A Tableaux System for Dolev-Yao Multi-Agent Epistemic Logic

Luiz C. F. Fernandez[1], **Mario R. F. Benevides**[2]

[1]PESC/Coppe – Universidade Federal do Rio de Janeiro (UFRJ)
Rio de Janeiro, RJ – Brazil

[2]Instituto de Computação – Universidade Federal Fluminense (UFF)
Niterói, RJ – Brazil

lcfernandez@cos.ufrj.br, mario@ic.uff.br

Abstract. *Given the increasing importance of security protocols in our daily activities and communication via internet, the efforts to develop mechanisms and models for verification of such protocols are always relevant. In this work, we explore the Dolev-Yao Multi-Agent Epistemic Logic by providing a tableaux method for it. This logic is an extension of Multi-Agent Epistemic Logic, aimed to verify authenticity and safety in communication protocols and inspired by the Dolev-Yao model, a seminal work in formal cryptography.*

1. Introduction

Security protocols are increasingly present in our daily lives: behind financial transactions, communication, file downloads, i.e., information access in general. There are some risks involved, such as key or password cracking, the tracking of users' actions and so on. A good implementation is a difficult issue due to saboteur's behavior possibilities.

Most security protocols are based on *one-way functions*, which is a good way of encryption, since it uses functions that are easy to compute, but hard to invert without knowing a specific complementary information. Works related to the logical verification of such specifications, also called *formal cryptography* [Dolev and Yao 1983, Burrows et al. 1990, Syverson 1991], consider a perfect encryption scheme (the vulnerability of the protocol results from a logical error in the specification) and the models are obtained from encryption and decryption functions.

Multi-agent epistemic logics are designed to reason about knowledge of agents and groups [Fagin et al. 2004]. As pointed by [van Ditmarsch et al. 2007], nowadays, these logics are influenced by the development of modal logics and the system $\mathbb{S}5$ is the most popular one. Its use is relevant in many distinct areas, such as philosophy, economics, linguistics, cryptography and computer science.

The use of epistemic logic to reasoning about protocol specifications inspired several approaches [Cohen and Dam 2007, Boureanu et al. 2009, Kramer 2008], including the Dolev-Yao Multi-Agent Epistemic Logic [Benevides et al. 2018], a novel multi-agent epistemic logic for reasoning about properties in protocols. It uses structured propositions, which is a new technique to deal with messages, keys and properties in security protocols in uniform manner, keeping the logic propositional.

There are many different automated theorem provers, e.g., resolution, natural deduction and tableaux, from different approaches, namely *direct* or *indirect deduction* and

labeled deductive systems. In the latter, we have *prefixed tableaux* [Fitting 1983], which has a proof representation similar to *Kripke semantics* [Kripke 1959]. Our main objective in this work is to provide a tableaux method for Dolev-Yao Multi-Agent Epistemic Logic.

In the next section we present the background for our work: the Dolev-Yao model, the multi-agent epistemic logic $\mathbb{S}5$ and the tableaux method; in Section 3 we present the Dolev-Yao multi-agent epistemic logic $\mathbb{S}5_{DY}$; in Section 4 we provide a tableaux method for $\mathbb{S}5_{DY}$; finally, in Section 5 we conclude with some final remarks.

2. Background

In this section, first we present the Dolev-Yao model, with a brief explanation about public key protocols and an example. Then, we show the formalization of multi-agent epistemic logic $\mathbb{S}5$ and, finally, we describe the tableaux proof procedure.

2.1. Dolev-Yao Model

Introduced by [Dolev and Yao 1983], at the time of great discussion about the use of public key encryption in network communication, this work intends to show why a formal model is desirable to deal with security protocols.

Public key systems are efficient when we have a "passive" saboteur (also called eavesdropper, attacker, intruder and so on), one who only intercepts the communication and tries to decode the message. But [Needham and Schroeder 1978] points out that a not well specified protocol permits an "active" intruder, one who may fake his identity and manipulate the intercepted message, to succeed.

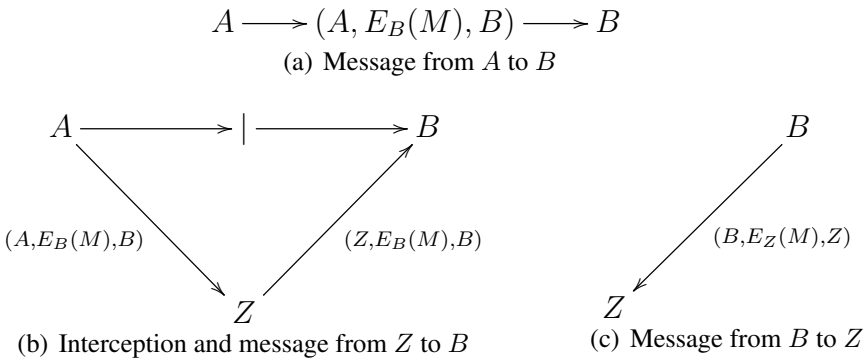
To briefly explain this system [Diffie and Hellman 1976, Rivest et al. 1978], we assume that every user X in the network has an *encryption function* E_X, which generates a pair (X, E_X), inserted in a secure public directory, and a *decryption function* D_X, known only to user X. It is important to notice that the sender's public key is represented, in the message exchange, as a subscript of E. The main requirements are:

- $D_X(E_X(M)) = M$;
- for any user Y, knowing $E_X(M)$ and the directory containing all the public pairs does not reveal anything about M.

A message transmitted between two users is denoted by: the sender's name, the text (encrypted) and the receiver's name. One of the basic assumptions in the perfect public key system is that the functions are unbreakable.

Example 2.1. *In this example, also called* Man-in-the Middle (MITM) attack*, the plaintext is encoded with an encryption function, where the receiver always replies using the sender's public key. Suppose user A wants to send a plaintext M to user B:*

a) A sends message $(A, E_B(M), B)$ to B [Figure 1(a)]*;*
b) Intruder Z intercepts the above message and sends message $(Z, E_B(M), B)$ to B [Figure 1(b)]*;*
c) B sends message $(B, E_Z(M), Z)$ to Z [Figure 1(c)]*;*
d) Z decodes $E_Z(M)$ and obtains M.



(a) Message from A to B

(b) Interception and message from Z to B

(c) Message from B to Z

Figure 1. Illustration of Example 2.1

2.2. Multi-agent epistemic logic

This section presents the multi-agent epistemic logic $\mathbb{S}5$. Using a Kripke structure, the multi-agent approach allows us to represent knowledge and belief of an agent or a group of agents, making it useful in various applications involving communication. We begin with some well-known definitions [Fagin et al. 2004, van Ditmarsch et al. 2007].

Definition 2.1. *The multi-agent epistemic language consists of an enumerable set of propositional symbols Φ, a finite set of agents $\mathcal{A}$, the Boolean connectives $\neg$ and $\wedge$ and a modality K_a for each agent a. The formulae are defined as follows:*

$$\varphi ::= p \mid \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid K_a\varphi, \text{ where } p \in \Phi,\ a \in \mathcal{A}$$

$K_a\varphi$ is intended to mean that "agent a knows φ". We are considering the standard abbreviations and conventions: $\bot \equiv \neg\top$, $\varphi \vee \phi \equiv \neg(\neg\varphi \wedge \neg\phi)$, $\varphi \rightarrow \phi \equiv \neg(\varphi \wedge \neg\phi)$ and $B_a\varphi \equiv \neg K_a \neg\varphi$ ($B_a\varphi$ may be read as "agent a believes φ").

Definition 2.2. *A multi-agent epistemic* frame *is a tuple $\mathcal{F} = (S, R_a)$ where:*

- *S is a non-empty set of states;*
- *R_a is a binary relation over S, for each agent $a \in \mathcal{A}$.*

Definition 2.3. *A multi-agent epistemic* model *is a pair $\mathcal{M} = (\mathcal{F}, V)$, where $\mathcal{F}$ is a multi-agent epistemic frame and V is a valuation function $V : \Phi \rightarrow 2^S$. We call a rooted multi-agent epistemic model $(\mathcal{M}, s)$ an epistemic* state *and we will often write $\mathcal{M}, s$ rather than $(\mathcal{M}, s)$.*

In most applications of multi-agent epistemic logic, the relations R_a are equivalence relations (reflexive, transitive and symmetric relations). In this work we only consider that case, so we use $\sim_a$ for each agent a instead of R_a.

Definition 2.4. *Let $\mathcal{M} = \langle S, \sim_a, V\rangle$ be a multi-agent epistemic model. The notion of satisfaction $\mathcal{M}, s \models \varphi$ is defined as follows:*

- $\mathcal{M}, s \models \top$ *always*
- $\mathcal{M}, s \models p$ *iff $s \in V(p)$*
- $\mathcal{M}, s \models \neg\phi$ *iff $\mathcal{M}, s \not\models \phi$*
- $\mathcal{M}, s \models \phi \wedge \psi$ *iff $\mathcal{M}, s \models \phi$ and $\mathcal{M}, s \models \psi$*
- $\mathcal{M}, s \models K_a\phi$ *iff for all $s' \in S$, if $s \sim_a s'$ then $\mathcal{M}, s' \models \phi$*

2.3. Tableaux method

This system is a tree-structured *refutational method*, in which, in order to prove a formula φ, we start the proof supposing $\neg\varphi$ and then we try to obtain unsatisfiable subformulae in each branch from this negation. If *every* branch is unsatisfiable, then $\neg\varphi$ is unsatisfiable as well, therefore φ is valid. We can also consider it in the sense of *logical consequence* checking: for a database $DB = \{\phi_1, \ldots, \phi_n\}$ and a question φ, $DB \vDash \varphi$ if and only if $(\phi_1 \wedge \cdots \wedge \phi_n) \rightarrow \varphi$ is a tautology, that is, if its negation is a contradiction.

The method presented below is based on the tableaux method for modal logics [Massacci 2000]. As our main concern at the moment is to prove and model the deductions resulted from the bad behaviour of a particular agent, the intruder, certain changes were made to adapt the method to our needs. Some definitions are that: a branch θ of a tableau $\mathcal{T}$ is closed if there is φ and $\neg\varphi$ for any formula φ; and a tableau $\mathcal{T}$ is closed if every branch is closed.

For $\mathbb{S}5$, we must use the sub-tableaux concept to obtain a refutation. A sub-tableau intends to simulate the possible world relation. So, if a sub-tableau is closed, the branch that originated it also closes. As we should use rules that creates a new sub-tableau or add a new formula to previously generated one, we need a mechanism to label it. Each tableau will have a different name, so a formula φ in a tableau refutation is unique, identified by (σ, φ), where σ is the *prefix*. A prefix is any expression used to name a tableau. To manage the creation of new tableaux and the addition of new formulae to a previously generated tableau, we denote ρ as the operator which applied on a formula (σ, φ) it will:

- create a new tableau σ, starting with φ, if σ is not a name for a previously generated tableau subordinated to the branch which φ holds; or
- add φ to the tableau specified by the prefix σ.

Now we present the propositional tableaux rules, for all formulae α and β:

$$\mathrm{R}_{\wedge}\ \frac{\alpha \wedge \beta}{\begin{array}{c}\alpha\\ \beta\end{array}} \qquad \mathrm{R}_{\mathrm{Dneg}}\ \frac{\neg\neg\alpha}{\alpha} \qquad \mathrm{R}^{\neg}_{\wedge}\ \frac{\neg(\alpha \wedge \beta)}{\neg\alpha \quad \neg\beta} \qquad \mathrm{R}_{\rightarrow}\ \frac{\alpha \rightarrow \beta}{\neg\alpha \quad \beta} \qquad \mathrm{R}^{\neg}_{\rightarrow}\ \frac{\neg(\alpha \rightarrow \beta)}{\begin{array}{c}\alpha\\ \neg\beta\end{array}}$$

When rules $\mathrm{R}_{\wedge}$, $\mathrm{R}_{\mathrm{Dneg}}$ and $\mathrm{R}^{\neg}_{\rightarrow}$ are applied, we add the derived subformulae in the same branch of the original formula, while rules $\mathrm{R}^{\neg}_{\wedge}$ and $\mathrm{R}_{\rightarrow}$ split the original branch. The rules for $\mathbb{S}5$ are defined as follows, inspired by [Massacci 2000]:

$$\mathrm{R}_{\pi}\ \frac{\neg K_a\alpha}{\rho(\mathcal{T}'_a, \neg\alpha)}, \text{ where } \mathcal{T}'_a \text{ is a new tableau, indexed by agent } a$$

$$\mathrm{R}_{t}\ \frac{K_a\alpha}{\alpha} \qquad \mathrm{R}^{r}_{4}\ \frac{\rho(\mathcal{T}''_a, K_a\alpha)}{K_a\alpha}$$

$$\mathrm{R}_{4}\ \frac{K_a\alpha}{\rho(\mathcal{T}''_a, K_a\alpha)}, \text{ where } \mathcal{T}''_a \text{ is a previously generated tableau, indexed by agent } a$$

We have rule R_{π} for the π-formulas (from possibility), while rules R_t, R_4 and R^r_4 indicate the correspondence between axioms $K_a\varphi \rightarrow \varphi$, $K_a\varphi \rightarrow K_aK_a\varphi$ and $\neg K_a\varphi \rightarrow K_a\neg K_a\varphi$, respectively, and the properties of accessibility relations mentioned in Definition 2.3.

3. Dolev-Yao Multi-Agent Epistemic Logic

This section summarizes the main concepts of the Dolev-Yao Multi-Agent Epistemic Logic, $\mathbb{S}5_{DY}$ [Benevides et al. 2018]. This system is based on the Dolev-Yao Model and was designed to analyze security protocols.

3.1. Language and semantics

There is a novelty in the language of $\mathbb{S}5_{DY}$: formulae are built from expressions and not only from propositional symbols. Intuitively, an expression is any piece of information that can be encrypted, decrypted or concatenated in order to be communicated.

Definition 3.1. *The Dolev-Yao multi-agent epistemic language consists of an enumerable set Φ of propositional symbols, a finite set $\mathcal{A}$ of agents, an enumerable set of keys $\mathcal{K} = \{k_1, \cdots\}$, the Boolean connectives $\neg$ and $\wedge$ and a modality K_a for each agent a. The expressions and formulae are defined as follows:*

$$E ::= p \mid k \mid (E_1, E_2) \mid \{E\}_k \text{, where } k \in \mathcal{K} \text{ and } p \in \Phi$$
$$\varphi ::= e \mid \top \mid \neg\varphi \mid \varphi_1 \wedge \varphi_2 \mid K_a\varphi \text{, where } e \in E \text{ and } a \in \mathcal{A}$$

Definition 3.2. *A Dolev-Yao multi-agent epistemic* frame *is a tuple $\mathcal{F} = \langle S, \sim_a \rangle$ where:*

- *S is a non-empty set of states;*
- *$\sim_a$ is a reflexive, transitive and symmetric binary relation over S, for each $a \in \mathcal{A}$.*

Definition 3.3. *A Dolev-Yao multi-agent epistemic* model *is a pair $\mathcal{M} = \langle \mathcal{F}, V \rangle$, where $\mathcal{F}$ is a Dolev-Yao multi-agent epistemic frame and V is a valuation function $V : E \to 2^S$ satisfying the following conditions for all $m \in E$ and $k \in \mathcal{K}$:*

1. $V(m) \cap V(k) \subseteq V(\{m\}_k)$
2. $V(\{m\}_k) \cap V(k) \subseteq V(m)$
3. $V(m) \cap V(n) = V((m, n))$

We call a rooted Dolev-Yao multi-agent epistemic model $(\mathcal{M}, s)$ an epistemic *state* and again, we will often write $\mathcal{M}, s$ rather than $(\mathcal{M}, s)$.

Definition 3.4. *Let $\mathcal{M} = \langle S, \sim_a, V \rangle$ be a Dolev-Yao multi-agent epistemic model. The notion of satisfaction $\mathcal{M}, s \models \varphi$ is defined as follows:*

1. $\mathcal{M}, s \models \top$ — *always*
2. $\mathcal{M}, s \models e$ — *iff* $s \in V(e)$
3. $\mathcal{M}, s \models \neg\varphi$ — *iff* $\mathcal{M}, s \not\models \varphi$
4. $\mathcal{M}, s \models \varphi_1 \wedge \varphi_2$ — *iff* $\mathcal{M}, s \models \varphi_1$ *and* $\mathcal{M}, s \models \varphi_2$
5. $\mathcal{M}, s \models K_a\varphi$ — *iff for all* $s' \in S$, *if* $s \sim_a s'$ *then* $\mathcal{M}, s' \models \varphi$

The axioms of $\mathbb{S}5_{DY}$ are listed as follows:

1. *All instantiations of propositional tautologies.*
2. $K_a(\varphi \to \psi) \to (K_a\varphi \to K_a\psi)$
3. $K_a\varphi \to \varphi$
4. $K_a\varphi \to K_aK_a\varphi$ [*positive introspection*]
5. $\neg K_a\varphi \to K_a\neg K_a\varphi$ [*negative introspection*]
6. $m \wedge k \to \{m\}_k$ [*encryption*]
7. $\{m\}_k \wedge k \to m$ [*decryption*]
8. $m \wedge n \leftrightarrow (m, n)$ [*pair composition* & *decomposition*]

Axioms 1 - 5 are standard in $\mathbb{S}5$ literature [Fagin et al. 2004] and axioms 6 - 8 enforce the semantical properties of the conditions of Definition 3.3.

Lemma 3.5. *The following formulas are theorems of* $\mathbb{S}5_{DY}$*:*

1. $K_a m \wedge K_a k \rightarrow K_a\{m\}_k$
2. $K_a\{m\}_k \wedge K_a k \rightarrow K_a m$
3. $K_a m \wedge K_a n \leftrightarrow K_a(m, n)$

Proof. This proof is straightforward from axioms 2, 6 - 8, inference rule *Universal Generalization* ($\frac{\varphi}{K_a\varphi}$) and the fact that $\vdash K_a(\varphi \wedge \psi) \leftrightarrow (K_a\varphi \wedge K_a\psi)$. □

Theorem 3.6. $\mathbb{S}5_{DY}$ *is sound and complete with respect to the class of* $\mathbb{S}5_{DY}$ *models.*

Proof. The soundness and completeness proofs can be found in [Benevides et al. 2018]. □

Example 3.1. *Revisiting Example 2.1, agent A wants to send a message m to B and the receiver always replies a message using the key shared with the sender. The protocol actions are represented in the metalanguage. Assuming that k_{xy} denote the shared key and $k_{xy} = k_{yx}$ for every agent x and y, KB stands for* Knowledge Base*,* i.k. *for* initial knowledge *and* lem. *refers to Lemma 3.5:*

0. $KB_0 = \{K_A k_{AB},\ K_B k_{AB},\ K_B k_{BZ},\ K_Z k_{BZ},\ K_A m\}$ *i.k.*

$KB_0 \vdash K_A\{m\}_{k_{AB}}$ *lem. 1*

$\downarrow$ *send*$_{AB}(\{m\}_{k_{AB}})$

$- - -$

$\downarrow$ *Z intercepts*

1. $KB_1 := KB_0 \cup K_Z\{m\}_{k_{AB}}$

$\downarrow$ *send*$_{ZB}(\{m\}_{k_{AB}})$

2. $KB_2 := KB_1 \cup K_B\{m\}_{k_{AB}}$

$KB_2 \vdash K_B m$ *lem. 2*

$KB_2 \vdash K_B\{m\}_{k_{ZB}}$ *lem. 1*

$\downarrow$ *send*$_{BZ}(\{m\}_{k_{BZ}})$

3. $KB_3 := KB_2 \cup K_Z\{m\}_{k_{BZ}}$

$KB_3 \vdash K_Z m$ *lem. 2*

Intruder Z knows m.

4. Tableaux Method for Dolev-Yao Multi-Agent Epistemic Logic

Now, we present the tableaux method for $\mathbb{S}5_{DY}$. Here we provide a set of rules that allow us to verify if a malicious user can obtain private messages from a communication network, for example, deriving this information from the messages he received or intercepted. The semantics and basic rules for our method are the same as in Section 2.3 and we add the following rules:

$$\mathrm{R_{Dec}}\ \frac{\{m\}_k \quad k}{m} \qquad \mathrm{R^{\neg}_{Enc}}\ \frac{\neg\{m\}_k}{\neg m \quad \neg k} \qquad \mathrm{R_{Pair}}\ \frac{(m,n)}{\begin{array}{c} m \\ n \end{array}} \qquad \mathrm{R^{\neg}_{Pair}}\ \frac{\neg(m,n)}{\neg m \quad \neg n}$$

where $m, \{m\}_k, n, (m,n) \in E$ and $k \in \mathcal{K}$.

Example 4.1. *Let's prove theorem 1 from Lemma 3.5:*

1.	$\neg(K_a m \wedge K_a k \rightarrow K_a\{m\}_k)$	[negation of the question]
2.	$K_a m \wedge K_a k$	[from 1, by $\mathrm{R^{\neg}_{\rightarrow}}$]
3.	$\neg K_a\{m\}_k$	[from 1, by $\mathrm{R^{\neg}_{\rightarrow}}$]
4.	$K_a m$	[from 2, by $\mathrm{R_{\wedge}}$]
5.	$K_a k$	[from 2, by $\mathrm{R_{\wedge}}$]
	Now, we generate a new tableau:	
3.1$_a$.	$\neg\{m\}_k$	[from 3, by $\mathrm{R_{\pi}}$]
3.2$_a$.	$K_a m$	[from 4, by $\mathrm{R_4}$]
3.3$_a$.	$K_a k$	[from 5, by $\mathrm{R_4}$]
3.4$_a$.	m	[from 3.2$_a$, by $\mathrm{R_t}$]
3.5$_a$.	k	[from 3.3$_a$, by $\mathrm{R_t}$]
3.6$_a$.	$\neg m \qquad \neg k$	[from 3.1$_a$, by $\mathrm{R^{\neg}_{Enc}}$]

Since each of the branches closes, we have a closed tableau.

4.1. Soundness, Completeness and Termination property

The soundness and completeness of our tableaux method are based on [Fitting 1983], preserving satisfiability and using the notion of *completed tableau*, respectively. For the tableaux rules presented in Definition 2.3, [Massacci 2000] provides a termination argument, which we extended for our purpose [Fernandez and Benevides 2023].

5. Conclusion

In this work, we provide a proof method for $\mathbb{S}5_{DY}$, a new epistemic logic for reasoning about security protocols. This logic introduces a new semantics based on structured propositions. Instead of building formulas from atomic propositions, they are built from expressions.

The proof method we propose is based on prefixed tableaux method. We made an extension of this concept with our semantics. We already proved soundness, completeness and the termination argument for the system.

We believe that this work contributes to the growing demand for security studies, by integrating concepts of logic in intuitive way and using knowledge formalisms.

Acknowledgements

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Finance Code 001 and by the Brazilian Research Agencies CNPq and FAPERJ.

References

Benevides, M. R. F., Fernandez, L. C. F., and de Oliveira, A. C. C. M. (2018). Dolev-Yao Multi-Agent Epistemic Logic. *SAJL*, 4(2):281–312.

Boureanu, I., Cohen, M., and Lomuscio, A. (2009). Automatic verification of temporal-epistemic prop. of cryptographic protocols. *J. of Applied Non-Classical Logics*, 19(4):463–487.

Burrows, M., Abadi, M., and Needham, R. (1990). A Logic of Authentication. *ACM Trans. on Computer Systems*, 8(1):18–36.

Cohen, M. and Dam, M. (2007). A Complete Axiomatization of Knowledge and Cryptography. In *22nd Annual IEEE Symp. on LICS*, pages 77–88.

Diffie, W. and Hellman, M. E. (1976). New Directions in Cryptography. *IEEE Trans. on Information Theory*, IT-22(6):644–654.

Dolev, D. and Yao, A. C. (1983). On the Security of Public Key Protocols. *IEEE Trans. on Information Theory*, 29(2):198–208.

Fagin, R., Halpern, J. Y., Moses, Y., and Vardi, M. Y. (2004). *Reasoning About Knowledge*. The MIT Press.

Fernandez, L. C. F. and Benevides, M. R. F. (2023). A Tableaux System for $S5_{DY}$ - Soundness, Completeness and Termination Argument. `https://github.com/lcfernandez/wbl-2023-appendix/blob/main/wbl-2023-appendix.pdf`.

Fitting, M. (1983). *Proof Methods for Modal and Intuitionistic Logics*. Springer.

Kramer, S. (2008). Cryptographic protocol logic: Satisfaction for (timed) Dolev-Yao cryptography. *J. of Logic and Algebraic Programming*, 77(1–2):60–91.

Kripke, S. (1959). A Completeness Theorem in Modal Logic. *J. Symbolic Logic*, 24(1):1–14.

Massacci, F. (2000). Single Step Tableaux for Modal Logics. *J. of Automated Reasoning*, 24(3):319–364.

Needham, R. M. and Schroeder, M. D. (1978). Using Encryption for Authentication in Large Networks of Computers. *Comms. of the ACM*, 21(12):993–999.

Rivest, R. L., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Comms. of the ACM*, 21(2):120–126.

Syverson, P. (1991). The Use of Logic in the Analysis of Cryptographic Protocols. In *1991 IEEE Computer Society Symp. on Research in Secur. Priv.*, pages 156–170.

van Ditmarsch, H., van der Hoek, W., and Kooi, B. (2007). *Dynamic Epistemic Logic*. Springer.