for an internal action of the form $a\ int\ M$.

(v) $hist(s \cdot \Box_a F) = hist(s) \cdot a \texttt{ int } F$

(vi) $hist(s \cdot F) = hist(s)$, otherwise

Condition (2) assures that every message which s claims is old, is old at $hist(s)$ according to the semantics of predicate *old*. Condition (3) sees to it that every message that s claims a received, a received at $hist(s)$ according to the semantics of predicate *receive*. Analogously for condition (4). Condition (5) places a token, or evidence, in $hist(s)|a$, for every statement s claims a knows.

We denote the set $w \cap \Gamma$ by $[w]_\Gamma$, or simply $[w]$, when Γ is clear from the context. Write $hist_e([w])$ for $hist(e([w]))$. The canonical message passing model for finite Γ and BAN theory L is $\mathcal{M}_{L,\Gamma} = \langle H_{L,\Gamma}, \kappa_{L,\Gamma} \rangle$, where

(i) $H_{L,\Gamma} = \{hist_e([w]) \mid w \in W_L,\ \exists e\}$.

(ii) $\kappa_{L,\Gamma}(a, hist_e([w])) = Keys(a, [w])$

To ensure that condition (2) is well-defined we need some conditions on Γ. We say Γ is *adequate* if Γ is finite, Γ is closed under sub-statements (if $F \in \Gamma$ and F' is a sub-statement of F then $F' \in \Gamma$), Γ is closed under renamings (if $F \in \Gamma$ and r is any renaming then $r(F) \in \Gamma$), Γ contains all atomic statements and contains $\Box_a a$ *received* M, $\Box_a a$ *sent* M and $\Box_a a$ *rec* M, for all $a \in A$ and messages M.

Lemma 8.3 *Assume Γ is adequate and $w \in W_L$.*

(i) $old\, M \in [w] \Leftrightarrow \exists M' \geq M : old\, M' \in [w]$.

(ii) $a\ rec\, M \in [w] \Leftrightarrow \exists M' \geq M : a\ received\, M' \in [w]$.

(iii) $a\ sen\, M \in [w] \Leftrightarrow \exists M' \geq M : a\ sent\, M' \in [w]$.

(iv) $a\ received\, M \in [w] \Leftrightarrow \Box_a a\ received\, M \in [w]$.

(v) $a\ sent\, M \in [w] \Leftrightarrow \Box_a a\ sent\, M \in [w]$.

Proof. From axioms *R*, *S*, *R2*, *S2*, *Mono*, *I* and *T*. We show case (2), the remaining cases are analogous. $a\ rec\, M \in [w]$, if and only if (Γ is adequate), $a\ rec\, M \in w$, if and only if (*R*, *R2*, *Mono*, w is maximal consistent set), $\exists M' \geq M : a\ received\, M' \in w$, if and only if ($\Gamma$ is adequate), $\exists M' \geq M : a\ received\, M' \in [w]$. □

Lemma 8.4 (Injectivity) *Assume Γ is adequate. $hist_e([w]) = hist_{e'}([w']) \Rightarrow [w] = [w']$, for $w, w' \in W_L$.*

Proof. From Lemma 8.3. □

Lemma 8.4 assures us that the key assignment in $\mathcal{M}_{L,\Gamma}$ is well-defined for adequate Γ. We proceed to show that the transformation $w \curvearrowright hist_e([w])$ preserves truth values from $\mathcal{C}_L$ to $\mathcal{M}_{L,\Gamma}$ for statements in Γ.

Lemma 8.5 (Reflection) *Assume Γ is adequate and $w, w' \in W_L$. The following statements are equivalent:*

(i) $\exists e' : hist_e([w]) \longrightarrow_a^r hist_{e'}([w'])$ *in* $\mathcal{M}_{L,\Gamma}$

(ii) $r \triangleleft Keys(a,[w]) \wedge \forall F : \Box_a F \in [w] \Leftrightarrow \Box_a r(F) \in [w']$.

Proof. From Lemma 8.3. We show the implication from (2) to (1). So assume that $r \triangleleft Keys(a,[w]) \wedge \forall F : \Box_a F \in [w] \Leftrightarrow \Box_a r(F) \in [w']$. We show that a receives $M \in Actions(hist_e([w])|a)$ iff a receives $r(M) \in Actions(hist_e([w'])|a)$, and similarly for internal and send actions. The proofs in the latter cases are similar and left to the reader. For receive actions:

a receives $M \in Actions(hist_e([w])|a)$
$\Leftrightarrow a$ receives $M \in Actions(hist_e([w]))$
$\Leftrightarrow a$ *received* $M \in [w]$
$\Leftrightarrow \Box_a a$ *received* $M \in [w]$ (By lemma 8.3)
$\Leftrightarrow \Box_a a$ *received* $r(M) \in [w']$ (By the assumption)
$\Leftrightarrow a$ *received* $r(M) \in [w']$ (By lemma 8.3)
$\Leftrightarrow a$ receives $r(M) \in Actions(hist_e([w']))$
$\Leftrightarrow a$ receives $r(M) \in Actions(hist_e([w'])|a)$

We thus conclude that $Actions(r(hist_e([w])|a)) = Actions(hist_e([w'])|a)$. But then there is an enumeration e' such that $r(hist_e([w])|a) = hist_{e'}([w'])|a$, and it follows that $hist_e([w]) \longrightarrow_a^r hist_{e'}([w'])$ as desired. The implication from (1) to (2) is immediate from requirement (5) in the definition of *hist*. □

Lemma 8.6 (Filtration Lemma) *Assume* Γ *is closed and* $w, w' \in W_L$.

(i) $w \underset{L}{\longrightarrow_a^r} w' \Rightarrow \exists e' : hist_e([w]) \longrightarrow_a^r hist_{e'}([w'])$

(ii) $hist_e([w]) \longrightarrow_a^r hist_{e'}([w']) \Rightarrow \forall F : \Box_a F \in [w] \Rightarrow r(F) \in [w']$

(iii) $p(M) \in [w] \Leftrightarrow hist_e([w]) \models_{M_{L,\Gamma}} p(M)$, *any predicate* p.

Proof. (3): Immediate from Lemma 8.3 and, in the case of *old*, the fact that e is admissible. (1) and (2) depend on axioms T, 4 and 5 and Reflection Lemma 8.5. For (1), assume $w \underset{L}{\longrightarrow_a^r} w'$. First observe that $r \triangleleft Keys(a,[w])$. By Lemma 8.5 it suffices to show $\Box_a F \in [w]$ iff $\Box_a r(F) \in [w']$. For the only-if direction, if $\Box_a F \in [w]$ then $\Box_a F \in \Gamma \cap w$. By ax. 4, $\Box_a \Box_a F \in w$, since w is maximal consistent. Hence $\Box_a r(F) \in w'$, and so $\Box_a r(F) \in [w']$ as well, since Γ is closed under renamings. The if-direction uses ax. 5 in a similar way, and condition (2) uses T. We omit the details. □

Lemma 8.7 (Truth Lemma for $\mathcal{M}_{L,\Gamma}$) *Assume* Γ *is adequate and* $w \in W_L$. *For all* $F \in \Gamma$*:* $hist_e([w]) \models_{\mathcal{M}_{L,\Gamma}} F \Leftrightarrow F \in [w]$.

Proof. By induction in (the number of statement operators in) F, using Truth Lemma 8.2 and Filtration Lemma 8.6. Base case, atomic statements: From Filtration Lemma 8.6.3. Induction step, negation and conjunction: Since Γ is closed under sub-statements. Induction step, epistemic modality: From Truth Lemma 8.2 and Filtration Lemma 8.6, since Γ is closed under sub-statements

and renamings. □

We continue to show that the transformation $w \curvearrowright hist_e([w])$ preserves truth values from $\mathcal{C}_L$ to $H_{L,\Gamma}$ for statement in Γ.

Lemma 8.8 (Induction) *Assume Γ is adequate. $\mathcal{M}_{L,\Gamma}$ is inductive.*

Proof. By Truth Lemma for $\mathcal{M}_{L,\Gamma}$, as Γ contains *sees*, $K \in \kappa_{L,\Gamma}(a, hist_e([w]))$ iff $hist_e([w]) \models_{\mathcal{M}_{L,\Gamma}} a\ sees\ K$ for all K, w, a. Assume that κ is strictly smaller than $\kappa_{L,\Gamma}$. Then we find some K, w, a such that $K \notin \kappa(a, hist_e([w]))$ and $K \in \kappa_{L,\Gamma}(a, hist_e([w]))$. By the definition of $\kappa_{L,\Gamma}$, $\Box_a a\ rec\ K \in [w]$. It follows that $(a\ \texttt{int}\ a\ rec\ K) \in Actions(hist_e([w])|a)$. We want to show that $hist_e([w]) \models_{\langle H_{L,\Gamma},\kappa\rangle} \Box_a a\ rec\ K$, so that the inductive property fails for κ. To this end assume that $hist_e([w]) \longrightarrow_a^r hist_{e'}([w'])$. Then $r(hist_e([w])|a) = hist_{e'}([w'])|a$, and so $(a\ \texttt{int}\ a\ rec\ r(K)) \in Actions(hist_{e'}([w'])|a)$. It follows that $\Box_a a\ rec\ r(K) \in [w']$, so also $a\ rec\ r(K) \in [w']$, by T, since Γ is closed under sub-statements and w' is maximal. Then $hist_{e'}([w']) \models_{\mathcal{M}_{L,\Gamma}} a\ rec\, r(K)$, by the Truth Lemma 8.7. Since truth of an atomic statement in a message passing model is independent of the key assignment, it follows that $hist_{e'}([w']) \models_{\langle H_{L,\Gamma},\kappa\rangle} a\ rec\, r(K)$ as well. This is sufficient to establish the result, as w' and r were chosen arbitrary. □

Lemma 8.9 (Truth Lemma for $H_{L,\Gamma}$) *Assume Γ is adequate and $w \in W_L$. For all $F \in \Gamma$: $hist_e([w]) \models_{H_{L,\Gamma}} F \Leftrightarrow F \in [w]$.*

Proof. Immediate from Truth Lemma 8.7 for $\mathcal{M}_{L,\Gamma}$ and Induction Lemma 8.8. □

Corollary 8.10 *Assume Γ is adequate. For all $F \in \Gamma$: $\models_{H_{L,\Gamma}} F \Leftrightarrow F \in L$.*

Proof. Assume $F \in \Gamma$. Then $F \in L$, if and only if, $\forall w \in W_L : F \in w$, if and only if (since $F \in \Gamma$), $\forall w \in W_L : F \in [w]$, if and only if (by Truth Lemma 8.9 for $H_{L,\Gamma}$), $\models_{H_{L,\Gamma}} F$. □

Theorem 8.11 (Finite Model Property) *If $\nvdash_{L\boldsymbol{A}} F$, then there is a finite message passing system $H \in \|A\|$ such that $\not\models_H F$.*

Proof. Assume $\nvdash_{L\boldsymbol{A}} F$. Let Γ be the smallest set closed under renamings and sub-statements and containing F and $\boldsymbol{A}$, containing all atomic statements, containing $a\ sees\ M$, $\Box_a a\ received\ M$ and $\Box_a a\ sent\ M$, for all $a \in A$ and messages M. Then Γ is finite, i.e., Γ is adequate. From Corollary 8.10, $\not\models_{H_{L\boldsymbol{A},\Gamma}} F$ and $\models_{H_{L\boldsymbol{A},\Gamma}} \boldsymbol{A}$. By construction, $H_{L\boldsymbol{A},\Gamma}$ is finite, since Γ is finite. □

From Finite Model Property 8.11, we immediately get Completeness Theorem 7.2. 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 7.3.

9 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. In fact, there have been no completeness results so far for BAN and related logics.

Adopting a recently proposed generalization of Kripke semantics that avoids logical omniscience, we have shown that a logic close 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 to logics induced by an arbitrary protocol specific base. The protocol base may express how participants in a given protocol are expected to behave, or state general assumptions about the network, such as honesty and origination assumptions.

The results assume a finite message space, thus excluding some systems, such as systems in which execution proceeds without an end, with agents constantly generating fresh messages. Also, the language in this paper covers only the symmetric key fragment of BAN.

In the future, we intend to look for effective decision procedures and to extend the completeness result in various directions: To an infinite message space, to asymmetric cryptography, to a description logic extension and to a reformulation of renaming necessitation using message variables, analogously to crypto normality in [5], rather than the quantification over renamings.

References

[1] Abadi, M. and M. Tuttle, *A semantics for a logic of authentication*, in: *Proceedings of the Tenth Annual ACM Symposium on Principles of Distributed Computing* (1991), pp. 201–216.

[2] Agray, N., W. van der Hoek and E. P. de Vink, *On ban logics for industrial security protocols.*, in: *CEEMAS*, 2001, pp. 29–36.

[3] Bieber, P., *A logic of communication in hostile environments.*, in: *Proceedings of the Computer Security Foundation Workshop III* (1990), pp. 14–22.

[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. and M. Dam, *Logical omniscience in the semantics of BAN logic*, in: *Proceedings of the Foundations of Computer Security Workshop*, 2005, pp. 121–132.

[6] Dekker, A. H., *C3po: A tool for automatic sound cryptographic protocol analysis.*, in: *PCSFW: Proceedings of The 13th Computer Security Foundations Workshop* (2000), pp. 77–87.

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

[8] 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.

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

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

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

[12] 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.

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

[14] 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.

[15] Wedel, G. and V. Kessler, *Formal semantics for authentication logics*, in: E. Bertino, H. Kurth and G. Martella, editors, *ESORICS'96*, LNCS 1146 (1996), pp. 219–241.