A semantics for BAN logic

Annette Bleeker[*]
CWI, Amsterdam
annette@cwi.nl

Lambert Meertens
CWI, Amsterdam, and
Department of Computing Science, Utrecht University, The Netherlands
lambert@cwi.nl

0 Introduction

In their ground-breaking paper [BAN89] Burrows, Abadi and Needham give a formalism, BAN logic, that can be used to reason about security properties of protocols. There are, however, several implicit or informally described assumptions. Moreover, the semantics gets very little attention, and is mentioned only in a short, informal description. As pointed out by Syverson [Syv91], having only an intuitive understanding of the semantics directly opposes the usual goal of having semantics at all: to see the logic as part of a system, and to be able to prove statements about a (more or less) existing model formally. Our aim was, therefore, to construct a sound semantics for BAN, as well as a notion of correctness that makes the additional requirements for both specification and protocol explicit.

Various authors have tried to give a semantics to BAN logic; some of them left the logic more or less intact, while others developed semantics for a new logic based on BAN logic. All these approaches are, just like BAN logic itself, restricted in their description of reality — the world can only be described through the (belief) eyes of the participants. However, to be able to judge cryptographic protocols, one cannot avoid looking beyond the individual beliefs of participants. Since all individual beliefs may be wrong, the outside world must be looked at separately. Therefore, we have not only looked for a precise semantics for BAN logic (and a proof of its soundness), but we have also chosen the semantics in such a way that it enables us to reason about knowledge (and, as a result, about the rightness of the participants' beliefs).

For our investigation we use an extension of BAN logic. Its language has, apart from the constructs taken from BAN, a few additional constructs, such as $P\,\mathsf{possesses}\,K$, used to express possession of a key — and the resulting ability to decrypt messages with that key — without necessarily believing that it belongs to a certain pair of principals; and $P\,\mathsf{rightly\_believes}\,\varphi$, which expresses that not only $P\,\mathsf{believes}\,\varphi$, but also φ itself holds.

We present the axioms of the logic in a general form: one can derive statements about the beliefs of principals, but also about the rightness of those beliefs (or of statements in general, independent of any beliefs). Defining a *rectify operation* that maps formulas of the form $P\,\mathsf{believes}\,\varphi$ to $P\,\mathsf{rightly\_believes}\,\varphi$, leaving other formulas intact, leads to a theorem that expresses that principals draw the right conclusions from their beliefs. In other words: if their initial beliefs are right, their conclusions will be right as well.

However, logical soundness does not yet establish that principals draw correct conclusions during a protocol run. We define, using operational semantics, what it means for a protocol to

[*] This research was supported by the Netherlands Organization for Scientific Research (NWO).

meet its specification. In order to prove that property of a protocol, we need certain restrictions on the protocol, depending on the assumptions. Besides, as it turns out, the assumptions need to be of a certain form as well, in order to secure monotonicity. Those requirements can be checked statically and do not exclude well-known examples of protocols.

1 The logic

In this section we introduce our logic with its language and axioms, while indicating the difference with the original BAN logic. After that, we prove that this logic is stronger than BAN.

1.1 The language

The sorts we distinguish are Principal, Key, Message and Formula. There are (further unspecified) universes of constants for the sorts Principal and Key. We view (logical) formulas as being a subsort of the sort of messages, since messages can also consist of nonces, timestamps or other constants, drawn from some further unspecified universe, as well as encrypted messages. So there is an implicit injection $\mathsf{M} :: \mathsf{Formula} \longrightarrow \mathsf{Message}$.

We use variables $A, B, P, Q, R, \ldots$ for principals, Greek letters $\varphi, \psi, \ldots$ for formulas, $M, X, Y, \ldots$ for messages in general, and $K, \ldots$ for keys.

For formulas, the language of the logic has the logical constant True, the logical operators $\wedge, \vee, \rightarrow$ and $\forall$, and the operator $=$ on the sort Message. Furthermore we have the following operators:

- $(\_, \_) :: \mathsf{Message} \times \mathsf{Message} \longrightarrow \mathsf{Message}$
(an associative, commutative and idempotent operator for message joining which is an extension of $\wedge$, the logical-and operator, so that the joining of two messages that happen to be formulas is interpreted as their conjunction[1])
- $\mathsf{believes} :: \mathsf{Principal} \times \mathsf{Formula} \longrightarrow \mathsf{Formula}$
- $\mathsf{once\_said} :: \mathsf{Principal} \times \mathsf{Message} \longrightarrow \mathsf{Formula}$
(for messages that have been uttered)
- $\mathsf{sees} :: \mathsf{Principal} \times \mathsf{Message} \longrightarrow \mathsf{Formula}$
(for messages that have been received)
- $\mathsf{possesses} :: \mathsf{Principal} \times \mathsf{Key} \longrightarrow \mathsf{Formula}$
(possession of information, in our case a key, does not imply any beliefs about validity or usage)
- $\_\ \mathsf{key\_of}\ (\_, \_) :: \mathsf{Key} \times \mathsf{Principal} \times \mathsf{Principal} \longrightarrow \mathsf{Formula}$
(symmetric in the last two arguments; intuitively, $K\ \mathsf{key\_of}\ (P, Q)$ means that K is a good key between P and Q)
- $\_\,(\_|\_) :: \mathsf{Key} \times \mathsf{Message} \times \mathsf{Principal} \longrightarrow \mathsf{Message}$
(for encryption; intuitively, $K(X|P)$ denotes X encrypted with K by P)

The "word" operators bind more tightly than the traditional logical operators, so that, e.g., $P\ \mathsf{believes}\ \varphi \ \wedge\ \psi$ must be interpreted as $(P\ \mathsf{believes}\ \varphi)\ \wedge\ \psi$.

Definition 1 *We define the operators* rightly_believes, controls *and* fresh *as follows:*

$$\mathsf{rightly\_believes} :: \mathsf{Principal} \times \mathsf{Formula} \longrightarrow \mathsf{Formula}$$

$$P\ \mathsf{rightly\_believes}\ \varphi := P\ \mathsf{believes}\ \varphi\ \wedge\ \varphi$$

[1] Using the injection M mentioned above, we could write: $(\mathsf{M}\varphi, \mathsf{M}\psi) = \mathsf{M}(\varphi \wedge \psi)$.

$$\mathsf{controls} :: \mathsf{Principal} \times \mathsf{Formula} \longrightarrow \mathsf{Formula}$$

$$P\,\mathsf{controls}\,\varphi := P\,\mathsf{believes}\,\varphi \;\rightarrow\; P\,\mathsf{rightly\_believes}\,\varphi$$

$$\mathsf{fresh} :: \mathsf{Message} \longrightarrow \mathsf{Formula}$$

$$\mathsf{fresh}\,X := (\forall P, \varphi :: P\,\mathsf{once\_said}\,(X, \varphi) \;\rightarrow\; P\,\mathsf{believes}\,\varphi)$$

(intuitively: $\mathsf{fresh}\,X$ *if* X *has not been uttered before the current protocol run)*

In BAN logic controls and fresh are primitive operators. We could, equivalently, have introduced these operators as primitives with their definitions turned into axioms.

1.2 Axiomatisation

For the axiomatisation we need to define the *contents* of a message as the collection of submessages when encryption is transparent:

Definition 2 *The function* $cts[\![\_]\!]$ *takes a message and delivers a set of messages:*

$$\begin{array}{ll} cts[\![(X,Y)]\!] & := \{(X,Y)\} \cup cts[\![X]\!] \cup cts[\![Y]\!] \\ cts[\![K(X|P)]\!] & := \{K(X|P)\} \cup cts[\![X]\!] \\ cts[\![X]\!] & := \{X\} \text{ (otherwise)} \end{array}$$

The axiomatisation includes the standard axioms for *equational logic* with Modus Ponens — which subsumes propositional logic — and the standard rules for universal quantification, where a formula $\varphi \leftrightarrow \psi$ is treated as shorthand for $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$.

Beneath, we introduce a collection of axioms for the specific operators of our logic, and mention the related axiom in the original BAN logic — if such an axiom exists. (Because of the presence of the Modus Ponens rule, we can replace inference rules $\frac{\varphi}{\psi}$ by axioms $\vdash \varphi \rightarrow \psi$.)

For message joining there are all axioms of the forms $\vdash (X,(Y,Z)) = ((X,Y),Z)$, $\vdash (X,Y) = (Y,X)$ and $\vdash (X,X) = X$, and for the key_of operator $\vdash K\,\mathsf{key\_of}\,(P,Q) = K\,\mathsf{key\_of}\,(Q,P)$. Equational logic allows us to apply theorems of the form $\vdash \varphi[x] \wedge x = y \;\rightarrow\; \varphi[y]$.

Furthermore, we have:

Rationality The rationality rule introduces a collection of axioms, one for every theorem of the logic:

$$\frac{\vdash \varphi}{\vdash P\,\mathsf{believes}\,\varphi}$$

This axiom, together with the next one, lifts the level of reasoning from beliefs of principals to general statements.

Believing Modus Ponens Modus Ponens under the believes operator:

$$\vdash P\,\mathsf{believes}\,(\varphi \rightarrow \psi) \;\rightarrow\; (P\,\mathsf{believes}\,\varphi \;\rightarrow\; P\,\mathsf{believes}\,\psi)$$

Saying parts of a joint message Uttering a joint message implies uttering each of the parts:

$$\vdash P\,\mathsf{once\_said}\,(X,Y) \;\rightarrow\; P\,\mathsf{once\_said}\,X$$

The related BAN logic axiom is:

$$\vdash_{BAN} P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,(X,Y) \;\rightarrow\; P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,X$$

Saying contents of an encrypted message Uttering an encrypted message, signed by yourself, while you believe that the key is good, implies uttering of the encrypted message:

$$\vdash P\,\mathsf{once\_said}\,K(X|P)\ \wedge\ P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,Q)\ \rightarrow\ P\,\mathsf{once\_said}\,X$$

There is no similar axiom in BAN logic.

Seeing parts of a joint message Seeing a joint message means seeing each part separately as well:

$$\vdash P\,\mathsf{sees}\,(X,Y)\ \rightarrow\ P\,\mathsf{sees}\,X$$

The BAN logic has this axiom (exactly so) as well.

Awareness Awareness of what one sees:

$$\vdash P\,\mathsf{sees}\,X\ \rightarrow\ P\,\mathsf{believes}\,P\,\mathsf{sees}\,X$$

There is no similar axiom in BAN logic.

Possessing keys of a seen key statement If one sees a key statement, one possesses the key that it mentioned:

$$\vdash P\,\mathsf{sees}\,K\,\mathsf{key\_of}\,(Q,R)\ \rightarrow\ P\,\mathsf{possesses}\,K$$

In BAN logic, the notion of possession does not exist.

Possessing believed keys One can only believe that a certain key is good if possessing the key:

$$\vdash P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(Q,R)\ \rightarrow\ P\,\mathsf{possesses}\,K$$

Decryption Seeing an encrypted message while having the key in possession, means seeing the message itself:

$$\vdash P\,\mathsf{possesses}\,K \wedge P\,\mathsf{sees}\,K(X|Q)\ \rightarrow\ P\,\mathsf{sees}\,X$$

The related BAN logic axiom is **decryption**:

$$\vdash_{BAN} P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,Q)\ \wedge\ P\,\mathsf{sees}\,K(X|Q)\ \rightarrow\ P\,\mathsf{sees}\,X$$

In BAN logic one can only decrypt with keys that are believed to be one's own key. With any other key in possession, decryption cannot be derived, since BAN logic does not have a notion of possession.

Good key ensures the utterer A collection of axioms, stating that if a key is good, the only ones that use it for encryption are the owners, so if somewhere, someone sees a message that contains a part encrypted with that key, that part must have been said by the key owner who encrypted it:
For all P, Q, R, X, Y, K such that $K(X|Q) \in cts[\![Y]\!]$:

$$\vdash K\,\mathsf{key\_of}\,(P,Q) \wedge R\,\mathsf{sees}\,Y\ \rightarrow\ Q\,\mathsf{once\_said}\,X$$

The related BAN logic axiom is the **message meaning rule**:

$$\vdash_{BAN} P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,Q)\ \wedge\ P\,\mathsf{sees}\,K(X|Q)\ \rightarrow\ P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,X$$

The BAN axioms that were not mentioned above are:

$$\vdash_{BAN} P\,\mathsf{believes}\,\varphi \;\wedge\; P\,\mathsf{believes}\,\psi \;\rightarrow\; P\,\mathsf{believes}\,(\varphi,\psi)$$

$$\vdash_{BAN} P\,\mathsf{believes}\,(\varphi,\psi) \;\rightarrow\; P\,\mathsf{believes}\,\varphi$$

$$\vdash_{BAN} P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(Q,R) \;\rightarrow\; P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(R,Q)$$

$$\vdash_{BAN} P\,\mathsf{believes}\,\mathsf{fresh}\,\varphi \;\wedge\; P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,\varphi \;\rightarrow\; P\,\mathsf{believes}\,Q\,\mathsf{believes}\,\varphi$$

$$\vdash_{BAN} P\,\mathsf{believes}\,\mathsf{fresh}\,X \;\rightarrow\; P\,\mathsf{believes}\,\mathsf{fresh}\,(X,Y)$$

$$\vdash_{BAN} P\,\mathsf{believes}\,Q\,\mathsf{controls}\,\varphi \;\wedge\; P\,\mathsf{believes}\,Q\,\mathsf{believes}\,\varphi \;\rightarrow\; P\,\mathsf{believes}\,\varphi$$

1.3 Comparison with BAN logic

In order to understand the relation between our logic and BAN logic, we show that every theorem of BAN logic is a theorem of our logic — in other words, that our logic is stronger. Because our logic stripped off the believes operator from most of the axioms, the following lemma will be useful in the proof.

Lemma 3 *If* $\vdash \varphi \rightarrow \psi$*, then* $\vdash P\,\mathsf{believes}\,\varphi \;\rightarrow\; P\,\mathsf{believes}\,\psi$*.*

Proof

$$\begin{array}{ll} & \vdash \varphi \rightarrow \psi \\ \Rightarrow & \qquad \{\text{Rationality}\} \\ & \vdash P\,\mathsf{believes}\,(\varphi \rightarrow \psi) \\ \Rightarrow & \qquad \{\text{Believing Modus Ponens, Modus Ponens}\} \\ & \vdash P\,\mathsf{believes}\,\varphi \;\rightarrow\; P\,\mathsf{believes}\,\psi \end{array}$$

□

From Believing Modus Ponens and the Rationality Rule we now obtain:

Lemma 4 $\vdash P\,\mathsf{believes}\,(\varphi \;\wedge\; \psi) \;\leftrightarrow\; P\,\mathsf{believes}\,\varphi \;\wedge\; P\,\mathsf{believes}\,\psi$

If part of a message is fresh, the whole of the message must be fresh as well:

Lemma 5 $\vdash \mathsf{fresh}\,X \;\rightarrow\; \mathsf{fresh}\,(X,Y)$

Note that the reverse does not hold, since a message can contain "old news" next to new data; the combination is fresh, but every element is not.

Theorem 6 *The logic as defined in this article, is stronger than BAN logic.*

Proof It suffices to prove that all axioms of the BAN logic are theorems of our logic.

$$\vdash_{BAN} P\,\mathsf{sees}\,(X,Y) \;\rightarrow\; P\,\mathsf{sees}\,X$$

is our axiom **Seeing parts of a joint message**, and therefore a theorem.

$$\vdash_{BAN} P\,\mathsf{believes}\,\varphi \;\wedge\; P\,\mathsf{believes}\,\psi \;\rightarrow\; P\,\mathsf{believes}\,(\varphi,\psi)$$

$$\vdash_{BAN} P\,\mathsf{believes}\,(\varphi,\psi) \;\rightarrow\; P\,\mathsf{believes}\,\varphi$$

both follow from Lemma 4 using the identification of the joining operator on formulas with the logical-and operator.

$$\vdash_{BAN} P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(Q,R) \;\rightarrow\; P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(R,Q)$$

follows from the symmetry of the $\mathsf{key\_of}$ operator.

$$\vdash_{BAN} P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,(X,Y) \;\rightarrow\; P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,X$$

follows from our axiom **Saying parts of a joint message** and Lemma 3.

$$\vdash_{BAN} P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,Q) \;\wedge\; P\,\mathsf{sees}\,K(X|Q) \;\rightarrow\; P\,\mathsf{sees}\,X$$

follows from our axioms **Possessing believed keys** and **Decryption**.

$$\vdash_{BAN} P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,Q) \;\wedge\; P\,\mathsf{sees}\,K(X|Q) \;\rightarrow\; P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,X$$

follows from our axiom **Awareness** and Lemmas 3 and 4.

$$\vdash_{BAN} P\,\mathsf{believes}\,\mathsf{fresh}\,\varphi \;\wedge\; P\,\mathsf{believes}\,Q\,\mathsf{once\_said}\,\varphi \;\rightarrow\; P\,\mathsf{believes}\,Q\,\mathsf{believes}\,\varphi$$

follows from the definition of fresh , the idempotence of $(\_,\_)$, and Lemmas 3 and 4.

$$\vdash_{BAN} P\,\mathsf{believes}\,\mathsf{fresh}\,X \;\rightarrow\; P\,\mathsf{believes}\,\mathsf{fresh}\,(X,Y)$$

follows from Lemmas 3 and 5.

$$\vdash_{BAN} P\,\mathsf{believes}\,Q\,\mathsf{controls}\,\varphi \;\wedge\; P\,\mathsf{believes}\,Q\,\mathsf{believes}\,\varphi \;\rightarrow\; P\,\mathsf{believes}\,\varphi$$

follows from the definitions of $\mathsf{controls}$ and $\mathsf{rightly\_believes}$ and Lemmas 3 and 4.
□

2 Rectification of formulas

The rectify operation $\mathcal{R}[\![\_]\!]$ maps formulas to formulas. In particular, it maps formulas of the form $P\,\mathsf{believes}\,\varphi$ to $P\,\mathsf{rightly\_believes}\,\varphi$. It is defined as follows:

Definition 7

$$\begin{array}{lcl}
\mathcal{R}[\![P\,\mathsf{believes}\,\varphi]\!] & := & P\,\mathsf{rightly\_believes}\,\varphi \\
\mathcal{R}[\![\varphi \wedge \psi]\!] & := & \mathcal{R}[\![\varphi]\!] \wedge \mathcal{R}[\![\psi]\!] \\
\mathcal{R}[\![\varphi \vee \psi]\!] & := & \mathcal{R}[\![\varphi]\!] \vee \mathcal{R}[\![\psi]\!] \\
\mathcal{R}[\![\varphi \rightarrow \psi]\!] & := & \mathcal{R}[\![\varphi]\!] \;\rightarrow\; \mathcal{R}[\![\psi]\!] \\
\mathcal{R}[\![\forall x :: \varphi]\!] & := & (\forall x :: \mathcal{R}[\![\varphi]\!]) \\
\mathcal{R}[\![\varphi]\!] & := & \varphi,\ \text{other cases}
\end{array}$$

Note the limited recursion, which stops whenever a formula with a "word" operator is encountered. The operation is extended to a set-to-set mapping in the usual way.

Directly from the definition on sets it follows that:

Lemma 8 *If $\mathcal{A}_1 \subseteq \mathcal{A}_2$, then $\mathcal{R}[\![\mathcal{A}_1]\!] \subseteq \mathcal{R}[\![\mathcal{A}_2]\!]$*

Theorem 9 *If $\mathcal{A} \vdash \mathcal{C}$ then $\mathcal{R}[\![\mathcal{A}]\!] \vdash \mathcal{R}[\![\mathcal{C}]\!]$.*

Proof
We prove it with structural induction on the derivation.

Case trivial proof: A trivial proof is a derivation step of the form $\mathcal{A} \vdash \mathcal{C}$, where $\mathcal{C} \subseteq \mathcal{A}$.

$$\begin{array}{ll}
 & \mathcal{R}\llbracket\mathcal{A}\rrbracket \text{ and } \mathcal{C} \subseteq \mathcal{A} \\
\Rightarrow & \qquad \{\text{Lemma 8}\} \\
 & \mathcal{R}\llbracket\mathcal{A}\rrbracket \text{ and } \mathcal{R}\llbracket\mathcal{C}\rrbracket \subseteq \mathcal{R}\llbracket\mathcal{A}\rrbracket \\
\Rightarrow & \qquad \{\text{trivial proof}\} \\
 & \mathcal{R}\llbracket\mathcal{C}\rrbracket
\end{array}$$

Case deduction: Deduction is the introduction of implication by derivation:

If $\varphi \vdash \psi$, then $\vdash \varphi \;\rightarrow\; \psi$.

Using deduction, we may instantiate:

If $\mathcal{R}\llbracket\varphi\rrbracket \vdash \mathcal{R}\llbracket\psi\rrbracket$, then $\vdash \mathcal{R}\llbracket\varphi\rrbracket \;\rightarrow\; \mathcal{R}\llbracket\psi\rrbracket$.

From here we can derive, under the assumption $\mathcal{R}\llbracket\varphi\rrbracket \vdash \mathcal{R}\llbracket\psi\rrbracket$:

$$\begin{array}{ll}
 & \mathsf{True} \\
\Rightarrow & \qquad \{\text{deduction, } \mathcal{R}\llbracket\varphi\rrbracket \vdash \mathcal{R}\llbracket\psi\rrbracket\} \\
 & \mathcal{R}\llbracket\varphi\rrbracket \;\rightarrow\; \mathcal{R}\llbracket\psi\rrbracket \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \mathcal{R}\llbracket\varphi \;\rightarrow\; \psi\rrbracket
\end{array}$$

Cases axioms of predicate logic: As an example, we prove our claim for the introduction of $\wedge$. Other introductions and eliminations ($\vee$, $\rightarrow$, $\neg$, $\forall$) have analogous proofs.

$$\begin{array}{ll}
 & \mathcal{R}\llbracket\varphi\rrbracket \text{ and } \mathcal{R}\llbracket\psi\rrbracket \\
\Rightarrow & \qquad \{\text{introduction } \wedge\} \\
 & \mathcal{R}\llbracket\varphi\rrbracket \wedge \mathcal{R}\llbracket\psi\rrbracket \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \mathcal{R}\llbracket\varphi \wedge \psi\rrbracket
\end{array}$$

Case Rationality: Let $\vdash \varphi$. We prove $\vdash \mathcal{R}\llbracket P \;\mathsf{believes}\; \varphi\rrbracket$.

$$\begin{array}{ll}
 & \mathsf{True} \\
\Rightarrow & \qquad \{\text{Rationality, } \vdash \varphi\} \\
 & P \;\mathsf{believes}\; \varphi \wedge \varphi \\
\equiv & \qquad \{\text{definition } \mathsf{rightly\_believes}\} \\
 & P \;\mathsf{rightly\_believes}\; \varphi \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \mathcal{R}\llbracket P \;\mathsf{believes}\; \varphi\rrbracket
\end{array}$$

Case axiom: For every axiom $\vdash \varphi \;\rightarrow\; \psi$, we will prove $\vdash \mathcal{R}\llbracket\varphi \;\rightarrow\; \psi\rrbracket$, by deriving $\mathcal{R}\llbracket\varphi\rrbracket \vdash \mathcal{R}\llbracket\psi\rrbracket$.

case Believing Modus Ponens: We prove it for the equivalent form $\vdash (P\,\mathsf{believes}\,(\varphi \;\rightarrow\; \psi) \wedge P\,\mathsf{believes}\,\varphi) \;\rightarrow\; P\,\mathsf{believes}\,\psi$

$$
\begin{array}{ll}
 & \mathcal{R}[\![P\,\mathsf{believes}\,(\varphi \;\rightarrow\; \psi) \wedge P\,\mathsf{believes}\,\varphi]\!] \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & P\,\mathsf{rightly\_believes}\,(\varphi \;\rightarrow\; \psi) \wedge P\,\mathsf{rightly\_believes}\,\varphi \\
\equiv & \qquad \{\text{definition } \mathsf{rightly\_believes}\,\} \\
 & P\,\mathsf{believes}\,(\varphi \;\rightarrow\; \psi) \wedge (\varphi \;\rightarrow\; \psi) \wedge (P\,\mathsf{believes}\,\varphi) \wedge \varphi \\
\Rightarrow & \qquad \{\text{Believing Modus Ponens, Modus Ponens}\} \\
 & P\,\mathsf{believes}\,\psi \wedge \psi \\
\equiv & \qquad \{\text{definition } \mathsf{rightly\_believes}\,\} \\
 & P\,\mathsf{rightly\_believes}\,\psi \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \mathcal{R}[\![P\,\mathsf{believes}\,\psi]\!]
\end{array}
$$

case Saying contents of an encrypted message:

$$
\begin{array}{ll}
 & \mathcal{R}[\![P\,\mathsf{once\_said}\,K(X|P) \wedge P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,Q)]\!] \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & P\,\mathsf{once\_said}\,K(X|P) \wedge P\,\mathsf{rightly\_believes}\,K\,\mathsf{key\_of}\,(P,Q) \\
\Rightarrow & \qquad \{\text{definition } \mathsf{rightly\_believes}\,\} \\
 & P\,\mathsf{once\_said}\,K(X|P) \wedge P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,Q) \\
\Rightarrow & \qquad \{\text{Saying contents of an encrypted message}\} \\
 & P\,\mathsf{once\_said}\,X \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \mathcal{R}[\![P\,\mathsf{once\_said}\,X]\!]
\end{array}
$$

case Awareness:

$$
\begin{array}{ll}
 & \mathcal{R}[\![P\,\mathsf{sees}\,X]\!] \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & P\,\mathsf{sees}\,X \\
\Rightarrow & \qquad \{\text{Awareness, introduction } \wedge\} \\
 & P\,\mathsf{believes}\,P\,\mathsf{sees}\,X \wedge P\,\mathsf{sees}\,X \\
\equiv & \qquad \{\text{definition } \mathsf{rightly\_believes}\,\} \\
 & P\,\mathsf{rightly\_believes}\,P\,\mathsf{sees}\,X \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \mathcal{R}[\![P\,\mathsf{believes}\,P\,\mathsf{sees}\,X]\!]
\end{array}
$$

case Possessing believed keys:

$$
\begin{array}{ll}
 & \mathcal{R}[\![P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(Q,R)]\!] \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & P\,\mathsf{rightly\_believes}\,K\,\mathsf{key\_of}\,(Q,R)
\end{array}
$$

$\Rightarrow$ $\{$definition $\mathsf{rightly\_believes}\}$

P $\mathsf{believes}$ K $\mathsf{key\_of}$ (Q, R)

$\Rightarrow$ $\{$Possessing believed keys$\}$

P $\mathsf{possesses}$ K

$\equiv$ $\{$definition rectify$\}$

$\mathcal{R}[\![P \ \mathsf{possesses}\ K]\!]$

The remaining axioms do not contain a believe operator, so they do not change under the rectify function.
□

3 The model

We view the environment as a system consisting of a finite collection of *principals*. We define for a principal P a *local state* as a tuple $(\mathcal{B}_P, \mathcal{O}_P, \mathcal{S}_P, \mathcal{K}_P)$, with the intuitive interpretation:

- $\mathcal{B}_P$, the set of formulas that P currently believes;
- $\mathcal{O}_P$, the set of (sub-)messages P once said;
- $\mathcal{S}_P$, the set of messages that P has seen so far;
- $\mathcal{K}_P$, the set of keys P possesses.

It is *closed* if it satisfies the following (mutually defined) closure properties, each of which corresponds directly to an axiom:

(i). (Rationality) Principals believe every theorem of the logic:

$$(\vdash \varphi) \Rightarrow \varphi \in \mathcal{B}_P$$

(ii). (Believing Modus Ponens) Principals apply Modus Ponens in their beliefs:

$$(\varphi \to \psi) \in \mathcal{B}_P \wedge \varphi \in \mathcal{B}_P \Rightarrow \psi \in \mathcal{B}_P$$

(iii). (Saying parts of a joint message) If a principal said a combination of messages at a certain time, then that principal said each of the messages as well:

$$(X, Y) \in \mathcal{O}_P \Rightarrow X \in \mathcal{O}_P \wedge Y \in \mathcal{O}_P$$

The reverse does not hold, since the presence of a joint message in $\mathcal{O}_P$ implies that both components were uttered (as a joint message) at the same time;

(iv). (Saying contents of an encrypted message) If a principal said an encrypted message and believes the key is good, then that principal said the contents of the encrypted message as well:

$$K(X|P) \in \mathcal{O}_P \wedge K \ \mathsf{key\_of}\ (P, Q) \in \mathcal{B}_P \Rightarrow X \in \mathcal{O}_P$$

(v). (Seeing parts of a joint message) If a principal sees a joint message, that principal sees each of the messages as well:

$$(X, Y) \in \mathcal{S}_P \Rightarrow X \in \mathcal{S}_P \wedge Y \in \mathcal{S}_P$$

(Note that the reverse does not hold, since a joint message implies utterance of its components *at the same time*, i.e., within the same message.)

(vi). (Awareness) If a principal sees a message, then that principal also believes he sees it:

$$X \in \mathcal{S}_P \Rightarrow (P\,\mathsf{sees}\,X) \in \mathcal{B}_P$$

(vii). (Possessing keys of a seen key statement) If a principal sees a key statement, then that principal possesses the key mentioned:

$$K\,\mathsf{key\_of}\,(Q, R) \in \mathcal{S}_P \Rightarrow K \in \mathcal{K}_P$$

(viii). (Possessing believed keys) If a principal believes that a certain key is a good key statement, then that principal must possess that key as well:

$$K\,\mathsf{key\_of}\,(Q, R) \in \mathcal{B}_P \Rightarrow K \in \mathcal{K}_P$$

(ix). (Decryption) If a principal P possesses a key K, and if P sees a message X labeled with Q and encrypted with K, then P also sees X itself:

$$K \in \mathcal{K}_P \wedge K(X|Q) \in \mathcal{S}_P \Rightarrow X \in \mathcal{S}_P$$

(Note that there is no closure property corresponding to the axiom **Good key ensures the utterer**.)

The *closure* of a local state s is the least closed local state s' such that $s \subseteq s'$, where the ordering is obtained by component-wise lifting of the set ordering. Note that taking the closure only adds elements to the sets involved, and leaves an already closed local state unchanged.

A *global state* is a mapping from principals to local states (for each principal in the environment). Global states are ordered by lifting the ordering on local states. The closure of a global state s, denoted by $clo(s)$, is defined in the obvious way. The unqualified term "*state*" will, from now on, mean a *closed global* state.

We consistently use the convention that for a state denoted by the variable s its local state for principal P is denoted by the tuple $(\mathcal{B}_P, \mathcal{O}_P, \mathcal{S}_P, \mathcal{K}_P)$, and likewise that for a state s' its local state for principal P is denoted by the tuple $(\mathcal{B}'_P, \mathcal{O}'_P, \mathcal{S}'_P, \mathcal{K}'_P)$

Lemma 10 *The function clo is monotonic, augmenting and idempotent:*

$$x \subseteq y \;\Rightarrow\; clo(x) \subseteq clo(y)$$

$$x \subseteq clo(x)$$

$$clo(clo(x)) = clo(x)$$

4 Semantics of formulas

We define the relation $\models$ between states and formulas (where $s \models \varphi$ means: in state s formula φ holds) inductively on the structure of formulas as the least relation satisfying:

$$\begin{array}{lll}
s \models \mathsf{True}; & & \\
s \models \varphi \wedge \psi & \text{if} & s \models \varphi \text{ and } s \models \psi; \\
s \models (\varphi, \psi) & \text{if} & s \models \varphi \wedge \psi; \\
s \models \varphi \rightarrow \psi & \text{if} & s \models \varphi \text{ implies } s \models \psi; \\
s \models (\forall x :: \varphi) & \text{if} & s \models \varphi[x \leftarrow u] \text{ holds for all terms } u \text{ of the appropriate kind} \\
 & & \text{not containing unbound variables;} \\
s \models P \,\mathsf{believes}\, \varphi & \text{if} & \varphi \in \mathcal{B}_P; \\
s \models P \,\mathsf{once\_said}\, X & \text{if} & X \in \mathcal{O}_P; \\
s \models P \,\mathsf{sees}\, X & \text{if} & X \in \mathcal{S}_P; \\
s \models P \,\mathsf{possesses}\, K & \text{if} & K \in \mathcal{K}_P; \\
s \models K \,\mathsf{key\_of}\, (P, Q) & \text{if} & \text{for all } S \in \{P, Q\}, \text{ all } R, \text{ and all } X, Y \text{ such that} \\
 & & \qquad K(X|S) \in cts[\![Y]\!] : \\
 & & s \models R \,\mathsf{sees}\, Y \text{ implies } s \models S \,\mathsf{once\_said}\, X.
\end{array}$$

The notation $\varphi[x \leftarrow u]$ above means: φ with u substituted for the free occurrences of x. If $\psi = (\forall \varphi :: \varphi)$, the whole formula ψ may be substituted for φ, and since $\varphi[\varphi \leftarrow \psi] = \psi$, the "recursion" in the definition of $\models$ is unbounded, whence the appeal above to "least relation".

Note that the relation $\models$ is not monotonic in its left argument, i.e., when $s \subseteq s'$, $s \models \mathcal{A}$ does in general not imply $s' \models \mathcal{A}$.

5 Soundness

Theorem 11 (Soundness) *The logic as described in this article is sound with respect to the newly defined semantics.*

Corollary 12 *BAN logic is sound.*

Proof of Theorem 11 For each axiom $\vdash \varphi \rightarrow \psi$, as summed up in section 1.2, we prove $s \models \varphi \Rightarrow s \models \psi$.

Rationality does not have the form $\vdash \varphi \rightarrow \psi$; instead, we have to show that for each theorem φ (and any P in the environment) the formula $P \,\mathsf{believes}\, \varphi$ is a tautology.

$$\begin{array}{ll}
 & \vdash \varphi \\
\Rightarrow & \qquad \{\text{closure property (i) }\} \\
 & \text{for all states } s : \ \varphi \in \mathcal{B}_P \\
\equiv & \qquad \{\text{semantics of } \mathsf{believes}\,\} \\
 & \text{for all states } s : \ s \models P \,\mathsf{believes}\, \varphi
\end{array}$$

Believing Modus Ponens We prove the soundness of the following, equivalent variant of the axiom: $\vdash P \,\mathsf{believes}\, (\varphi \rightarrow \psi) \wedge P \,\mathsf{believes}\, \varphi \quad \rightarrow \quad P \,\mathsf{believes}\, \psi$.

$$\begin{array}{ll}
 & s \models P \,\mathsf{believes}\, (\varphi \rightarrow \psi) \ \wedge \ P \,\mathsf{believes}\, \varphi \\
\equiv & \qquad \{\text{semantics of } \mathsf{believes}\,\} \\
 & (\varphi \rightarrow \psi) \in \mathcal{B}_P \text{ and } \varphi \in \mathcal{B}_P \\
\Rightarrow & \qquad \{\text{closure property (ii)}\} \\
 & \psi \in \mathcal{B}_P
\end{array}$$

$$\begin{array}{ll}
\equiv & \quad \{\text{semantics of } \mathsf{believes}\} \\
 & s \models P \,\mathsf{believes}\, \psi
\end{array}$$

Saying parts of a joint message

$$\begin{array}{ll}
 & s \models P \,\mathsf{once\_said}\, (X, Y) \\
\equiv & \quad \{\text{semantics of } \mathsf{once\_said}\} \\
 & (X, Y) \in \mathcal{O}_P \\
\Rightarrow & \quad \{\text{closure property (iii)}\} \\
 & X \in \mathcal{O}_P \\
\equiv & \quad \{\text{semantics of } \mathsf{once\_said}\} \\
 & s \models P \,\mathsf{once\_said}\, X
\end{array}$$

Saying contents of an encrypted message

$$\begin{array}{ll}
 & s \models P \,\mathsf{once\_said}\, K(X|P) \;\wedge\; P \,\mathsf{believes}\, K \,\mathsf{key\_of}\, (P, Q) \\
\equiv & \quad \{\text{semantics of } \mathsf{once\_said} \text{ and } \mathsf{believes}\} \\
 & K(X|P) \in \mathcal{O}_P \text{ and } K \,\mathsf{key\_of}\, (P, Q) \in \mathcal{B}_P \\
\Rightarrow & \quad \{\text{closure property (iv)}\} \\
 & X \in \mathcal{O}_P \\
\equiv & \quad \{\text{semantics of } \mathsf{once\_said}\} \\
 & s \models P \,\mathsf{once\_said}\, X
\end{array}$$

Seeing parts of a joint message

$$\begin{array}{ll}
 & s \models P \,\mathsf{sees}\, (X, Y) \\
\equiv & \quad \{\text{semantics of } \mathsf{sees}\} \\
 & (X, Y) \in \mathcal{S}_P \\
\Rightarrow & \quad \{\text{closure property (v)}\} \\
 & X \in \mathcal{S}_P \\
\equiv & \quad \{\text{semantics of } \mathsf{sees}\} \\
 & s \models P \,\mathsf{sees}\, X
\end{array}$$

Awareness

$$\begin{array}{ll}
 & s \models P \,\mathsf{sees}\, X \\
\equiv & \quad \{\text{semantics of } \mathsf{sees}\} \\
 & X \in \mathcal{S}_P \\
\Rightarrow & \quad \{\text{closure property (vi)}\} \\
 & P \,\mathsf{sees}\, X \in \mathcal{B}_P \\
\equiv & \quad \{\text{semantics of } \mathsf{sees}\} \\
 & s \models P \,\mathsf{believes}\, P \,\mathsf{sees}\, X
\end{array}$$

Possessing keys of a seen key statement

$$\begin{array}{ll}
 & s \models P\,\mathsf{sees}\,K\,\mathsf{key\_of}\,(Q,R) \\
\equiv & \qquad \{\text{semantics of } \mathsf{sees}\,\} \\
 & K\,\mathsf{key\_of}\,(Q,R) \in \mathcal{S}_P \\
\Rightarrow & \qquad \{\text{closure property (vii)}\} \\
 & K \in \mathcal{K}_P \\
\equiv & \qquad \{\text{semantics of } \mathsf{possesses}\,\} \\
 & s \models P\,\mathsf{possesses}\,K
\end{array}$$

Possessing believed keys

$$\begin{array}{ll}
 & s \models P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(Q,R) \\
\equiv & \qquad \{\text{semantics of } \mathsf{believes}\,\} \\
 & K\,\mathsf{key\_of}\,(Q,R) \in \mathcal{B}_P \\
\Rightarrow & \qquad \{\text{closure property (viii)}\} \\
 & K \in \mathcal{K}_P \\
\equiv & \qquad \{\text{semantics of } \mathsf{possesses}\,\} \\
 & s \models P\,\mathsf{possesses}\,K
\end{array}$$

Decryption

$$\begin{array}{ll}
 & s \models P\,\mathsf{possesses}\,K \wedge P\,\mathsf{sees}\,K(X|Q) \\
\equiv & \qquad \{\text{semantics of } \mathsf{possesses} \text{ and } \mathsf{sees}\,\} \\
 & K \in \mathcal{K}_P \wedge K(X|Q) \in \mathcal{S}_P \\
\Rightarrow & \qquad \{\text{closure property (ix)}\} \\
 & X \in \mathcal{S}_P \\
\equiv & \qquad \{\text{semantics of } \mathsf{sees}\,\} \\
 & s \models P\,\mathsf{sees}\,X
\end{array}$$

Good key ensures the utterer We prove the soundness of this equivalent variant of the axiom: $\vdash K\,\mathsf{key\_of}\,(P,Q) \;\rightarrow\; (R\,\mathsf{sees}\,Y \;\rightarrow\; Q\,\mathsf{once\_said}\,X)$, where we may use the assumption that $K(X|Q) \in cts[\![Y]\!]$:

$$\begin{array}{ll}
 & s \models K\,\mathsf{key\_of}\,(P,Q) \\
\Rightarrow & \qquad \{\text{semantics of } \mathsf{key\_of}\} \\
 & \text{for all } S \in \{P,Q\}\text{, all } R\text{, and all } X,Y \text{ such that} K(X|S) \in cts[\![Y]\!] : \\
 & s \models R\,\mathsf{sees}\,Y \text{ implies } s \models S\,\mathsf{once\_said}\,X \\
\Rightarrow & \qquad \{\text{instantiate } S{\leftarrow}Q,\ R{\leftarrow}R,\ X{\leftarrow}X,\ Y{\leftarrow}Y\} \\
 & \ \text{if } K(X|Q) \in cts[\![Y]\!],\ s \models R\,\mathsf{sees}\,Y \text{ implies } s \models Q\,\mathsf{once\_said}\,X \\
\Rightarrow & \qquad \{\text{discharge the assumption}\} \\
 & s \models R\,\mathsf{sees}\,Y \text{ implies } s \models Q\,\mathsf{once\_said}\,X \\
\equiv & \qquad \{\text{semantics of } \rightarrow\,\} \\
 & s \models R\,\mathsf{sees}\,Y \;\rightarrow\; Q\,\mathsf{once\_said}\,X
\end{array}$$

□

6 Protocols

In the previous section we have proven our logic sound, so every theorem of the logic is a tautology in the model. This, however, does not by itself establish in any way the suitability of the logic as a tool for proving protocols correct. In fact, protocols were not referred to at all.

Definition 13 *A* protocol *is a finite sequence of* actions*, where each protocol action has the form $P \rightarrow Q : X$, signifying the sending of a message X from P to Q.*

The empty protocol is denoted by $\emptyset$, and the sequencing operator "$;$" is used to denote concatenation of protocols.

The participants *of a protocol are the principals mentioned in its actions.*

We model actions as transitions from states to states. If in state s the action $P \rightarrow Q : X$ is performed, only the local states for P and Q will be changed. The new state s' is the least (closed global) state such that $s \subseteq s'$, $X \in \mathcal{O}'_P$ and $X \in \mathcal{S}'_Q$. From the closure properties we know that the local states for other principals stay unchanged. Formally:

Definition 14 *We define the transition function tra, mapping a state and an action to a new state, by*

$$tra(s, (P \rightarrow Q : X)) \;:=\; clo(s[\mathcal{O}_P \leftarrow \mathcal{O}_P \cup \{X\},\, \mathcal{S}_Q \leftarrow \mathcal{S}_Q \cup \{X\}])$$

that is, for the action of sending a message X from P to Q, X is added to both $\mathcal{O}_P$ and $\mathcal{S}_Q$, and then the closure is taken (to make it a well-formed state).

We define the extension of tra to protocols by:

$$\begin{array}{lll} tra(s, \emptyset) & := & s \\ tra(s, \mathcal{P}_1; \mathcal{P}_2) & := & tra(tra(s, \mathcal{P}_1), \mathcal{P}_2) \end{array}$$

Using Lemma 10 it follows immediately from the definition of *tra* that the transition function is augmenting for a fixed protocol:

Lemma 15 $s \subseteq tra(s, \mathcal{P})$

A *specification* of a protocol is given by two sets of formulas, $\mathcal{A}$ (the *assumptions*) and $\mathcal{C}$ (the *conclusions*). Protocol $\mathcal{P}$ *satisfies* such a specification (notation: $\{\mathcal{A}\}\,\mathcal{P}\,\{\mathcal{C}\}$) when "$\mathcal{A}$ holds initially" guarantees that "$\mathcal{C}$ holds finally", i.e., after running $\mathcal{P}$. We extend the relation $\models$ between states and formulas to a relation between states and *sets* of formulas, as follows:

$$s \models \mathcal{F} \quad := \quad \text{for all } \varphi \in \mathcal{F} :\ s \models \varphi$$

Using this, the semantics of the *specification triple* $\{\mathcal{A}\}\,\mathcal{P}\,\{\mathcal{C}\}$ is now defined as follows:

$$\models \{\mathcal{A}\}\,\mathcal{P}\,\{\mathcal{C}\} \quad \text{iff} \quad \text{for all states } s :\ s \models \mathcal{A} \text{ implies } tra(s, \mathcal{P}) \models \mathcal{C}.$$

Lemma 16 *The specifications may be composed: If $\models \{\mathcal{A}\}\,\mathcal{P}_1\,\{\mathcal{B}\}$ and $\models \{\mathcal{B}\}\,\mathcal{P}_2\,\{\mathcal{C}\}$, then $\models \{\mathcal{A}\}\,\mathcal{P}_1; \mathcal{P}_2\,\{\mathcal{C}\}$*

Proof

$$\begin{array}{ll}
 & \models \{\mathcal{A}\}\,\mathcal{P}_1\,\{\mathcal{B}\} \text{ and } \models \{\mathcal{B}\}\,\mathcal{P}_2\,\{\mathcal{C}\} \\
\equiv & \qquad \{\text{semantics of specification triples}\} \\
 & \text{for all states } s :\ s \models \mathcal{A} \text{ implies } tra(s, \mathcal{P}_1) \models \mathcal{B} \text{ and} \\
 & \text{for all states } s' :\ s' \models \mathcal{B} \text{ implies } tra(s', \mathcal{P}_2) \models \mathcal{C} \\
\Rightarrow & \qquad \{\text{instantiate } s' \leftarrow tra(s, \mathcal{P}_1)\} \\
 & \text{for all states } s :\ s \models \mathcal{A} \text{ implies } tra(s, \mathcal{P}_1) \models \mathcal{B} \text{ and} \\
 & tra(s, \mathcal{P}_1) \models \mathcal{B} \text{ implies } tra(tra(s, \mathcal{P}_1), \mathcal{P}_2) \models \mathcal{C}
\end{array}$$

$$
\begin{array}{ll}
\Rightarrow & \qquad \{\text{transitivity of implication}\} \\
 & \text{for all states } s: \ s \models \mathcal{A} \text{ implies } \mathit{tra}(\mathit{tra}(s, \mathcal{P}_1), \mathcal{P}_2) \models \mathcal{C} \\
\equiv & \qquad \{\text{definition of } \mathit{tra}\} \\
 & \text{for all states } s: \ s \models \mathcal{A} \text{ implies } \mathit{tra}(s, \mathcal{P}_1; \mathcal{P}_2) \models \mathcal{C} \\
\equiv & \qquad \{\text{semantics of specification triples}\} \\
 & \models \{\mathcal{A}\}\, \mathcal{P}_1; \mathcal{P}_2\, \{\mathcal{C}\}
\end{array}
$$

□

Similarly, one can prove:

Lemma 17 *If* $\models \{\mathcal{A}\}\,\mathcal{P}\,\{\mathcal{B}\}$ *and* $\models \{\mathcal{A}'\}\,\mathcal{P}\,\{\mathcal{B}'\}$, *then* $\models \{\mathcal{A}\cup\mathcal{A}'\}\,\mathcal{P}\,\{\mathcal{B}\cup\mathcal{B}'\}$

7 Correctness of protocols

Our aim now is to prove that if $\mathcal{C}$ can be derived in our logic from $\mathcal{A}$ together with (some yet-to-be-defined logic translation of) $\mathcal{P}$, then $\models \{\mathcal{A}\}\,\mathcal{P}\,\{\mathcal{C}\}$ holds. From that we can conclude a rectified version, so that we know that participants in protocols draw correct conclusions.

As we have seen, the sending of a message is modelled by adding the message to the sender's $\mathcal{O}$ set of messages once-said, and to the receiver's $\mathcal{S}$ set of messages seen, and then to apply the closure as mentioned in section 3. We now define the logical equivalent of this:

Definition 18 *For an action* $P \to Q : X$, *i.e., the sending of a message* X *from* P *to* Q, *we define its* logic translation $\mathbf{T}(P \to Q : X)$ *as a (singleton) set of formulas:*

$$\mathbf{T}(P \to Q : X) \quad := \quad \{P \,\textsf{once\_said}\, X \ \wedge \ Q \,\textsf{sees}\, X\}$$

The extension to protocols is recursively defined:

$$
\begin{array}{lcl}
\mathbf{T}(\emptyset) & := & \emptyset \\
\mathbf{T}(\mathcal{P}_1; \mathcal{P}_2) & := & \mathbf{T}(\mathcal{P}_1)\cup\mathbf{T}(\mathcal{P}_2)
\end{array}
$$

Lemma 19 *For all actions a:* $\models \{\emptyset\}\, a\, \{\mathbf{T}(a)\}$

Proof Let a be $P \to Q : X$.

$$
\begin{array}{ll}
 & \models \{\emptyset\}\, P \to Q : X\, \{\mathbf{T}(P \to Q : X)\} \\
\equiv & \qquad \{\text{semantics of specification triples}\} \\
 & \text{for all } s: \ s \models \emptyset \text{ implies } \mathit{tra}(s, P \to Q : X) \models \mathbf{T}(P \to Q : X) \\
\equiv & \qquad \{\text{definition of } \mathbf{T}\} \\
 & \text{for all } s: \ s \models \emptyset \text{ implies } \mathit{tra}(s, P \to Q : X) \models \{P \,\textsf{once\_said}\, X \wedge Q \,\textsf{sees}\, X\} \\
\equiv & \qquad \{\text{definition of } \models \text{ on sets of formulas}\} \\
 & \text{for all } s: \ \mathit{tra}(s, P \to Q : X) \models P \,\textsf{once\_said}\, X \wedge Q \,\textsf{sees}\, X \\
\equiv & \qquad \{\text{definition of } \mathit{tra}\} \\
 & \text{for all } s: \ \mathit{clo}(s[\mathcal{O}_P \leftarrow \mathcal{O}_P\cup\{X\}, \mathcal{S}_Q \leftarrow \mathcal{S}_Q\cup\{X\}]) \models P \,\textsf{once\_said}\, X \wedge Q \,\textsf{sees}\, X
\end{array}
$$

Now let s be any state, and put $s' = \mathit{clo}(s[\mathcal{O}_P \leftarrow \mathcal{O}_P\cup\{X\}, \mathcal{S}_Q \leftarrow \mathcal{S}_Q\cup\{X\}])$. We have

$$
\begin{array}{ll}
 & X \in \mathcal{O}_P\cup\{X\} \wedge X \in \mathcal{S}\cup\{X\} \\
\Rightarrow & \qquad \{\mathit{clo} \text{ is augmenting}\} \\
 & X \in \mathcal{O}'_P \wedge X \in \mathcal{S}'_Q \\
\equiv & \qquad \{\text{semantics of } \textsf{once\_said} \text{ and } \textsf{sees}\} \\
 & s' \models P \,\textsf{once\_said}\, X \wedge Q \,\textsf{sees}\, X
\end{array}
$$

□

Definition 20 *For a collection of predicates $\mathcal{A}$ and a protocol step $a = P \to Q : X$, the predicate $\mathcal{A}\,allows\,a$ is defined recursively with respect to the structure of the message X:*

$$\begin{array}{lcl}
\mathcal{A}\,allows\;P \to Q : K(X|P) & := & \textit{for some } S:\; \mathcal{A} \vdash P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,S) \\
 & & \textit{and } \mathcal{A}\,allows\;P \to S : X \\
\mathcal{A}\,allows\;P \to Q : K(X|R), R \neq P & := & \mathcal{A} \vdash P\,\mathsf{sees}\,K(X|R) \\
\mathcal{A}\,allows\;P \to Q : (X,Y) & := & \mathcal{A}\,allows\;P \to Q : X \text{ and } \mathcal{A}\,allows\;P \to Q : Y \\
\mathcal{A}\,allows\;P \to Q : \varphi & := & \mathcal{A} \vdash P\,\mathsf{believes}\,\varphi \\
\mathcal{A}\,allows\;P \to Q : X & := & \textit{true (all other cases)}
\end{array}$$

Longer protocols are allowed if each of the steps is allowed in the respective states:

$$\begin{array}{lcl}
\mathcal{A}\,allows\;\emptyset & := & true \\
\mathcal{A}\,allows\;(a;\mathcal{P}) & := & \mathcal{A}\,allows\;a \text{ and } (\mathcal{A} \cup \mathbf{T}(a))\;allows\;\mathcal{P}
\end{array}$$

Lemma 21 *If $\mathcal{A}\,allows\,a$, then $\mathcal{R}[\![\mathcal{A}]\!]\,allows\,a$.*

Proof We prove $\mathcal{R}[\![\mathcal{A}]\!]\,allows\;P \to Q : X$ from $\mathcal{A}\,allows\;P \to Q : X$ with induction on X.

Case $K(X|P)$:

$$\begin{array}{ll}
 & \mathcal{A}\,allows\;P \to Q : K(X|P) \\
\equiv & \qquad \{\text{definition } \textit{allows}\,\} \\
 & \text{for some } S:\; \mathcal{A} \vdash P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,S) \\
 & \text{and } \mathcal{A}\,allows\;P \to S : X \\
\Rightarrow & \qquad \{\text{Theorem 9}\} \\
 & \text{for some } S:\; \mathcal{R}[\![\mathcal{A}]\!] \vdash \mathcal{R}[\![P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,S)]\!] \\
 & \text{and } \mathcal{A}\,allows\;P \to S : X \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \text{for some } S:\; \mathcal{R}[\![\mathcal{A}]\!] \vdash P\,\mathsf{rightly\_believes}\,K\,\mathsf{key\_of}\,(P,S) \\
 & \text{and } \mathcal{A}\,allows\;P \to S : X \\
\Rightarrow & \qquad \{\text{definition } \mathsf{rightly\_believes}\,\} \\
 & \text{for some } S:\; \mathcal{R}[\![\mathcal{A}]\!] \vdash P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,S) \\
 & \text{and } \mathcal{A}\,allows\;P \to S : X \\
\Rightarrow & \qquad \{\text{Induction Hypothesis}\} \\
 & \text{for some } S:\; \mathcal{R}[\![\mathcal{A}]\!] \vdash P\,\mathsf{believes}\,K\,\mathsf{key\_of}\,(P,S) \\
 & \text{and } \mathcal{R}[\![\mathcal{A}]\!]\,allows\;P \to S : X \\
\equiv & \qquad \{\text{definition } \textit{allows}\,\} \\
 & \mathcal{R}[\![\mathcal{A}]\!]\,allows\;P \to Q : K(X|P)
\end{array}$$

Case $K(X|R), R \neq P$:

$$\begin{array}{ll}
 & \mathcal{A}\,allows\;P \to Q : K(X|R) \\
\equiv & \qquad \{\text{definition } \textit{allows}\,\} \\
 & \mathcal{A} \vdash P\,\mathsf{sees}\,K(X|R) \\
\Rightarrow & \qquad \{\text{Theorem 9}\} \\
 & \mathcal{R}[\![\mathcal{A}]\!] \vdash \mathcal{R}[\![P\,\mathsf{sees}\,K(X|R)]\!] \\
\equiv & \qquad \{\text{definition rectify}\}
\end{array}$$

$$
\begin{array}{ll}
 & \mathcal{R}[\![\mathcal{A}]\!] \vdash P\,\mathsf{sees}\,K(X|R) \\
\equiv & \qquad \{\text{definition } \mathit{allows}\,\} \\
 & \mathcal{R}[\![\mathcal{A}]\!]\ \mathit{allows}\ P \rightarrow Q : K(X|R)
\end{array}
$$

Case (X, Y):

$$
\begin{array}{ll}
 & \mathcal{A}\ \mathit{allows}\ P \rightarrow Q : (X, Y) \\
\equiv & \qquad \{\text{definition } \mathit{allows}\,\} \\
 & \mathcal{A}\ \mathit{allows}\ P \rightarrow Q : X \text{ and } \mathcal{A}\ \mathit{allows}\ P \rightarrow Q : Y \\
\Rightarrow & \qquad \{\text{Induction Hypothesis}\} \\
 & \mathcal{R}[\![\mathcal{A}]\!]\ \mathit{allows}\ P \rightarrow Q : X \text{ and } \mathcal{R}[\![\mathcal{A}]\!]\ \mathit{allows}\ P \rightarrow Q : Y \\
\equiv & \qquad \{\text{definition } \mathit{allows}\,\} \\
 & \mathcal{R}[\![\mathcal{A}]\!]\ \mathit{allows}\ P \rightarrow Q : (X, Y)
\end{array}
$$

Case φ:

$$
\begin{array}{ll}
 & \mathcal{A}\ \mathit{allows}\ P \rightarrow Q : \varphi \\
\equiv & \qquad \{\text{definition } \mathit{allows}\,\} \\
 & \mathcal{A} \vdash P\,\mathsf{believes}\,\varphi \\
\Rightarrow & \qquad \{\text{Theorem 9}\} \\
 & \mathcal{R}[\![\mathcal{A}]\!] \vdash \mathcal{R}[\![P\,\mathsf{believes}\,\varphi]\!] \\
\equiv & \qquad \{\text{definition rectify}\} \\
 & \mathcal{R}[\![\mathcal{A}]\!] \vdash P\,\mathsf{rightly\_believes}\,\varphi \\
\Rightarrow & \qquad \{\text{definition } \mathsf{rightly\_believes}\,\} \\
 & \mathcal{R}[\![\mathcal{A}]\!] \vdash P\,\mathsf{believes}\,\varphi \\
\equiv & \qquad \{\text{definition } \mathit{allows}\,\} \\
 & \mathcal{R}[\![\mathcal{A}]\!]\ \mathit{allows}\ P \rightarrow Q : \varphi
\end{array}
$$

Case other X:

$$
\begin{array}{ll}
 & \mathcal{A}\ \mathit{allows}\ P \rightarrow Q : X \\
\equiv & \qquad \{\text{definition } \mathit{allows}\,\} \\
 & \text{true} \\
\equiv & \qquad \{\text{definition } \mathit{allows}\,\} \\
 & \mathcal{R}[\![\mathcal{A}]\!]\ \mathit{allows}\ P \rightarrow Q : X
\end{array}
$$

□

Definition 22 *We define* positive *formulas as the least set such that:*

φ	*is positive if*	$\vdash \varphi$;
$K\ \mathsf{key\_of}\ (P, Q)$	*is positive*;	
$P\ \mathsf{possesses}\ K$	*is positive*;	
$P\ \mathsf{believes}\ \mathsf{fresh}\ X$	*is positive*;	
$P\ \mathsf{believes}\ \varphi$, *other formulas*	*is positive if*	φ *is positive;*
$(P\ \mathsf{controls}\ \varphi) \wedge \varphi$	*is positive if*	φ *is positive;*
$(P\ \mathsf{believes}\ Q\ \mathsf{controls}\ \varphi) \wedge (R\ \mathsf{believes}\ \varphi)$	*is positive if*	φ *is positive;*
$P\ \mathsf{sees}\ X$	*is positive*;	
$P\ \mathsf{once\_said}\ X$	*is positive*;	
$\varphi \wedge \psi$	*is positive if*	φ *is positive and* ψ *is positive;*
$\varphi \vee \psi$	*is positive if*	φ *is positive and* ψ *is positive;*
$(\forall x :: \varphi)$	*is positive if*	$\varphi[x \leftarrow u]$ *is positive for all terms* u *of the appropriate kind not containing unbound variables.*

This is extended to finite sets of formulas: $\mathcal{F}$ is positive whenever the formula $\bigwedge \mathcal{F}$ is.

Lemma 23 *If* $\mathcal{A} \cup \mathbf{T}(a)$ *is positive and* $\mathcal{A}$ *allows* a, *then* $\models \{\mathcal{A}\}\, a\, \{\mathcal{A}\}$

This follows immediately from the following lemma:

Lemma 24 *If* $\mathcal{A}$ *allows* a, $\mathcal{A} \vdash \varphi$ *and* φ *positive, then* $\models \{\mathcal{A}\}\, a\, \{\varphi\}$

The proof of this lemma can be found in the appendix.

Lemma 25 *If* $\mathcal{A} \cup \mathbf{T}(a)$ *positive and* $\mathcal{A}$ *allows* a, *then* $\models \{\mathcal{A}\}\, a\, \{\mathcal{A}, \mathbf{T}(a)\}$.

Proof This follows now directly from Lemmas 17, 19 and 23. □

Definition 26 *We define a collection of predicates* $\mathcal{A}$ *to be* safe *iff* $\mathcal{A}$ *positive or there exists a positive collection* $\mathcal{A}'$ *such that* $\mathcal{A} = \mathcal{R}[\![\mathcal{A}']\!]$.

The following lemma follows immediately from the definition of safe.

Lemma 27 *If* $\mathcal{A}$ *is positive, then* $\mathcal{R}[\![\mathcal{A}]\!]$ *is safe.*

We now formulate Lemma 23 for the weaker requirement of $\mathcal{A}$ being safe, rather than positive.

Lemma 28 *If* $\mathcal{A} \cup \mathbf{T}(a)$ safe and $\mathcal{A}$ *allows* a, *then* $\models \{\mathcal{A}\}\, a\, \{\mathcal{A}\}$

The proof of this lemma can be found in the appendix.

Lemma 29 *If* $\mathcal{A} \cup \mathbf{T}(a)$ *safe and* $\mathcal{A}$ *allows* a, *then* $\models \{\mathcal{A}\}\, a\, \{\mathcal{A}, \mathbf{T}(a)\}$.

Proof This follows now directly from Lemmas 17, 19 and 23.
□

Theorem 30 *If* $\mathcal{A} \cup \mathbf{T}(\mathcal{P})$ *safe,* $\mathcal{A}$ *allows* $\mathcal{P}$ *and* $\mathcal{A} \cup \mathbf{T}(\mathcal{P}) \vdash \mathcal{C}$, *then* $\models \{\mathcal{A}\}\, \mathcal{P}\, \{\mathcal{C}\}$.

Proof We prove the theorem by induction on the protocol.

Case $\emptyset$ **:**

$$\begin{array}{ll}
 & \mathcal{A}\cup\mathbf{T}(\emptyset) \vdash \mathcal{C} \\
\equiv & \qquad \{\text{definition of } \mathbf{T}(\emptyset)\} \\
 & \mathcal{A} \vdash \mathcal{C} \\
\Rightarrow & \qquad \{\text{soundness (Theorem 11)}\} \\
 & \text{for all states } s\text{: } s \models \mathcal{A} \text{ implies } s \models \mathcal{C} \\
\equiv & \qquad \{\text{definition of } \mathit{tra}(s,\emptyset)\} \\
 & \text{for all states } s\text{: } s \models \mathcal{A} \text{ implies } \mathit{tra}(s,\emptyset) \models \mathcal{C} \\
\equiv & \qquad \{\text{definition of } \models \{\mathcal{A}\}\, \mathcal{P}\, \{\mathcal{C}\}\} \\
 & \models \{\mathcal{A}\}\, \emptyset\, \{\mathcal{C}\}
\end{array}$$

Case $(a;\mathcal{P})$ **:**

$$\begin{array}{ll}
 & \mathcal{A}\cup\mathbf{T}(a;\mathcal{P}) \text{ safe, } \mathcal{A}\, \mathit{allows}\, (a;\mathcal{P}) \text{ and } \mathcal{A}\cup\mathbf{T}(a;\mathcal{P}) \vdash \mathcal{C} \\
\Rightarrow & \qquad \{\text{definitions of } \mathbf{T} \text{ and } \mathit{allows}\ \} \\
 & \mathcal{A}\cup\mathbf{T}(a)\cup\mathbf{T}(\mathcal{P}) \text{ safe, } \mathcal{A}\, \mathit{allows}\, a, \ \mathcal{A}\cup\mathbf{T}(a)\, \mathit{allows}\, \mathcal{P} \text{ and } \mathcal{A}\cup\mathbf{T}(a)\cup\mathbf{T}(\mathcal{P}) \vdash \mathcal{C} \\
\Rightarrow & \qquad \{\text{Induction hypothesis}\} \\
 & \mathcal{A}\cup\mathbf{T}(a) \text{ safe, } \mathcal{A}\, \mathit{allows}\, a \text{ and } \models \{\mathcal{A}\cup\mathbf{T}(a)\}\, \mathcal{P}\, \{\mathcal{C}\} \\
\Rightarrow & \qquad \{\text{Lemma 29}\} \\
 & \models \{\mathcal{A}\}\, a\, \{\mathcal{A}\cup\mathbf{T}(a)\} \text{ and } \models \{\mathcal{A}\cup\mathbf{T}(a)\}\, \mathcal{P}\, \{\mathcal{C}\} \\
\Rightarrow & \qquad \{\text{composition of specifications (Lemma 16)}\} \\
 & \models \{\mathcal{A}\}\, a;\mathcal{P}\, \{\mathcal{C}\}
\end{array}$$

□

From Theorem 9 our main theorem now follows: a proof of a specification in the logic indeed ensures the right conclusions of the principals during the protocol.

Theorem 31 *If* $\mathcal{A}\cup\mathbf{T}(\mathcal{P})$ *positive,* $\mathcal{A}\, \mathit{allows}\, \mathcal{P}$ *and* $\mathcal{A}\cup\mathbf{T}(\mathcal{P}) \vdash \mathcal{C}$*, then* $\models \{\mathcal{R}\llbracket\mathcal{A}\rrbracket\}\, \mathcal{P}\, \{\mathcal{R}\llbracket\mathcal{C}\rrbracket\}$.

Proof Let $\mathcal{A}\cup\mathbf{T}(\mathcal{P})$ be positive, $\mathcal{A}\, \mathit{allows}\, \mathcal{P}$ and $\mathcal{A}\cup\mathbf{T}(\mathcal{P}) \vdash \mathcal{C}$. Then $\mathcal{R}\llbracket\mathcal{A}\cup\mathbf{T}(\mathcal{P})\rrbracket$ is safe (Lemma 27), $\mathcal{R}\llbracket\mathcal{A}\rrbracket\, \mathit{allows}\, \mathcal{P}$ (Lemma 21) and $\mathcal{R}\llbracket\mathcal{A}\rrbracket\cup\mathbf{T}(\mathcal{P}) \vdash \mathcal{R}\llbracket\mathcal{C}\rrbracket$ (Lemma 9). Now we can apply Theorem 30. □

8 Conclusion

The original BAN logic has proved successful for finding many unintended errors in security protocols. It does, though, not spot all potential security breaches and thus is less suited for finding intentional (possibly malicious) errors.

Our formalism resulted from a systematic attempt to formulate precise restrictions under which the changing beliefs of principals during a protocol run accurately reflect the changing state of affairs while communication takes place. The restrictions that emerged from our investigation are rather unelegant and complicated, the reason being that we wanted to keep them such that they can be checked statically and do not exclude well-known examples of protocols. They are, however, necessary; for most of the restrictions we have an example of a simple concrete protocol (not obeying the restriction) that leads to a false conclusion.

The semantic correctness criterium we have formulated is weak; it does not take the threats imposed by intruders and impostors into account. It remains to be investigated whether a stronger correctness criterium requires further restrictions. Extrapolating from our experience, we think in fact that that is rather likely. In view of the complications already engendered, an appropriate question is whether the approach of translating protocols into a logical framework is the most felicitous one.

References

[AT91] Martín Abadi and Mark R. Tuttle. *A Semantics for a Logic of Authentication (Extended Abstract),* ACM Symposium on Principles of Distributed Computing, 1991, Montreal, Quebec, Canada.

[BAN89] Michael Burrows, Martín Abadi and Roger Needham. *A Logic of Authentication,* Report 39, Digital Systems Research Center, Palo Alto, CA.

[BAN90] Michael Burrows, Martín Abadi and Roger Needham. *A Logic of Authentication,* ACM Transactions on Computer Systems, Vol. 8, No. 1, February 1990, pp 18-36.

[GEN69] G. Gentzen, M.E. Szabo (ed.). *The collected papers of Gerhard Gentzen,* North-Holland, Amsterdam, 1969.

[GNY90] Li Gong, Roger Needham and Raphael Yahalom. *Reasoning about Belief in Cryptographic Protocols,* IEEE Computer Society Symposium on Research in Security and Privacy, 1990.

[Ness90] Dan M. Nessett. *A critique of the Burrows, Abadi and Needham Logic,* Operating Systems Review, Vol. 24, No. 2, April 1990, pp 35-38

[Snek91] Einar Snekkenes. *Exploring the BAN Approach to Protocol Analysis,* IEEE Computer Society Symposium on Research in Security and Privacy, 1991, Oakland, CA.

[Syv91] Paul Syverson. *The Use of Logic in the Analysis of Cryptographic Protocols,* IEEE Computer Society Symposium on Research in Security and Privacy, 1991, Oakland, CA.

[YW93] Alec F. Yasinsac and William A. Wulf. *Evaluating Cryptographic Protocols,* Report CS-93-66, CS & IPC, University of Virginia.