An application of justification logic to protocol verification

Thomas Studer
Institute of Computer Science and Applied Mathematics
University of Bern
Bern, Switzerland
tstuder@iam.unibe.ch

***Abstract*—Recently, Tsukada et al. propose to use multi-agent epistemic logic for a taxonomy of information-hiding/disclosure properties, in particular properties used in authentication protocols. We follow their proposal and introduce a new multi-agent justification logic for protocol analysis and verification. We show our logic at work analyzing a non-repudiation protocol due to Zhou and Gollmann. Based on this example, we then discuss the expressive power of the logic as well as possible further extensions.**

***Keywords*-protocol verification; justification logic; authentication; non-repudiation**

I. Introduction

In their recent paper [1], Tsukada et al. propose a taxonomy of privacy related information-hiding/disclosure properties in terms of traditional modal logic for multi-agent systems. The properties they consider are: anonymity, privacy, onymity, and identity. In particular, they discuss the relationship between identity and *non-repudiation*.

Non-repudiation can be regarded as a variant of authentication. Non-repudiation of origin (NRO) is the property that protects against an originator's false denial of having sent a message and non-repudiation of receipt (NRR) is the property that protects against a recipient's false denial of having received a message.

Using the language of modal logic, the formal specifications of NRO and NRR can be given in the form of maximal identity as

$$\mathsf{says}_a M \to \Box_J \mathsf{says}_a M$$

and

$$\mathsf{sees}_b M \to \Box_J \mathsf{sees}_b M,$$

respectively. Here we assume that a is the originator and b is the recipient of the message M, and J is the judge. Thus, in the language of epistemic logic, NRO reads *if a says M, then the judge will know that a said M* and NRR reads *if b sees M, then the judge will know that b sees M*.

Our aim in the present paper is to take up this epistemic logic definition of non-repudiation. We are going to verify NRO and NRR for a certain protocol using the framework of epistemic logic. However, we will not use traditional modal logic for multi-agent systems but employ a so-called justification logic.

Justification logics [2], [3], [4] are epistemic logics that extend traditional modal logic by adding explicit justifications for an agent's knowledge or belief. Instead of statements *A is known*, denoted $\Box A$, justification logics reason about justifications for knowledge by using the construct $[t]A$ to formalize statements *t is a justification for A*, where the evidence term t can be viewed as an informal justification or a formal mathematical proof depending on the application. For our purpose of protocol verification, we have to introduce a new multi-agent variant of justification logic where some modalities are justified counterparts of the basic modalities from K and some modalities satisfy a justified version of the transitivity axiom (4).

The protocol we are going to study is due to Zhou and Gollmann [5]. It has been proposed as a fair non-repudiation protocol that supports non-repudiation of origin and non-repudiation of receipt with a lightweight involvement of a trusted third party. Neither the originator nor the recipient should gain an advantage by quitting the protocol early. Zhou and Gollmann [6] already provide a formal analysis of their protocol using a BAN [7] like logic, the SVO logic [8] to specify and verify NRO and NRR. Today, there are many variants of this protocol available and also there are several attacks known on this kind of protocols, see for instance [9], [10].

The paper is organized as follows. First we present the new multi-agent justification logic that we will use later for the protocol analysis. In the third section we briefly recall the basic idea of the non-repudiation protocol. Section III is the main part of the paper containing our formalization of the protocol and the derivation of NRO and NRR from certain assumptions. Then we discuss the assumptions of our formalization. We show some hidden (implicit) requirements and their relation to possible attacks. We also study the role of justification terms in our derivation of NRO and NRR and hint at some possible extensions of justification logic that would allow a more precise analysis. Finally we mention related work and conclude the paper.

II. Justification logic

Definition 1 (Language)**.** We start with two countable set of indices $\{\mathsf{A}, \mathsf{B}, \ldots\}$ and $\{\mathsf{sA}, \mathsf{sB}, \ldots\}$. The first set contains the agents that we consider. The second set is needed in order to have modalities that can express when an agent says something. An index of the second set is called a *sender index*.

We fix countable sets Cons of *constants*, Vars of *variables*, and Prop of *atomic propositions*. The *language of* J consists of the *terms* $t \in \mathsf{Tm}$ and the *formulas* $A \in \mathsf{Fml}$ formed by the following grammar

$$\begin{aligned} t &::= x \mid c \mid (t \cdot t) \mid !^{i,j} t \\ A &::= p \mid \neg A \mid (A \to A) \mid [t]^i A \end{aligned}$$

where i and j are indices, $x \in \mathsf{Vars}$, $c \in \mathsf{Cons}$, and $p \in \mathsf{Prop}$. We define the connectives $\wedge$ and $\vee$ as usual. To say that a term $t \in \mathsf{Tm}$ is *ground* means that t does not contain variables

Often the language of justification logic also includes a binary term operator $+$. However, for the purpose of this paper we do not need this operator and, therefore, dispense with it.

Definition 2 (Deductive System)**.** The *axioms of* J consist of all Fml-instances of the following schemes.

1) All classical propositional tautologies
2) $[t]^i (C \to D) \to ([s]^i C \to [t \cdot s]^i D)$ (application)
3) $[t]^i C \to [!^{i,j} t]^j [t]^i C$ where i is a sender index (checker)

A *constant specification* $\mathcal{CS}$ is any subset

$$\mathcal{CS} \subseteq \bigcup \{ [c]^i A \;\; c \in \mathsf{Cons} \text{ and } A \text{ is an axiom of } \mathsf{J} \}.$$

A constant specification $\mathcal{CS}$ is called *axiomatically appropriate* if for each axiom A of J and each index i there is a constant $c \in \mathsf{Cons}$ such that $[c]^i A \in \mathcal{CS}$.

The *deductive system* $\mathsf{J}(\mathcal{CS})$ is the Hilbert system consisting of the above axioms of J and the following rules of *modus ponens* (MP)

$$\frac{A \quad A \to B}{B}$$

and *axiom necessitation* (AN)

$$\frac{[c]^{i_1} A \in \mathcal{CS}}{[!^{i_{n-1}, i_n} \ldots !^{i_1, i_2} c]^{i_n} \ldots [!^{i_1, i_2} c]^{i_2} [c]^{i_1} A}$$

where $n > 0$ is an integer.

For an arbitrary $\mathcal{CS}$ we write $\Delta \vdash_{\mathcal{CS}} A$ to state that A is derivable from Δ in $\mathsf{J}(\mathcal{CS})$.

Internalization is a crucial property of justification logics which states that the logic internalizes its own notion of proof.

Lemma 3 (Internalization)**.** *Let $\mathcal{CS}$ be an axiomatically appropriate constant specification. If*

$$B_1, \ldots, B_n \vdash_{\mathcal{CS}} A$$

then there is a term $t(x_1, \ldots, x_n) \in \mathsf{Tm}$ such that

$$[x_1]^i : B_1, \ldots, [x_n]^i B_n \vdash_{\mathcal{CS}} [t(x_1, \ldots, x_n)]^i A.$$

Corollary 4. *[Necessitation] Let $\mathcal{CS}$ be an axiomatically appropriate constant specification. If*

$$\vdash_{\mathcal{CS}} A$$

then there is a ground term $t \in \mathsf{Tm}$ such that

$$\vdash_{\mathcal{CS}} [t]^i A.$$

Usually in justification logic, there is no distinction between sender and ordinary indices. We think, however, that this distinction is needed for the application of justification logic to protocol verification. We read $[t]^{\mathsf{sA}} C$ as agent A said C with t being checkable evidence for this, i.e. t may be a message that is signed by A and that contains C. The formula $[t]^{\mathsf{A}} C$ means that agent A beliefs or sees the message t containing C. Further, we read $[!^{\mathsf{sA},\mathsf{J}} t]^{\mathsf{J}} [t]^{\mathsf{sA}} C$ as the agent J beliefs that A said C because he checked A's signature and $!^{\mathsf{A},\mathsf{J}} t$ is the evidence generated by J checking A's signature in the message t. Thus the (checker) axiom states that checkable evidence may indeed by checked by another agent and, moreover, that the checking agent gets new belief by checking the signature.

The distinction between sender and ordinary indices also explains why we have the (checker) axiom as well as an axiom necessitation rule with iterated modalities. The axiom necessitation rule states that if A is an axiom, then there is common belief of A. That means everyone beliefs A, and everyone beliefs that everyone beliefs A, and so on. Corollary 4 then implies that this is not only the case for axioms but for all provable formulas. The reason for this is that in order to check a provable formula one only has to check the proof, but no checking of signatures is needed.

Later in our example, Corollary 4 will be applied to general properties of the protocol. Of course, there should be common belief about how the protocol works and hence also about those general properties. The (checker) axiom, on the other hand, allows an agent to check whether another agent sent a certain signed message. These messages are non-provable since otherwise they would not convey any information.

III. The protocol

In this section we briefly recall the fair non-repudiation protocol by Zhou and Gollmann [5]. Their main idea was to split the message M into two parts: a commitment C and a key K such that C is the message M encrypted with K. The protocol works as follows.

1) The originator A sends the commitment C to the recipient B.
2) The recipient B send a receipt R back to A.
3) The originator A sends the key K to the trusted third party T who makes it publicly available.

4) The recipient obtains the key from T and can thus decrypt the message.
5) The originator checks whether the key is available from T in order to know whether B received the message.

The protocol assumes that the communication channels are not permanently broken. That means the key published by T will be available to A and B.

Our presentation of the protocol is simplified but sufficient for our purpose. The original protocol includes for instance flags that indicate the purpose of a message as well as labels to link C and M. Since we are only interested in one run of the protocol that matching is clear and need not be modeled. It is also clear who the originator and recipient are and thus we also do not encode them in our messages (in contrast to the original protocol).

IV. Formal verification

A. Goals

Non-repudiation of origin means that the judge beliefs that A said M. Formally we require that there are terms t_1 and t_2 such that

$$[t_1]^{\mathsf{J}}[t_2]^{\mathsf{sA}}M. \tag{NRO}$$

Non-repudiation of receipt means that judge beliefs that B beliefs that M. Formally we require that there are terms t_1 and t_2 such that

$$[t_1]^{\mathsf{J}}[t_2]^{\mathsf{B}}M. \tag{NRR}$$

B. Axioms about the protocol

The commitment (ciphertext) and the key together provide the message:

$$C \wedge K \to M \tag{1}$$

If the trusted third party publishes the key, then A must have said it before (to the third party):

$$[x]^{\mathsf{sT}}K \to [p_1(x)]^{\mathsf{sA}}K \tag{2}$$

If the trusted third party publishes the key, then B will see it:

$$[x]^{\mathsf{sT}}K \to [p_2(x)]^{\mathsf{B}}K \tag{3}$$

If B provides a receipt, then B got the commitment:

$$[x]^{\mathsf{sB}}R \to [q(x)]^{\mathsf{B}}C \tag{4}$$

We assume that these facts about the protocol are general common belief among the agents taking part in in the protocol. Therefore, we model them as axioms of our logic. In particular, that means that an axiomatically appropriate constant specification must take them into account by providing justifications for each agent and each of these facts. Then we can apply Necessitation and obtain the following.

From (1) we get that there exists a term s_1 with

$$[s_1]^{\mathsf{sA}}(C \wedge K \to M).$$

Hence we have

$$[x]^{\mathsf{sA}}(C \wedge K) \to [s_1 \cdot x]^{\mathsf{sA}}M.$$

Applying Necessitation again provides us with a term r_1 such that

$$[r_1]^{\mathsf{J}}([x]^{\mathsf{sA}}(C \wedge K) \to [s_1 \cdot x]^{\mathsf{sA}}M). \tag{5}$$

Similarly, we find terms s_2 and r_2 such that

$$[r_2]^{\mathsf{J}}([x]^{\mathsf{B}}(C \wedge K) \to [s_2 \cdot x]^{\mathsf{B}}M). \tag{6}$$

Moreover, applying Necessitation to (2) yields a term t_1 with

$$[t_1]^{\mathsf{J}}([x]^{\mathsf{sT}}K \to [p_1(x)]^{\mathsf{sA}}K). \tag{7}$$

The same reasoning applied to (3) yields a term t_2 with

$$[t_2]^{\mathsf{J}}([x]^{\mathsf{sT}}K \to [p_2(x)]^{\mathsf{B}}K). \tag{8}$$

Similarly, we obtain from (4) that there exists a term k with

$$[k]^{\mathsf{J}}([x]^{\mathsf{sB}}R \to [q(x)]^{\mathsf{B}}C). \tag{9}$$

C. Premises

To prove the goal NRO, B ought to provide the message it has received from A to the judge. That is

$$[sC]^{\mathsf{sA}}C. \tag{10}$$

To prove the goal NRR, A ought to provide the receipt from B to the judge. That is

$$[sR]^{\mathsf{sB}}R. \tag{11}$$

The trusted third party provides the key. That is

$$[sK]^{\mathsf{sT}}K. \tag{12}$$

D. Verification

We will now show that we can derive our goals from the premises given in the previous subsection. Let us first show (NRO).

First, the judge verifies A's signature in (10), that is from (10) we obtain

$$[!^{\mathsf{sA},\mathsf{J}}sC]^{\mathsf{J}}[sC]^{\mathsf{sA}}C. \tag{13}$$

Then, the judge verifies the third party's signature in (12), that is from (12) we obtain

$$[!^{\mathsf{sT},\mathsf{J}}sK]^{\mathsf{J}}[sK]^{\mathsf{sT}}K. \tag{14}$$

The judge beliefs that since the third party publishes the key, A must have said it. That is applying (7) to (14) yields

$$[t_1 \cdot !^{\mathsf{sT},\mathsf{J}}sK]^{\mathsf{J}}[p_1(sK)]^{\mathsf{sA}}K. \tag{15}$$

From (13) and (15) we find by logical reasoning terms v, w such that

$$[v]^{\mathsf{J}}[w]^{\mathsf{sA}}(C \wedge K).$$

The judge beliefs that the commitment and the key together provide the message. That is applying (5) finally yields

$$[r_1 \cdot v]^{\mathsf{J}}[s_1 \cdot w]^{\mathsf{sA}}M.$$

Thus (NRO) is established.

We will now show (NRR). From (11) we obtain

$$[!^{\mathsf{sB},\mathsf{J}} sR]^{\mathsf{J}}[sR]^{\mathsf{sB}}R.$$

Applying (9) gives us

$$[k \cdot !^{\mathsf{sB},\mathsf{J}} sR]^{\mathsf{J}}[q(sR)]^{\mathsf{B}}C. \tag{16}$$

As above, we get from (12) and (8)

$$[t_2 \cdot !^{\mathsf{sT},\mathsf{J}} sK]^{\mathsf{J}}[p_2(sK)]^{\mathsf{B}}K. \tag{17}$$

Again as above, by (16) and (17) there are terms h, l such that

$$[h]^{\mathsf{J}}[l]^{\mathsf{B}}(C \wedge K).$$

Applying (6) finally yields

$$[r_2 \cdot h]^{\mathsf{J}}[s_2 \cdot l]^{\mathsf{B}}M.$$

Thus (NRR) is established.

V. Discussion

As already mentioned in the introduction, there are several attacks known on this kind of protocols [9], [10]. So, what is wrong with our analysis? From a mathematical perspective everything is OK, of course. However, the problem is that we have to guarantee that a concrete implementation satisfies the (implicit) assumptions of our formalization. For instance, axiom (9) states that the recipient sends a receipt R after seeing the commitment C. In our formalization, there is no connection between R and C. So when A presents R to the judge to prove that she said a certain message, we implicitly assume that R and C match to the same message. A concrete implementation of the protocol has to guarantee this connection of R and C which is one of the attack points that has been exploited and that has to be addressed in a future extension of our logic.

The justification terms precisely reflect how the judge proceeds. In particular they show which signatures the judge verifies. For instance, in (15) the term $t_1 \cdot !^{\mathsf{sT},\mathsf{J}} sK$ means that the judge verifies T's signature, thus beliefs $[sK]^{\mathsf{sT}}K$ from which the judge then infers that $[p_1(sK)]^{\mathsf{sA}}K$.

There is also another proof of this fact. The judge may not check T's signature but from (12) and (2) directly go to $[p_1(sK)]^{\mathsf{sA}}K$ and then verify A's signature. We could model this as follows. From (12) and (2) we infer by modus ponens $[p_1(sK)]^{\mathsf{sA}}K$. Verifying the signature then gives $[!^{\mathsf{sA},\mathsf{J}} p_1(sK)]^{\mathsf{J}}[p_1(sK)]^{\mathsf{sA}}K$. We note that the indices in the ! operation clearly show that a different signature has been checked.

This also hints at two possible extension of our present work. In our current formalization, if an agent A says a message, then this message is always signed, and any other agent may check the signature. We do not have the possibility to express who possesses the public signature keys of A and may thus verify the origin of the message and who does not have access to the keys and thus cannot check the signature.

We neither have the possibility to send unsigned messages. If we look at (2), then x is signed by T (which we want) but also necessarily by our modeling $p_1(x)$ is signed by A. This is why the above alternative proof where J checks A's signature is possible. But maybe T drops A's signature and sends the message only with its own signature. However, currently we are not able to model this. A possible solution would be to introduce annotated terms where t^{A} means that t is signed by A and simply t means that it is unsigned. Then we can distinguish

$$[x^{\mathsf{T}}]^{\mathsf{sT}}K \to [p_1(x)^{\mathsf{A}}]^{\mathsf{sA}}K$$

where A's signature is kept and passed on from

$$[x^{\mathsf{T}}]^{\mathsf{sT}}K \to [p_1(x)]^{\mathsf{sA}}K$$

where A's signature is dropped.

VI. Related Work

Of course, a lot of work has been carried out on formal protocol verification. But as far as we know, the present paper is the first one that uses justification logic for this purpose. Still there are some important related results in the area of justification logic for communicating agents and security.

Yavorskaya [11] studies a multi-agent justification logic with various operations of evidence transfer between the agents. In particular, she introduced the $!^{\mathsf{A},\mathsf{B}}$ operator with which one agent can check another agent's evidence.

Artemov [12] also studies a multi-agent scenario with two agents that have unequal epistemic powers: the Observer has sufficient evidence to reproduce the Object Agent's thinking, but not vice versa.

Bucheli et al. [13] introduce a justification logic with common knowledge. As an application, they study the problem of coordinated attack. Classically, the issue there is that messages may get lost. Bucheli et al. show that when the problem is modeled using justification logic (instead of traditional modal logic), then there may also be another issue, namely insufficient evidence for the origin of the message. That may be, for instance, missing signatures.

The idea of supplying messages with justifications is also used in [14] to describe a distributed system that authorizes the disbursement of sensitive information, such as medical records, while maintaining a specified privacy policy. Although that approach is not formalized in a justification logic, the ideas are very similar.

The recent paper [15] introduces a combination of description logic and justification logic. One of the applications that are mentioned for this combination is data privacy for description logic knowledge bases. There the idea is to use the justification terms to track the inferences made in the deduction of sensitive information from public knowledge.

VII. Conclusion

We took up the proposal of Tsukada et al. to use epistemic logic to specify non-repudiation properties. To do so, we introduced a new multi-agent justification logic where

1) some modalities (modeling that an agent beliefs or sees something) are justified counterparts of the basic modalities from K and
2) some modalities (modeling that an agent says something) satisfy a certain justified multi-agent version of the transitivity axiom (4).

In the process of deriving the verification goals evidence terms are constructed that justify the beliefs of the agents. Those terms reflect who actually checks which signatures in a run of the protocol. Our example also shows that there are implicit assumptions in our formalization that (currently) cannot be expressed in justification logic. The identification of these issues will lead to stronger justification logics that will be able to express more subtle details occurring in agent communication.

Acknowledgment

We would like to thank Johannes Werner for pointing us to [1]. We also would like to thank Roman Kuznets for many discussions about justification logics.

References

[1] Y. Tsukada, K. Mano, H. Sakurada, and Y. Kawabe, "Anonymity, privacy, onymity, and identity: A modal logic approach," *Journal of Applied Non-classical Logics*, vol. 3, no. 3, pp. 177–198, 2010.

[2] S. N. Artemov, "Operational modal logic," Cornell University, Tech. Rep. MSI 95–29, Dec. 1995.

[3] ——, "Explicit provability and constructive semantics," *Bulletin of Symbolic Logic*, vol. 7, no. 1, pp. 1–36, Mar. 2001.

[4] ——, "The logic of justification," *The Review of Symbolic Logic*, vol. 1, no. 4, pp. 477–513, Dec. 2008.

[5] J. Zhou and D. Gollman, "A fair non-repudiation protocol," in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 1996, pp. 55–61.

[6] J. Zhou and D. Gollmann, "Towards verification of non-repudiation protocols," in *Proceedings of 1998 International Refinement Workshop and Formal Methods*. Springer-Verlag, 1998, pp. 370–380.

[7] M. Burrows, M. Abadi, and R. Needham, "A logic of authentication," *ACM Transactions on Computer Systems*, vol. 8, pp. 18–36, 1990.

[8] P. F. Syverson and P. C. V. Oorschot, "On unifying some cryptographic protocol logics," in *Proceedings of the 1994 IEEE Symposium on Security and Privacy*. IEEE Computer Society, 1994, pp. 14–28.

[9] C. Boyd and P. Kearney, "Exploring fair exchange protocols using specification animation," in *Information Security*, ser. Lecture Notes in Computer Science, G. Goos, J. Hartmanis, J. van Leeuwen, J. Pieprzyk, J. Seberry, and E. Okamoto, Eds., vol. 1975. Springer Berlin / Heidelberg, 2000, pp. 427–500.

[10] S. Grgens, C. Rudolph, and H. Vogt, "On the security of fair non-repudiation protocols," in *Information Security*, ser. Lecture Notes in Computer Science, C. Boyd and W. Mao, Eds. Springer Berlin / Heidelberg, 2003, vol. 2851, pp. 193–207.

[11] T. Yavorskaya (Sidon), "Interacting explicit evidence systems," *Theory of Computing Systems*, vol. 43, no. 2, pp. 272–293, Aug. 2008.

[12] S. N. Artemov, "Tracking evidence," in *Fields of Logic and Computation, Essays Dedicated to Yuri Gurevich on the Occasion of His 70th Birthday*, ser. Lecture Notes in Computer Science, A. Blass, N. Dershowitz, and W. Reisig, Eds. Springer, 2010, vol. 6300, pp. 61–74.

[13] S. Bucheli, R. Kuznets, and T. Studer, "Justifications for common knowledge," *Journal of Applied Non-classical Logics*, vol. 21, pp. 35–60, 2011.

[14] A. Blass, Y. Gurevich, M. Moskal, and I. Neeman, "Evidential authorization," in *The Future of Software Engineering*, S. Nanz, Ed. Springer, 2011, pp. 73–99.

[15] T. Studer, "Justified terminological reasoning," in *Ershov Informatics Conference (Proceedings)*, E. Clarke, I. Virbitskaite, and A. Voronkov, Eds. Ershov Institute of Informatics Systems, 2011, pp. 177–185.