ANONYMITY IN SECURITY PROTOCOLS

PhD thesis summary

Supervisor:
Prof. Dr. Ferucio Laurenţiu Ţiplea

Author:
Nicolae Cosmin Vârlan

April, 2013

Nicolae Cosmin Vârlan
Department of Computer Science
"Al.I.Cuza" University of Iaşi, Romania
e-mail: vcosmin@info.uaic.ro

PhD commission

Prof. Dr. Dorel Lucanu, Chairman (Univ. "Al.I.Cuza" Iaşi)
Prof. Dr. Ferucio Laurenţiu Ţiplea, Supervisor (Univ. "Al.I.Cuza" Iaşi)
Prof. Dr. Adrian Atanasiu (Bucharest University)
Prof. Dr. Cătălin Dima (Université Paris-Est Créteil)
Associate Prof. Dr. Ing. Marius Minea (Politehnica University of Timişoara)

Contents

List of published papers

My personal contributions from this thesis were also published [51, 64, 63, 62, 69, 68, 67] as it follows:

1. W. Razouk, F. L. Ţiplea, A. Sekkaki, and **C. Vârlan**. Providing Anonymity for RFID Systems. *Journal of Information and Communication Technologies*, 3, Mar.2013. To appear.

2. F. L. Ţiplea and **C. Vârlan**. Group Anonymity and Role Interchangeability in Security Protocols. In *8th International Workshop on Security and High Performance Computing Systems, 2013.* submitted.

3. F. L. Ţiplea, L. Vamanu, and **C. Vârlan**. Reasoning About Minimal
Anonymity in Security Protocols. *Future Generation Computer Systems*, 29(3):828-842, 2013.

4. F. L. Ţiplea, L. Vamanu, and **C. Vârlan**. Complexity of Anonymity for Security Protocols. In D. Gritzalis, B. Preneel, and TM. Theoharidou, editors, *European Symposium on Research in Computer Security (ESORICS 2010)*, volume 6345 of *Lecture Notes in Computer Science*, pages 558–572, 2010.

5. **C. Vârlan**., C. Sotomayor and A. F. Gomez Skarmeta A Social Approach on Creating Dynamic Maps, In *Positioning and Context-Awarness International Conference*, Antwerpen, Belgium 2009

6. **C. Vârlan**. ITS Approaches in Romania: Applying a Dynamical Perception to Vehicle Navigation, In *Workshop On ITS Applications And European Electronic Tolling*, Bucharest, Romania, 2009

7. **C. Vârlan**. Dynamic GPS Maps, In 11th *International Conference on Development and Application Systems*, Suceava, Romania, 2008

1 Introduction

The origin of the word *anonymity* can be traced back to the Greek language where ἀνωνυμία (*anonymia*) means *nameless.* The anonymity is frequently used with respect to an action some individual does and its intended purpose is to hide the identity of that individual. Usually, the identity of the person who did the action is hidden among a group of identities of some persons that could do the action (the *anonymity set*) [48].

Some domains where the anonymity is required are: information forensics, voting systems, charity acts, sharing unpopular ideas or, when thinking about the actions an individual might do in an electronic environment, the anonymity can be applied to electronic mail, electronic commerce, electronic cash etc.

În literature, the anonymity concept might be found in different forms. Some of them are:

- *unlinkability* – meaning that an observer is unable to establish a link between two agents that collaborated in order to do an action (e.g. the observer is unable to see that two agents communicated);
- *undetectability* – meaning that the observer is unable to see if the item of interest (agent, message or action) really exists in the system;
- *role interchangeability* – meaning that, as far as the observer is concerned, two agents can interchange their roles in the sense that the actions performed by one of them may be seen by the observer as being performed by the other agent [48].

Untraceability is a type of anonymity meaning that an observer is not able to correctly say the path an agent, an individual or a product has followed to travel between two points. This type of anonymity has various application like anonymize the route of an individual who travel through different countries and, even though in each country his passport will be verified, his traveling plans have to remain secret to an external observer. Various techniques were proposed to obtain untraceability of passports, most of them based on RFID untraceability and anonymity [51]. An other field where untraceability is necessary is in inteligent transport systems (ITS), for obtaining anonymous feedback about traffic condition. The idea is for an user to record GPS information and to wirelessly pass it from car to car in a certain area. When a traffic jam appears, the drivers are informed about it in real time; however, because there are more then only one car in the traffic, none of the drivers or external observers can see who originated the information about the jam and that assures both anonymity and untraceability to the drivers [67, 69, 68].

The thesis is organized in seven chapters.

In the introduction we presented a brief overview of the domain, the novelty of the thesis, its structure, and basic elements of cryptography.

Chapter 2 has three sections. In the first section, two methods for obtaining anonymity, their problems, and solutions to those problems are described: Mix Nets and DC-nets. In the second section, following [48], the terminology used in anonymity studies is presented. We conclude this chapter with two models that can be used to describe anonymity: CSP and epistemic logic.

In chapter 3, starting from the basic modal logic, an epistemic logic is created. In order to be able to talk about epistemic logic, an observational equivalence between the states of the system has to be defined. We describe a formalism that can be used to model security protocol and enrich it in order to be able to reason not only about the messages that are sent in the system, but also about the actions made by the agents. Based on this model, we create an observational equivalence and an epistemic logic suited for our needs. A set of deduction rules that can be used by the agents to reason about the facts they recorded is also provided in this chapter. We conclude by formalising several types of observers (with partial view, total view, mobility).

In chapter 4, starting from the formalism and the epistemic logic defined in chapter 3, we define the anonymity concepts we are interested in: *minimal anonymity*, *group anonymity*, *unlinkability*, and *role interchangeability*. Different relationships between the anonymity concepts are established. We also prove that anonymity can be broken if the protocol is played in an active intruder environment and also that an active intruder may induce it even though the protocol is not designed to preserve anonymity.

In chapter 5, we study the decidability problems induced by minimal and group anonymity. It is shown that both minimal and group anonymity decision problems w.r.t. an honest agent (or the intruder) in an unrestricted security protocol are undecidable.

In chapter 6, the complexity of minimal and group anonymity

in (T, k)[1]-bounded protocols is studied. It is shown that the minimal anonymity problem for basic-term actions w.r.t. an honest agent or the intruder is in $NEXPTIME$. For 1-session bounded protocols with basic terms actions, the minimal anonymity problem is in NP. Similar results are obtained for group anonymity.

I would like to thank my supervisor Professor Dr. Ferucio Laurenţiu Ţiplea for the time he invested in working with me, for not only telling me how to research, but showing me as well, for being there for me not only as a supervisor, but also as a friend. My thanks also go to the student Loredana Vamanu who helped in developing the framework used here.

[1] a (T, k)-bounded protocol uses only a finite set of basic terms $T \subseteq \mathcal{T}_0$ and the length of the messages has to be at most k.

2 Modelling Anonymity

The seminal work that marked the development of a formal study of anonymity-related properties is that of David Chaum [6, 7, 8] who proposed a method by which an agent A can send a message to an agent B without revealing his identity. The main idea is to use a *mix net* which takes the message from A and resend it from one mix to another until it reaches B. Each mix hides the correspondences between its input messages and its output messages. The messages are multiple encrypted by public keys so that no mix knows who originated the messages. By using a *return address*, the sender A can protect his identity as a receiver too. Moreover, someone observing the network traffic cannot tell that A and B communicated and, therefore, this method provides *unlinkability* as well. Chaum's mix nets have had a great impact on the development of anonymity technologies, such as *The Onion Routing* [16].

In 1996, a formalization of anonymity in the process algebra of *Communicating Sequential Processes* [55], has been proposed. The main idea was to use a renaming function f_A on a set A of events and to say that a process P is *strongly anonymous* on A if $f_A^{-1}(f_A(P)) = P$. That is, whenever an event α is possible in the renamed process $f_A(P)$, then any possible event from A should have been possible in the original process P. The strong anonymity concept was then used to model Chaum's *dining cryptographers problem* [8].

An epistemic formalization of various anonymity properties has later been pioneered in [59, 28]. The epistemic approach in [59] focuses on anonymity in security protocols. The authors show how the agent states can be augmented with information about actions performed by agents during protocol computations, and then propose an inference mechanism by which more information can be deduced. Several anonymity concepts are then proposed and discussed. The epistemic approach in [28] models anonymity in a multi-agent system framework. This is a very nice and general approach to talk about anonymity-related properties and many other papers on anonymity built on it [42, 65, 62, 14, 66].

A rather different but very interesting approach to anonymity was proposed by Hughes and Shmatikov [33]. Based on the concept of a *function view* as a concise representation of the intruder's partial knowledge about a function, a rich variety of anonymity-related properties were proposed. As it was shown in [28], Hughes and Shmatikov's approach is closely related to the epistemic approach, although function views are not expressive enough to capture all aspects of information hiding.

The *cryptographic protocol logic* (CPL) proposed in [38] came as an ambitious general framework for formalizing a very large class of security properties. While CPL seems very expressive, the model checking problem for it is undecidable and not too much about decidable fragments and proof systems for the core CPL is known.

A *trace-based property* is a property that holds for a system if it holds for individual traces (runs) of the system. Authentication for security protocols is such a property, but anonymity cannot (naturally) be defined as a trace-based property; it usually requires an *observational equivalence.* The anonymity concepts in [59] are not based on any observational equivalence.

Halpern's approach [28] in studying anonymity is a very general one, so the observational equivalence is not precisely defined. The approach in [23] uses a reinterpretation function in order to define the equivalence of two messages with respect to a given set of messages. Then, the observational equivalence is defined on runs (restrictions of runs to the actions performed by some agent): if two corresponding states are not equivalent, then the runs are not. Observational equivalence is also the main topic in [11, 13]. However, these papers focus on the relationship between a form of the observational equivalence in an applied π-calculus framework, indistinguishability, and trace equivalence.

3 Epistemic Logic

Starting from the formalism in [50], we created a new formalism in which agent states are couples of the form $s_A = (s_{A,m}, s_{A,f})$, where $s_{A,m}$ is a set of messages known by agent A in state s and $s_{A,f}$ is the set of facts recorded or deduced by A in s.

3.1 Action Analysis in a Security Protocol

Roughly speaking, a security protocol is a sequence of actions made by some agents in order to protect some exchanged data. These actions can be of the type:

- a *send action* is of the form $A!B : (M)t$;
- a *receive action* is of the form $A?B : t$.

Such a securoity protocol is the one in 1

$$\begin{array}{lcl}
A\,!\,B & : & (\{N_A, K\})\ \{A, B, H, N_A, K\}_{K_B^e} \\
B\,?\,A & : & \{A, B, H, N_A, K\}_{K_B^e} \\
B\,!\,A & : & \{N_A, B, Ticket\}_K, \{N_A, B, Ticket\}_{K_B^d} \\
A\,?\,B & : & \{N_A, B, Ticket\}_K, \{N_A, B, Ticket\}_{K_B^d} \\
A\,!\,C & : & \{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}} \\
C\,?\,A & : & \{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}} \\
C\,!\,H & : & \{\{Ticket\}_{K_{AH}}\}_{K_{CH}} \\
H\,?\,C & : & \{\{Ticket\}_{K_{AH}}\}_{K_{CH}}
\end{array}$$

Figure 1: Security protocol example

In this example, agent A wants to access a resource H which is guarded by an agent C. Agent C will grant access to any agent that posses a ticket that can be obtained from agent B. In order to obtain the ticket, agent A generates a nonce N_A and a key that will be used by agent B to securely send him the ticket. The agent B will also provide a proof that indeed he is the one that generated the ticket by signing it. In the end, the agent A uses the ticket to access H through C.

Security protocols can be analyzed in order to check if they satisfy a certain property. A property intensively studied was secrecy. To check secrecy, it is enough to analyze the messages known by the agents (especially the ones known by the intruder). To verify that a protocol satisfies the anonymity, we are interested if an observer can link the identity of an agent with the action he made (e.g. the sending or the receiving action); therefore, both messages and actions made by the agents are important and have to be considered.

We considered six types of facts that the agents can record by observing the actions executed in the security protocol. These facts are: *sent*, *rec*, *shared_key*, *gen*, *auth*, and *hop*. The facts are atomic propositions and will be used in the epistemic logic that we will define later. A detailed description and an example for each fact follows.

- *sent* facts – Each agent X who sends a message t to some agent Y records a fact $sent(X, t, Y)$. For instance, when the first action of the protocol in our example will be performed, A records $sent(A, \{A, B, H, N_A, K\}_{K_B^e}, B)$;
- *rec*-facts. According to the intruder type, two cases are to

be considered:

1. *passive intruder*. If an action $X\,?\,Y : t$ was performed by X, then X may safely record a fact $rec(X,t,Y)$ because he knows that the message he received is from Y. For instance, if the second action in our running example was performed in some computation, then B may record $rec(B,\{A,B,H,N_A,K\}_{K_B^e},A)$;
2. *active intruder*. If an action $X\,?\,Y : t$ was performed by X, then X might not be sure whether t comes from Y or from the intruder. In such a case X records a fact $rec(X,t,(Y,I))$ which shows that t may be from Y or from I. For instance, if the second action in our running example was performed in some computation, then B records the fact $rec(B,\{A,B,H,N_A,K\}_{K_B^e},(A,I))$;

- *shared_key*-facts. The fact $shared\_key(Z,X,Y,K)$ means that Z randomly generated a short-term key K to be used by X and Y as a shared-key. In our protocol, the fact $shared\_key(A,A,B,K)$ is the fact to be recorded by A when the first action of the protocol is performed. When B receives the message from A, by protocol meaning he will also be able to record the same fact;
- *gen*-facts. When an agent X encrypts a message such that only an agent Y could understand it, the agent also records a fact of the form $gen(X,m,Y)$ (m is the encrypted message). For example, $gen(A,\{A,B,H,N_A,K\}_{K_B^e},B)$ is recorded by A after the execution of the first line of the

protocol in our example;

- *auth*-facts. In the third action of the protocol, the message sent by B to A contains a sub-message of the form $\{N_A, B, Ticket\}_{K_B^d}$. This is in fact B's digital signature on the message $(N_A, B, Ticket)$.This fact will be denoted by $auth(B, (N_A, B, Ticket, \{N_A, B, Ticket\}_{K_B^d}))$ and recorded in B's state;
- *hop*-facts. The ticket obtained by A from B is passed to the service H via C. We will say that C is a *hop* between A and H with respect to the message $Ticket$, and write $hop(A, C, H, Ticket)$. This fact will be recorded by H when he receives $Ticket$ because he knows that such a ticket can reach him only via C.

Definition 1 A message t is called *decomposable* over an agent state $s = (s_m, s_f)$ if it is in one of the cases:

- $t \in \mathcal{T}_0$;
- $t = (t_1, t_2)$ for some messages t_1 and t_2;
- $t = \{t'\}_K$ for some message t' and key K with $K^{-1} \in analz(s_m)$;
- $gen(A, t, B) \in s_f$ for some honest agents A and B.

The last case in Definition 1 (“$gen(A, t, B) \in s_f$”) covers the case when A generates t for B by encrypting some message by B's public key. Agent A does not know B's corresponding private key, but knows how he built t and, from this point of view, we may say that t is decomposable.

Definition 2 The function $trace(t, s)$, where t is a message and $s = (s_m, s_f)$ is an agent state, is given by:

- $trace(t, s) = \{t\}$, if $t \in \mathcal{T}_0$;
- $trace(t, s) = \{t\} \cup trace(t_1, s) \cup trace(t_2, s)$, if $t = (t_1, t_2)$ for some terms t_1 and t_2;
- $trace(t, s) = \{t\}$, if t is not decomposable over s;
- $trace(t, s) = \{t\} \cup trace(t', s)$, if $t = \{t'\}_K$ is an encrypted but decomposable message over s.

Starting from the recorded facts, an agent can deduce more facts. For example, when an agent knows that "Agent A sent the message t to agent B.", he should also be capable to infer that "Agent A sent the message t." or that "Agent A sent a message to agent B." or simply that "Agent A sent a message." ($sent(A, t)$, $sent(A, B)$, $sent(A)$). The inference rules from the tables 1 and 2 can be used by an agent to deduce new facts from the ones he already has.

Even though agent C does not directly record a fact of the form $sent(A, ticket, C)$, by using the inference system provided, he can easily infer that the *ticket* was sent by A. In Figure 2 we present the facts that are infered by the agent C after the execution of the sixth line of the protocol in Figure 1. In Figure 2, the left hand side represents the facts that agent C can deduce in state s while the right hand side justifies how those facts are obtained (e.g. the fact $rec(C, Ticket, A)$ obtained at line seven, uses the facts from the lines five and six together with the deduction rule $R5$).

$$(S1)\ \frac{sent(A,t,B)}{sent(A,t), sent(A,B), sent(t,B)} \qquad (S2)\ \frac{sent(A,B)}{sent(A)}$$

$$(S3)\ \frac{sent(A,t)}{sent(A), sent(t)} \qquad (S4)\ \frac{sent(t,B)}{sent(t)}$$

$$(S5)\ \frac{sent(A,t,B),\ t' \in trace(t,s)}{sent(A,t',B)}$$

$$(R1)\ \frac{rec(A,t,x)}{rec(A,t), rec(A,x), rec(t,x)} \qquad (R2)\ \frac{rec(A,x)}{rec(A)}$$

$$(R3)\ \frac{rec(A,t)}{rec(A), rec(t)} \qquad (R4)\ \frac{rec(t,x)}{rec(t)}$$

$$(R5)\ \frac{rec(A,t,x),\ t' \in trace(t,s)}{rec(A,t',x)}$$

Table 1: Deduction rules (1)

$$(RG)_A \ \frac{rec(A,\{t\}_{K_{AB}}),\ \neg gen(A,\{t\}_{K_{AB}},B)}{gen(B,\{t\}_{K_{AB}},A)} \qquad (RA) \ \frac{rec(t,\{t\}_{K_A^d})}{auth(A,(t,\{t\}_{K_A^d}))}$$

$$(RG')_A \ \frac{rec(A,\{t\}_K),\ shared\_key(C,A,B,K),\ \neg gen(A,\{t\}_K,B)}{gen(B,\{t\}_K,A)}$$

$$(RS) \ \frac{rec(A,t,B)}{sent(B,t,A)} \qquad (RGS) \ \frac{rec(A,t),\ gen(B,t,A)}{sent(B,t,A)}$$

$$(RAS) \ \frac{rec(t),\ auth(A,t)}{sent(A,t)} \qquad (SGS) \ \frac{sent(A,t),\ gen(A,t,B)}{sent(A,t,B)}$$

$$(RGR) \quad \frac{rec(A,t,(B,I)),\ gen(B,t,A)}{rec(A,t,B)}$$

$$(RShR) \quad \frac{rec(A,\{t\}_K),\ shared\_key(C,A,B,K),\ \neg gen(A,\{t\}_K,B)}{rec(B,K,C)}$$

$$(SGR) \quad \frac{sent(A,t,B),\ gen(C,t,B), hop(C,A,B,t)}{rec(A,t,C)}$$

$$(RGHS) \ \frac{rec(B,t,A),\ gen(C,t,B),\ hop(C,A,B,t)}{sent(C,t,A)}$$

Table 2: Deduction rules (2)

1.	$rec(C, \{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}}, (A, I))$	$\in s_C$
2.	$\neg gen(C, \{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}}, A)$	$\in s_C$
3.	$rec(C, \{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}})$	$1,\ S1$
4.	$gen(A, \{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}}, C)$	$3, 2,\ RG$
5.	$rec(C, \{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}}, A)$	$1, 4,\ RGR$
6.	$Ticket \in trace(\{Ticket, \{Ticket\}_{K_{AH}}\}_{K_{AC}})$	$\in s_C$
7.	$rec(C, Ticket, A)$	$5, 6,\ R5$
8.	$sent(A, Ticket, C)$	$7,\ RS$

Figure 2: Deduction example

3.2 Observational Equivalence

Anonymity, and other similar properties, are crucially based on what agents are able to "observe". If two distinct messages can be decomposed into the same atomic messages or both are encrypted by keys the agent A does not know, then the two messages are "*observationally equivalent*" from A's point of view in the sense that none of them reveals more "meaningful information" to A than the other. This can be extended to facts and agent states as follows.

Definition 3 Given a pair of agent states (s, s') define the binary relation $\sim_{s,s'}$ on message terms by:

- $t \sim_{s,s'} t$, for any $t \in \mathcal{T}_0$;
- $t \sim_{s,s'} t'$, for any term t undecomposable over s and any term t' undecomposable over s';
- $(t_1, t_2) \sim_{s,s'} (t'_1, t'_2)$, for any terms t_1, t_2, t'_1, and t'_2 with $t_1 \sim_{s,s'} t'_1$ and $t_2 \sim_{s,s'} t'_2$;
- $\{t\}_K \sim_{s,s'} \{t'\}_K$, for any terms t and t' and any key K with $t \sim_{s,s'} t'$ and $K^{-1} \in analz(s_m) \cap analz(s'_m)$.

Component-wise extend the relation $\sim_{s,s'}$ to facts:

$$P(t_1, \ldots, t_i) \sim_{s,s'} P(t'_1, \ldots, t'_i) \quad \Leftrightarrow \quad (\forall 1 \leq j \leq i)(t_j \sim_{s,s'} t'_j).$$

Definition 4 Two agent states $s = (s_m, s_f)$ and $s' = (s'_m, s'_f)$ are *observationally equivalent*, denoted $s \sim s'$, if the following hold:

- $analz(s_m) \cap \mathcal{T}_0 = analz(s'_m) \cap \mathcal{T}_0$;
- for any $\varphi \in Analz(s)$ there is $\varphi' \in Analz(s')$ such that $\varphi \sim_{s,s'} \varphi'$;
- for any $\varphi' \in Analz(s')$ there is $\varphi \in Analz(s)$ such that $\varphi' \sim_{s',s} \varphi$.

Let us consider that $s = (s_m, s_f)$ and $s' = (s'_m, s'_f)$ are two agent states, where $s_m = \{\{N_C\}_K\}$, $s_f = \{rec(A, \{N_C\}_K, B)\}$, $s'_m = \{\{C, N_C\}_K\}$, $s'_f = \{rec(A, \{C, N_C\}_K, B)\}$, and K is a symmetric key. According to Definition 4, s and s' are observationally equivalent. If we replace s_m above by $\{\{N_C\}_K, C, K\}$ and s'_m by $\{\{C, N_C\}_K, K\}$, then s and s' are not anymore observationally equivalent because from $rec(A, \{C, N_C\}_K, B)$ and

s'_m one can infer $rec(A, C, B)$, and this fact cannot be inferred from $rec(A, \{N_C\}_K, B)$ and s_m.

Proposition 5 The observational equivalence on agent states is an equivalence relation decidable in $\mathcal{O}(f^4 l^4)$ time complexity, where f is the maximum number of facts in the states, and l is the maximum length of the messages in the states.

3.3 Epistemic Logic and its Semantics in Security Protocols

The epistemic logic we use is only a fragment of classical epistemic logic in the sense that it does not allow the imbrication of knowledge operators.

Definition 6 The syntax of the epistemic logic is given by the formulas of type ψ defined as below:

$$\varphi ::= p \,|\, \varphi \wedge \varphi \,|\, \neg\varphi$$

$$\psi ::= \varphi \,|\, \psi \wedge \psi \,|\, \neg\psi \,|\, \mathtt{K}_A\varphi \,|\, \mathtt{E}_G\varphi \,|\, \mathtt{D}_G\varphi$$

where p ranges over a countable set Φ of atomic propositions, A ranges over a non-empty finite set $\mathcal{A}$ of agent names, and G ranges over non-empty subsets of $\mathcal{A}$.

As usual we use $\mathtt{P}_A\varphi$ as an abbreviation for $\neg\mathtt{K}_A\neg\varphi$.

Definition 7 Let $\mathcal{P}$ be a security protocol. The *truth value of a formula φ in $\mathcal{P}$* is defined inductively as follows:

- $\mathcal{P} \models \varphi$ iff $(\mathcal{P}, s) \models \varphi$, for any reachable state s in $\mathcal{P}$;
- $(\mathcal{P}, s) \models \varphi$ iff $(\mathcal{P}, s_A) \models \varphi$, for some agent $A \in \mathcal{A} - \{I\}$;
- $(\mathcal{P}, s) \models \neg\varphi$ iff $(\mathcal{P}, s) \not\models \varphi$;
- $(\mathcal{P}, s) \models \varphi \wedge \psi$ iff $(\mathcal{P}, s) \models \varphi$ and $(\mathcal{P}, s) \models \psi$;
- $(\mathcal{P}, s) \models \mathtt{K}_A\varphi$ iff $(\mathcal{P}, s'_A) \models \varphi$, for any reachable state s' with $s' \sim^A s$;
- $(\mathcal{P}, s) \models \mathtt{E}_G\varphi$ iff $(\mathcal{P}, s) \models \mathtt{K}_A\varphi$, for any $A \in G$;
- $(\mathcal{P}, s) \models \mathtt{D}_G\varphi$ iff $(\mathcal{P}, s'_G) \models \varphi$ for any reachable state s' with $s' \sim^G s$, where $\sim^G = \cap_{A\in G} \sim^A$ and $s'_G = \cup_{A\in G} s'_A$.

Definition 8 For any formula φ which does not contain any knowledge operators, and for any agent $A \in \mathcal{A}$, $(\mathcal{P}, s_A) \models \varphi$ is defined as:

- if $\varphi = p$ then $(\mathcal{P}, s_A) \models \varphi$ iff $p \in \mathit{Analz}(s_A)$;
- if $\varphi = \varphi_1 \wedge \varphi_2$ then $(\mathcal{P}, s_A) \models \varphi$ iff $(\mathcal{P}, s_A) \models \varphi_1$ and $(\mathcal{P}, s_A) \models \varphi_2$;
- if $\varphi = \neg\varphi_1$ then $(\mathcal{P}, s_A) \models \varphi$ iff $(\mathcal{P}, s_A) \not\models \varphi_1$.

The formula $\mathtt{K}_A\varphi$ means "agent A knows φ". It holds in a reachable state s iff φ holds in s and in any other reachable state that is observationally equivalent to s with respect to A.

The formula $\mathtt{E}_G\varphi$ stands for "all agents in group G know φ" and it holds in a reachable state s of the protocol if each agent $A \in G$ knows φ.

The formula $\mathtt{D}_G\varphi$ means "φ is a distributed knowledge among agents in G". It holds in a state s of the protocol iff it can be inferred from the knowledge the agents in G have in state s and it has to be true in each state equivalent to s that every agent from the D-coalition consider possible.

4 Minimal and Group Anonymity

In the fourth chapter of the thesis we formalized two types of anonymity: minimal anonymity and group anonymity. Variations of these concepts (like *unlinkability*, *role interchangeability*) and also relationships between the anonymity concepts formalized were presented in the thesis. In this summary we will only present minimal and group anonymity and the relations that can be established for different types of actions and various observer models. The reason for which we studied anonymity from two perspectives: when the protocol is executed in an environment where the intruder is active and passive respectively is motivated by one of the theorems that will follow.

4.1 Minimal Anonymity

Intuitively, minimal anonymity means that an action made by an agent is not seen by the observer. This might be because the observer has partial view and the agent is not in his view set or because the observer is not able to deduce that the action happened.

Definition 9 Let $\mathcal{P}$ be a security protocol, X an observer,

An action *act* of $\mathcal{P}$ is *minimally anonymous w.r.t.* X if the following property holds:

$$\mathcal{P} \models act \Rightarrow \neg \mathtt{K}_X act.$$

Minimal anonymity of *act* w.r.t. an observer X in $\mathcal{P}$ means that, whenever *act* has occurred at some state $s \in Reach(\mathcal{P})$, then there exists a state $s' \in \mathit{Reach}(\mathcal{P})$ such that $s' \sim^X s$ and X is not able to infer *act* in s'_X. We abbreviate the formula "$\mathit{act} \Rightarrow \neg \mathtt{K}_X \mathit{act}$" by $\varphi(\mathit{act}, X)$.

As an example, the action $\mathit{sent}(B, \mathit{Ticket}, A)$ is minimally anonymous w.r.t. C in the protocol in Figure 1. This is because, whenever this action is performed, C is not able to deduce it from his knowledge.

An active intruder might change the anonymity status of an action in a protocol; we prove that in the following theorem.

Theorem 10

1. There are protocols $\mathcal{P}$, actions *act*, and observers X such that *act* is minimally anonymous w.r.t. X in $\mathcal{P}$ under a passive intruder, but *act* is not minimally anonymous w.r.t. X in $\mathcal{P}$ under an active intruder.

2. There are protocols $\mathcal{P}$, actions *act*, and observers X such that *act* is minimally anonymous w.r.t. X in $\mathcal{P}$ under an active intruder, but *act* is not minimally anonymous w.r.t. X in $\mathcal{P}$ under a passive intruder.

3. For any protocol $\mathcal{P}$, basic-term action *act*, and observer X, if *act* is minimally anonymous w.r.t. X in $\mathcal{P}$ under an active intruder, then *act* is minimally anonymous w.r.t. X in $\mathcal{P}$ under a passive intruder.

The proof of this theorem is based on finding some particular security protocols and some specific attacks that can be performed by an active intruder and those attacks have the role of modifying the anonymity status of a certain action. The case in which the action is built only using basic terms has to be treated differently because if such a fact exists in a state s and s is observational equivalent with s' from some agent's perspective, then s' also has to satisfy the basic term action (this is due to the way observational equivalence relation over facts is built). The proof of the third part of the theorem is based on the fact that an active intruder might choose to behave as a passive one.

4.2 Group Anonymity

Intuitively, an action is anonymous in a group of agents if, after the run is finished, the observer can see the action as being done by each agent from that group. Formally, de group anonymity is defined as it follows.

Definition 11 Let $\mathcal{P}$ be a security protocol, X an observer, and G a nonempty set of agents with $G \cap (\mathcal{X}_1 \cup \mathcal{X}_2 \cup \{X, I\}) = \emptyset$.

A mono-agent action $act(A)$ of $\mathcal{P}$ is *anonymous within G w.r.t. X* if $\mathcal{P} \models \psi(act(A), G, X)$, where

$$\psi(act(A), G, X) = (\mathtt{P}_X act(A) \Rightarrow \bigwedge_{C \in G} \mathtt{P}_X act(C)).$$

($act(C)$ is obtained from $act(A)$ by replacing A by C).

Anonymity of $act(A)$ within G w.r.t. an observer X means that, whenever $act(A)$ has occurred at some state s then, for any $C \in G$, there exists a state s' such that $s' \sim^X s$ and X can infer $act(C)$ in s'_X (in other words, X thinks that any $C \in G$ might have been performed act).

In order to exemplify the group anonymity, consider the protocol $\mathcal{P}$ in Figure 3.

The fact $sent(A,t)$ is anonymous in the group $\{A,B\}$ from S's point of view. The agent S is not able to deduce if the message t comes from agent A. That is because this message is encrypted with a key known by both agents A and B. Because any of these agents is able to encrypt the message t with the key K, and because the messages can reach S only via H who does not share information about the origin of the message, after the last line of the protocol had been executed, agent S will be able to deduce both $sent(A,t)$ and $sent(B,t)$.

$$\begin{array}{lcl}
S\,!\,A & : & (\{K\})\{K,H\}_{K_{SA}} \\
A\,?\,S & : & \{K,H\}_{K_{SA}} \\
S\,!\,B & : & \{K,H\}_{K_{SB}} \\
B\,?\,S & : & \{K,H\}_{K_{SB}} \\
A\,!\,H & : & \{\{t\}_K,S\}_{K_{AH}} \\
H\,?\,A & : & \{\{t\}_K,S\}_{K_{AH}} \\
B\,!\,H & : & \{\{t'\}_K,S\}_{K_{BH}} \\
H\,?\,B & : & \{\{t'\}_K,S\}_{K_{BH}} \\
H\,!\,S & : & \{\{t\}_K,\{t'\}_K\}_{K_{SH}} \\
S\,?\,H & : & \{\{t\}_K,\{t'\}_K\}_{K_{SH}}
\end{array}$$

Figure 3: Security protocol for exemplifying group anonymity

A similar result as in the case of the minimal anonymity was proved also for group anonymity:

Theorem 12

1. There are protocols $\mathcal{P}$, actions $act(x)$, groups G of agents or message terms, and observers X such that $act(x)$ is anonymous within G w.r.t. X in $\mathcal{P}$ under a passive intruder, but $act(x)$ is not anonymous within G w.r.t. X in $\mathcal{P}$ under an active intruder.
2. There are protocols $\mathcal{P}$, actions $act(x)$, groups G of agents or message terms, and observers X such that $act(x)$ is anonymous within G w.r.t. X in $\mathcal{P}$ under an active intruder, but $act(x)$ is not anonymous within G w.r.t. X in $\mathcal{P}$ under a passive intruder.
3. For any protocol $\mathcal{P}$, basic-term action $act(x)$, group G of agents or basic terms, and observer X, if $act(x)$ is anonymous within G w.r.t. X in $\mathcal{P}$ under an active intruder, then $act(x)$ is anonymous within G w.r.t. X in $\mathcal{P}$ under a passive intruder.

The proof idea is based on finding specific security protocols examples and attacks that can modify their anonymity status.

4.3 Relationships Between Various Anonymity Concepts

The analysis of different anonymity concepts defined earlier has conduct to various relationships when the anonymity is formulated with respect to observers who have different network monitoring capabilities. Felations between anonymity of different action types were obtained.

Observers can have different network monitoring capabilities. From this point of view, we will denote with H an honest agent that can only observe the actions in which he is directly involved, with H_{tv} (*total view*) an agent that can observe all the actions in the system, with H_{pv} (*partial view*) an observer that can monitor only a fixed subset of agents and with H_m (*mobility*) an agent that can monitor a dynamic subset of agents (the monitored agent set can be changed in each system state).

Proposition 13 Let $\mathcal{P}$ be a security protocol.

1. The implications in the diagram in Figure 4 hold for any basic-term action *act* and any honest agent H (an arrow means a logical implication; if two nodes are unrelated, then the corresponding formulas are incomparable with respect to the logical implication).

$$\begin{tikzcd}
 & \varphi(act, H_{pv}) \arrow[dr] & \\
\varphi(act, H_{tv}) \arrow[ur] \arrow[dr] & & \varphi(act, H) \\
 & \varphi(act, H_m) \arrow[ur] &
\end{tikzcd}$$

Figure 4: Minimal anonymity w.r.t. observers with different views

2. For any coalition $\mathcal{X}$ of observers and any agent $X \in \mathcal{X}$, if $\varphi_D(act, \mathcal{X})$ holds in $\mathcal{P}$, then $\varphi(act, X)$ holds in $\mathcal{P}$.

The proof idea is based on the fact that if an action *act* is minimal anonymous w.r.t. an agent that can monitor the entire network, then if we reduce its view, he will definitely not be able to deduce *act*. Because the mobility agent can monitor a different set of agents then the partial view agent, the anonymity from their point of view is incomparable.

Proposition 14 An action $sent(A)$ ($rec(A)$) is minimally anonymous w.r.t. an observer X with a total view in a protocol $\mathcal{P}$ if and only if A does not perform any send (receive) action in any run of $\mathcal{P}$.

The action $sent(A)$ contains only basic terms. If this action would be in the observer's state then all the other observational equivalent states have also to contain it which means that the observer knows $sent(A)$. Because the intruder can also monitor the entire network, the previous proposition also holds for him.

Theorem 15 The implications in the diagram in Figure 5 hold in the same protocol, where $act \in \{sent, rec\}$ and X is an observer (an arrow means a logical implication; if two nodes are unrelated, then the corresponding formulas are incomparable with respect to the logical implication).

The proof idea (for $\varphi(sent(A), X) \ \Rightarrow \varphi(sent(A, B), X)$) is that if the action $act(A, B)$ would not be anonymous form X's point of view than he could deduce that A sent something and then $\varphi(sent(A), X)$ will not hold.

The same direction in obtaining relations was followed for group anonymity. To study group anonymity for various types

$$\begin{tikzcd}
\varphi(act(A), X) \arrow[rr] \arrow[dr] & & \varphi(act(A, B), X) \arrow[dr] & \\
& \varphi(act(A, t), X) \arrow[rr] & & \varphi(act(A, t, B), X) \\
\varphi(act(t), X) \arrow[rr] \arrow[ur] & & \varphi(act(t, B), X) \arrow[ur] &
\end{tikzcd}$$

Figure 5: Relationships between minimal anonymity concepts

of observers, the concept of *outside identifiable* has to be defined. Roughly speaking, *act* is outside X identifiable if X cannot observe *act* without *act* being observed by other agents.

Definition 16 Let $\mathcal{P}$ be a security protocol, X and observer, and *act* an action. We say that *act* is *outside X identifiable* if, for any reachable state s of the protocol, the following property holds:

$$s \models act \quad \Rightarrow \quad (\exists A \neq X)(s_A \models act).$$

Proposition 17 Let $\mathcal{P}$ be a security protocol.

1. The implications in the diagram in Figure 6 hold for any honest agent H and basic-term action *act* outside H identifiable (an arrow means a logical implication; if two nodes are unrelated, then the corresponding formulas are incomparable with respect to the logical implication).

2. If $\psi(act, G, X)$ holds in $\mathcal{P}$ for some $X \in \mathcal{X}$, where $\mathcal{X}$ is an E-coalition, then $\psi_E(act, G, \mathcal{X})$ holds in $\mathcal{P}$.

$$\begin{tikzcd}
 & \psi(act, G, H_{pv}) \arrow[dr] & \\
\psi(act, G, H) \arrow[ur] \arrow[dr] & & \psi(act, G, H_{tv}) \\
 & \psi(act, G, H_m) \arrow[ur] &
\end{tikzcd}$$

Figure 6: Group anonymity w.r.t. observers with different views

Let us consider an honest agent A who can only observe the actions in which he is directly involved and suppose that the action act is anonymous in a group G w.r.t. A. If we allow A to monitor some other agents then, for sure he will see more actions but he will still be able to see that the agents in G have performed the action. Therefore, giving more view power to an agent will maintain group anonymity for an action act. From this reason we can say that $\psi(act(A), G, H) \rightarrow \psi(act(A), G, H_{pv})$ holds. The proofs for the other implications are similar.

Theorem 18 The implications in the Figure 7 hold for the same security protocol $\mathcal{P}$ (G is a set of agents, T is a set of messages and X is an observer).

Assume that $\mathcal{P} \models \bigwedge_{B \in \mathcal{A} - \{A, I\}} \psi(sent(A, t, B), G, X)$ and let s be a reachable state of the protocol such that $s \models sent(A, t)$. Then, it must exists an honest agent B such that $s \models sent(A, t, B)$ (an agent can infer $sent(A, t)$ from a fact $sent(A, t, B)$ for some agent B, or by using the deduction rule (RAS). In the second case, $sent(A, t, B)$ must be in A's state, for some agent B).

$$\begin{tikzcd}
 & \psi(sent(A,B),G,X) \arrow[dr, "\forall B"] & \\
\psi(sent(A,t,B),G,X) \arrow[ur, "\forall t"] \arrow[dr, "\forall B"'] & & \psi(sent(A),G,X) \\
 & \psi(sent(A,t),G,X) \arrow[ur, "\forall t"'] &
\end{tikzcd}$$

$$\psi(sent(t,B),G',X) \xrightarrow{\forall B} \psi(sent(t),G',X)$$

Figure 7: Relationships between group anonymity concepts

According to the hypothesis, for any agent $C \in G$ there exists a reachable state s' such that $s' \sim^X s$ and $s'_X \models sent(C,t,B)$. But then, $s'_X \models sent(C,t)$, showing that $\mathcal{P} \models \psi(sent(A,t),G,X)$.

The other implication can be proved in the same manner.

Using a multi-agent framework, it has been shown in [28] that the anonymity of an action a performed by an agent i within G and w.r.t. an agent j implies the minimal anonymity of a w.r.t. j, whenever a is an *exclusive action* and $|G| \geq 3$. The exclusiveness of an action means that no two different agents can perform the action.

This result holds true in our setting for security protocols.

Definition 19 Let $\mathcal{P}$ be a security protocol and A an honest agent.

1. An action $act(A)$ performed by A is *globally exclusive* if $s \models \neg(act(A) \wedge act(A'))$, for any reachable state s of $\mathcal{P}$ and any honest agent $A' \neq A$.

2. An action $act(A)$ performed by A is *locally exclusive* if $s_B \models \neg(act(A) \wedge act(A'))$, for any reachable state s of $\mathcal{P}$, any honest agent B, and any honest agent $A' \neq A$.

Clearly, global exclusiveness implies local exclusiveness.

Proposition 20 If a locally exclusive action $act(A)$ of a security protocol $\mathcal{P}$ is anonymous within G w.r.t. an honest agent H and $|G| \geq 3$, then $act(A)$ is minimally anonymous w.r.t. H.

5 Decidability Results

In this chapter we establish several undecidability results for the anonymity concepts defined so far. The proofs are based on the halting problem for counter machines and various reduction techniques.

For easier expressing the results we obtained, we defined a type τ for each action.

Each action has a *type* which is a tuple. For instance, the action $sent(A, t, B)$ has the type (s, a, m, a), where s stands for "*sent*", a for "agent", and m for "message". Similarly, $sent(t, B)$ has type (s, m, a), $rec(A, t)$ has type (r, a, m), where r stands for "*rec*", and so on.

Minimal anonymity decision problems are denoted by MAP, the group anonymity decision problems are denoted by GAP. The observer type is specified as an index.

Theorem 21 The problems $MAP(\tau)$, $MAP_{pv}(\tau)$, $MAP_m(\tau)$, $MAP_{tv}(\tau)$, $MAP_D(\tau)$, and $MAP_E(\tau)$ are undecidable for unrestricted security protocols for any type of action τ.

Theorem 22 The problem $MAP_I(\tau)$ is undecidable for unrestricted security protocols for any type of action τ except the actions of the type (r, a, a), (r, m, a), and (r, a, m, a).

Theorem 23 The problems $GAP(\tau)$, $GAP_{pv}(\tau)$, $GAP_m(\tau)$, $GAP_{tv}(\tau)$, $GAP_D(\tau)$ and $GAP_E(\tau)$ are undecidable for unrestricted security protocols for any type of action τ.

Theorem 24 The problem $GAP_I(\tau)$ is undecidable for unrestricted security protocols for any type of action τ except the actions of the type (r, a, a), (r, m, a), and (r, a, m, a).

Theorem 25 Role interchangeability problem is undecidable for unrestricted security protocols for any type of action τ

To prove these theorems, the halt problem for counter machines is reduced to the complement of each of the problems in the theorems (using a similar tehnique as the one in [61]). Because counter machines are equivalent to Turing machines we can conclude that the analyzed problems are indeed undecidable.

6 Complexity Results

Let $\mathcal{P}$ be a security protocol, $T \subseteq \mathcal{T}_0$ a finite set of basic terms, and $k \geq 1$. A *(T, k)-run* of $\mathcal{P}$ is any run with the property that all terms in the run are built up upon T and all messages communicated in the course of the run have length at most k. When for $\mathcal{P}$ only (T, k)-runs are considered we will say that it is a *security protocol under (T, k)-runs* or a *(T, k)-bounded security protocol*, and denote this by $(\mathcal{P}, T, k)$. A *bounded security protocol* is a (T, k)-bounded protocol, for some finite set $T \subseteq \mathcal{T}_0$ and $k \geq 1$.

A *1-session bounded security protocol* is a (T, k)-bounded protocol obtained by applying each role at most once

Restricting security protocols in this manner, MAP and GAP problems are decidable and we can study their complexity.

Theorem 26 $MAP(\tau)$ and $MAP_I(\tau)$ are in $NEXPTIME$ for any τ if they are restricted to basic-term actions of type τ and bounded security protocols. Moreover, except for $MAP_I(r, a, a)$, $MAP_I(r, m, a)$, and $MAP_I(r, a, m, a)$, all the other minimal anonymity problems restricted as above are complete for $NEXPTIME$.

The proof of this theorem is based on the results in [61] where it was shown that the number of distinct events in a (T, k)-run of a security protocol $\mathcal{P}$ is exponential w.r.t. the length of the protocol. The fact that the problems are complete for $NEXPTIME$ was proved by reducing a language in $NEXPTIME$ to the complement of each problem (same idea as in [61]).

Theorem 27 $MAP(\tau)$ and $MAP_I(\tau)$ are in NP for any τ if they are restricted to basic-term actions of type τ and 1-session bounded security protocols. Moreover, except for $MAP_I(r, a, a)$, $MAP_I(r, m, a)$, and $MAP_I(r, a, m, a)$, all the other minimal anonymity problems restricted as above are complete for NP.

The completeness was shown by using a reduction from 3–SAT.

Similar results were obtained for group anonymity:

Theorem 28 $GAP(\tau)$ and $GAP_I(\tau)$ are in $NEXPTIME$ for any τ if they are restricted to basic-term actions of type τ and bounded security protocols. Moreover, except for $GAP_I(\tau)$ where τ is a rec-action type, all the other group anonymity problems restricted as above are complete for $NEXPTIME$.

Theorem 29 $GAP(\tau)$ and $GAP_I(\tau)$ are in NP for any τ if they are restricted to basic-term actions of type τ and 1-session bounded security protocols. Moreover, except for $GAP_I(\tau)$ where τ is a rec-action type, all the other group anonymity problems restricted as above are complete for NP.

The proofs for these theorems followed a similar line as the ones for minimal anonymity.

7 Conclusions and Future Work

In this thesis we presented a formalism based on a fragment of epistemic logic that can be used to reason about security protocols properties. The observational equivalence that is the basis of any epistemic logic was built to manage both the messages sent by the agents and the actions they do. We enriched the formalism in [49] by adding facts (representing agent actions) and we create an inference system that can be used by the agents to reason about the knowledge they have.

Anonymity can be formulated with respect to various types of observers. We have considered honest agents that only see the actions they are involved in, honest agents with partial or total view, agents that can change their view set (mobility), groups of agents (`E` and `D` groups), and the intruder as an observer. The intruder we considered is an active one. By our knowledge this is the first time an active intruder is taken into consideration when checking anonymity related properties. Our approach is justified in Chapter **??** where it was shown that an active intruder can break or add anonymity to a protocol.

Two types of anonymity were studied: minimal and group anonymity. Variants of these were also presented (unlinkability and role interchangeability). Anonymity of basic-term actions was analyzed and various properties of the minimal and group anonymity for these type of actions were presented. Relationships between anonymity under different types of observers were proved. Implications between the anonymity of different types of facts were also shown.

Decidability and complexity results were obtained for the problems induced by the anonymity types we studied. We proved that both minimal anonymity and group anonymity problems are undecidable for unbounded security protocols by simulating counter machines with security protocols. The decidability problems for both minimal anonymity and group anonymity for receive actions in an active intruder environment still remain opened.

For bounded security protocols, the anonymity problems become decidable and their complexity can be studied. It was shown that, for basic-term actions and bounded security protocols, all the problems induced by the minimal and group anonymity are in $NEXPTIME$. Moreover, except the anonymity cases for a receive action in an active intruder environment, all the problems are complete for $NEXPTIME$. If 1-session bounded security protocols are considered, the anonymity problems are in NP (and complete for NP if the actions are not the receiving actions in an active intruder environment).

As it was shown in [48, 28, 57, 46], anonymity property for security protocols can be treated in a probabilistic manner. Formalising and reasoning about the probabilities in anonymity might be an interesting starting point for further research.

The inference system we provided for the agent to reason about the knowledge was not proved to be sound nor complete. This is due to the fact that security protocol do not have a clear semantics attached. Further studies about security protocol semantics are also very appealing.

The formalism we used is limited in some cases: for example, it is not able to express protocols were the receiver is not fixed (such as Mix Nets protocols). This is due to the fact that messages are considered only at a syntactic level and no semantics is added. However, we are confident that the formalism we use can be improved to reason about protocols like Mix nets protocols.

References

[1] Federal information processing standards publication (FIPS 46). Data Encryption Standard (DES), 1991.

[2] Federal information processing standards publication (FIPS 197). Advanced Encryption Standard (AES). http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf, 2001.

[3] M. Abadi and A. D. Gordon. A calculus for cryptographic protocols: the spi calculus. In *Proceedings of the 4th ACM conference on Computer and communications security*, CCS '97, pages 36–47, 1997.

[4] J. Brickell and V. Shmatikov. Privacy-preserving graph algorithms in the semi-honest model. In *Proceedings of the 11th international conference on Theory and Application of Cryptology and Information Security*, ASIACRYPT'05, pages 236–252. Springer-Verlag, 2005.

[5] M. Burrows, M. Abadi, and R. Needham. A logic of authentication. *ACM Trans. Comput. Syst.*, 8(1):18–36, Feb. 1990.

[6] D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, 24(2):84–88, Feb 1981.

[7] D. Chaum. Security without identification: Transaction systems to make big brother obsolete. *Communications of the ACM*, 28(10):1030–1044, Oct 1985.

[8] D. Chaum. The dining cryptographers problem: Unconditional sender untraceability. *Journal of Cryptology*, 1(1):65–76, 1988.

[9] T. Chothia, S. Orzan, J. Pang, and M. T. Dashti. A framework for automatically checking anonymity with μcrl. In *In Proceedings TGC06, LNCS*, pages 301–318, 2007.

[10] V. Ciriani, S. De Capitani di Vimercati, S. Foresti, and P. Samarati. k-Anonymity. In T. Yu and S. Jajodia, editors, *Secure Data Management in Decentralized Systems.* Springer-Verlag, 2007.

[11] H. Comon-Lundh and V. Cortier. Computational soundness of observational equivalence. In *Proc. of the 15th ACM Conference on Computer and Communications Security 2008*, pages 109–118, 2008.

[12] H. Comon-Lundh, Y. Kawamoto, and H. Sakurada. Computational and symbolic anonymity in an unbounded network. *JSIAM Letters*, 1:28–31, 2009.

[13] V. Cortier and S. Delaune. A method for proving observational equivalence. In *CSF '09*, pages 266–276, 2009.

[14] S. Delaune, S. Kremer, and M. Ryan. Verifying privacy-type properties of electronic voting protocols. *J. Comput. Secur.*, 17(4):435–487, 2009.

[15] W. Diffie and M. Hellman. New directions in cryptography. *Information Theory, IEEE Transactions on*, 22(6):644 – 654, nov 1976.

[16] R. Dingledine, N. Mathewson, and P. Syverson. Tor: The second-generation onion router. *In 13th USENIX Security Symposium*, 2004.

[17] D. Dolev and A. Yao. On the security of public-key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[18] M. Edman and B. Yener. On anonymity in an electronic society: A survey of anonymous communication systems. *ACM Computing Surveys*, 42(1), 2009.

[19] T. El Gamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proceedings of CRYPTO 84 on Advances in cryptology*, pages 10–18. Springer-Verlag New York, Inc., 1985.

[20] F. J. T. Fabrega, F. Javier, J. C. Herzog, and J. D. Guttman. Strand spaces: Proving security protocols correct, 1999.

[21] R. Fagin, J. Y. Halpern, Y. Moses, and M. Y. Vardi. *Reasoning About Knowledge.* The MIT Press, 2003.

[22] P. C. Fischer, A. R. Meyer, and A. L. Rosenberg. Counter machines and counter languages. *Mathematical System Theory*, 2(3):265–283, 1968.

[23] F. D. Garcia, I. Hasuo, W. Pieters, and P. van Rossum. Provable anonymity. In *Proceedings of the 2005 ACM Workshop on Formal Methods in Security Engineering (FMSE'05)*, pages 63–72, 2005.

[24] S. Goel, M. Robson, M. Polte, and E.G.Sirer. Herbivore: A scalable and efficient protocol for anonymous communication. http://www.cs.cornell.edu/people/egs/papers/herbivore-tr.pdf, 2002. Manuscript.

[25] P. Golle and A. Juels. Dining cryptographers revisited. In *EUROCRYPT*, pages 456–473, 2004.

[26] S. A. Greibach. Remarks on blind and partially blind one-way multicounter machines. *Theoretical Computer Science*, 7(3):311–324, Dec 1978.

[27] J. Halpern and K. O'Neill. Secrecy in multiagent systems. *Proceedings 15th IEEE Computer Security Foundations Workshop. CSFW-15*, V:32–46, 2002.

[28] J. Y. Halpern and K. R. O'Neill. Anonymity and information hiding in multi-agent systems. *Journal of Computer Security*, 13(3):483–514, 2005.

[29] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409 (Proposed Standard), Nov. 1998. Obsoleted by RFC 4306, updated by RFC 4109.

[30] T. Harreveld. Dining Cryptographer Networks. *Computingscience.nl*, (June):1–5, 2012.

[31] C. A. R. Hoare. Communicating sequential processes. http://www.usingcsp.com/cspbook.pdf, 2004.

[32] J. Hoffstein, J. Pipher, and J. H. Silverman. Ntru: A ring-based public key cryptosystem. In *Lecture Notes in Computer Science*, pages 267–288. Springer-Verlag, 1998.

[33] D. Hughes and V. Shmatikov. Information hiding, anonymity and privacy: A modular approach. *Journal of Computer Security*, 12:3–36, Jan 2004.

[34] M. Huth and M. Ryan. *Logic in Computer Science: Modelling and Reasoning about Systems.* Cambridge University Press, New York, NY, USA, 2004.

[35] N. institute of standards and technology. FIPS 180-4, Secure Hash Standard, Federal Information Processing Standard (FIPS), Publication 180-4. Technical report, Department of Commerce, Feb. 2011.

[36] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. RFC 4306 (Proposed Standard), Dec. 2005. Obsoleted by RFC 5996, updated by RFC 5282.

[37] L. Kissner, A. Oprea, M. Reiter, D. Song, and K. Yang. Private keyword-based push and pull with applications to anonymous communication, 2004.

[38] S. Kramer. Cryptographic protocol logic: Satisfaction for (timed) dolev-yao cryptography. *The Journal of Logic and Algebraic Programming*, 77:60–91, Sep 2008.

[39] G. Lowe. An attack on the needham-schroeder public-key authentication protocol. *Information Processing Letters*, 56(3):131–133, Nov. 1995.

[40] G. Lowe. Breaking and fixing the needham-schroeder public-key protocol using fdr. In *Proceedings of the Second International Workshop on Tools and Algorithms for Construction and Analysis of Systems*, TACAs '96, pages 147–166, 1996.

[41] G. Lowe and B. Roscoe. Using CSP to detect errors in the TMN protocol. *Software Engineering, IEEE Transactions on*, 23(10):659–669, 1997.

[42] K. Mano, Y. Kawabe, H. Sakurada, and Y. Tsukada. Role interchangebility and verification of electronic voting. In *The 2006 Symposium on Cryptography and Information Security*, Hiroshima, Japan, Jan 2006.

[43] M. L. Minsky. Recursvive unsolvability of post's problem of "tag" and other topics in theory of turing machines. *Annals of Mathematics*, 74(3):437–455, 1961.

[44] R. M. Needham and M. D. Schroeder. Using encryption for authentication in large networks of computers. *Commun. ACM*, 21(12):993–999, Dec. 1978.

[45] L. E. Olson, M. J. Rosulek, and M. Winslett. Harvesting credentials in trust negotiation as an honest-but-curious adversary. In *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, WPES '07, pages 64–67, New York, NY, USA, 2007. ACM.

[46] C. Palamidessi. Probabilistic and nondeterministic aspects of anonymity. *Electron. Notes Theor. Comput. Sci.*, 155:33–42, 2006.

[47] T. P. Pedersen. Non-interactive and information-theoretic secure verifiable secret sharing. In *CRYPTO*, pages 129–140, 1991.

[48] A. Pfitzmann and M. Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management. http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf, Aug 2010.

[49] R. Ramanujam and S. P. Suresh. A decidable subclass of unbounded security protocols. In *Workshop on Issues in the Theory of Security (WITS'03)*, pages 11–20, 2003.

[50] R. Ramanujam and S. P. Suresh. Undecidability of secrecy for security protocols, Jul 2003. Manuscript.

[51] W. Razouk, F. L. Ţiplea, A. Sekkaki, and C. Varlan. Providing anonymity for rfid systems. *Journal of Information and Communication Technologies*, 3(3), Mar. 2013. To appear.

[52] R. L. Rivest. The MD5 Message-Digest Algorithm (RFC 1321). http://www.ietf.org/rfc/rfc1321.txt?number=1321.

[53] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, Feb. 1978.

[54] A. W. Roscoe. CSP and determinism in security modelling. In *In Proc. IEEE Symposium on Security and Privacy*, pages 114–127. Society Press, 1995.

[55] S. Schneider and A. Sidiropoulos. CSP and anonymity. In E. Bertino, H. Kurth, G. Martella, and E. Montolivo, editors, *4th European Symposium on Research in Computer Security (ESORICS'96)*, number 1146 in Lecture Notes in Computer Science, pages 198–218, 1996.

[56] R. Sherwood, B. Bhattacharjee, and A. Srinivasan. P5: A protocol for scalable anonymous communication. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, SP '02, pages 58–. IEEE Computer Society, 2002.

[57] V. Shmatikov. Probabilistic analysis of anonymity. In *In proc. 15th Computer Security Foundations Workshop*, pages 119–128. Society Press, 2002.

[58] E. G. Sirer, M. Polte, M. Robson, E. Gn, S. Milo, and P. M. Robson. Cliquenet: A self-organizing, scalable, peer-to-peer anonymous communication substrate. http://www.cs.cornell.edu/people/egs/papers/cliquenet-iptp.pdf, 2001.

[59] P. F. Syverson and S. G. Stubblebine. Group principals and the formalization of anonymity. In *World Congress on Formal Methods'99*, pages 814–833, 1999.

[60] F. L. Ţiplea, C. Enea, and C. V. Bîrjoveanu. Decidability and complexity results for security protocols. In

E. Clarke, M. Minea, and F. Tiplea, editors, *Verfication of Infinite-state Systems with Applications to Security (VISSAS 2005)*, pages 185–211. IOS Press, 2005.

[61] F. L. Ţiplea, C. Enea, C. V. Bîrjoveanu, and I. Boureanu. Secrecy for bounded protocols with freshness check is nexptime-complete. *Journal of Computer Security*, 16:689–712, Dec 2008.

[62] F. L. Ţiplea, L. Vamanu, and C. Vârlan. Complexity of anonymity for security protocols. In D. Gritzalis, B. Preneel, and T. Theoharidou, editors, *European Symposium on Research in Computer Security (ESORICS 2010)*, volume 6345 of *Lecture Notes in Computer Science*, pages 558–572, 2010.

[63] F. L. Ţiplea, L. Vamanu, and C. Vârlan. Reasoning about minimal anonymity in security protocols. *Future Generation Computer Systems*, 29(3):828–842, 2013.

[64] F. L. Ţiplea and C. Vârlan. Group anonymity and role interchangeability in security protocols. In *8th International Workshop on Security and High Performance Computing Systems*, 2013. submitted.

[65] Y. Tsukada, K. Mano, H. Sakurada, and Y. Kawabe. Anonymity, privacy, onymity, and identity: A modal logic approach. In *2009 International Conference on Computational Science and Engineering*, pages 42–51, 2009.

[66] J. van Eijck and S. Orzan. Epistemic verification of anonymity. *Electron. Notes Theor. Comput. Sci.*, 168:159–174, 2007.

[67] C. Vârlan. Dynamic GPS maps. In 11^{th} *International Conference on Development and Application Systems*, Suceava, Romania, 2008.

[68] C. Vârlan. ITS approaches in Romania: Applying a dynamical perception to vehicle navigation. In *Workshop On ITS Applications And European Electronic Tolling*, Bucharest, Romania, 2009.

[69] C. Vârlan, C. Sotomayor, and A. F. G. Skarmeta. A social approach on creating dynamic maps. In *Positioning and Context-Awarness International Conference*, Antwerpen, Belgium, 2009.

[70] L. von Ahn, A. Bortz, and N. J. Hopper. k-anonymous message transmission. In *Proceedings of the 10th ACM conference on Computer and communications security*, CCS '03, pages 122–130. ACM, 2003.

[71] M. Waidner. Unconditional sender and recipient untraceability in spite of active attacks. In *Advances in Cryptology - EUROCRYPT 1989*, Lecture Notes in Computer Science, pages 302–319. Springer-Verlag, 1989.

[72] M. Wooldridge. *An Introduction to Multiagent Systems.* John Wiley & Sons, LTD, 2002.