TRANSACTIONS ON DATA PRIVACY 3 (2010) 177–198

# Anonymity, Privacy, Onymity, and Identity: A Modal Logic Approach

**Yasuyuki Tsukada***, **Ken Mano***, **Hideki Sakurada***, **Yoshinobu Kawabe****

*NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi, Kanagawa, 243-0198 Japan.

**Aichi Institute of Technology, 1247 Yachigusa, Yakusa-cho, Toyota, Aichi, 470-0392 Japan.

E-mail: {tsukada,mano,sakurada}@theory.brl.ntt.co.jp, kawabe@aitech.ac.jp

**Abstract.** In this paper, we propose a taxonomy of privacy-related information-hiding/disclosure properties in terms of the modal logic of knowledge for multiagent systems. The properties considered here are anonymity, privacy, onymity, and identity. Intuitively, anonymity means the property of hiding who performed a certain specific action, privacy involves hiding what was performed by a certain specific agent, onymity refers to disclosing who performed a certain specific action, and identity relates to disclosing what was performed by a certain specific agent. Building on Halpern and O'Neill's work, we provide formal definitions of these properties and study the logical structure underlying them. In particular, we show that some weak forms of anonymity and privacy are compatible with some weak forms of onymity and identity, respectively. We also discuss the relationships between our definitions and existing standard terminology, in particular Pfitzmann and Hansen's consolidated proposal.

**Keywords.** Anonymity, Privacy, Onymity, Identity, Modal Logic of Knowledge

## 1 Introduction

The terminology and taxonomy of privacy and related information-hiding properties have attracted much attention. Indeed, a considerable amount of substantial research has been undertaken from various standpoints [30, 29, 18, 16, 24, 33]. The present paper also deals with privacy-related information-hiding properties in information systems, and studies the logical structure underlying them. A novel aspect of this paper is that it considers relevant privacy-related information-disclosure properties. This work proposes a new taxonomy for information hiding and information disclosure by contrasting them logically.

The privacy-related information-hiding/disclosure properties considered in this paper are *anonymity*, *privacy*, *onymity*, and *identity* (Fig. 1). Intuitively, we can understand anonymity to be the property of *hiding who* performed a certain specific action, privacy that of *hiding what* was performed by a certain specific agent, onymity that of *disclosing who* performed a certain specific action, and identity that of *disclosing what* was performed by a

*This is a revised and extended version of [36].

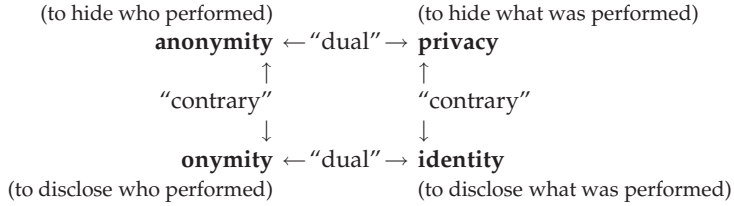


Figure 1: An intuitive taxonomy of privacy-related information-hiding/disclosure properties

certain specific agent. For example, if we are unaware of who, say Alice, Bob, or Charlie, has donated a million dollars to an orphanage, then this donation is said to be anonymous. If we discover that a specific person, say Charlie, is the donor, then this donation is onymous. Further, if you do not know what amount of money, say ten, a thousand, or a million dollars, I withdrew from my bank account yesterday, then my withdrawal is private. If you know that I withdrew a million dollars, then you can identify me as a millionaire.

In other words, these four properties can be related by two intuitive operations, namely "dual" and "contrary" operations. The "dual" operation functions horizontally in Fig. 1 and takes the subject/object reversal "dual" by interchanging *who* with *what*. In view of this operation, we can say that anonymity and onymity are "dual" for privacy and identity, respectively, and vice versa. On the other hand, the "contrary" operation functions vertically in Fig. 1 and takes the logical "contrary" by interchanging *hiding* with *disclosure*. In view of this operation, we can say that anonymity and privacy are contrary to onymity and identity, respectively, and vice versa. If we group anonymity and privacy into the *privacy category* and onymity and identity into the *identity category* (or, more generally, the *security category*), then this duality will provide us with a way of refining each category. The contrary relation may be regarded as representing what we call "tension" or "trade-off" between the privacy and security categories. These intuitions are, however, rather informal and need further elaboration.

The aim of the present paper is to provide a logically solid framework so that all the properties shown in Fig. 1 can be formally dealt with and the relationship between them clearly and elaborately expressed.

Towards this aim, we build on Halpern and O'Neill's work [14], which has shown that *the modal logic of knowledge* (or *epistemic logic*) for multiagent systems provides a fundamental framework for reasoning about anonymity. We first extend this framework to capture a formal definition of privacy. This has, however, already been done by Mano *et al.* [27]. More specifically, they have formulated privacy as the dual of anonymity within Halpern and O'Neill's framework and have shown that these two properties can be related by a newly proposed information-hiding property called *role interchangeability*.

Building on [14] and [27], in this paper we consider the logical contraries of anonymity and privacy, thereby giving formal definitions of onymity and identity. We also consider the duality between the obtained onymity and identity properties. Thus, we provide a detailed, formal version of Fig. 1 in terms of the modal logic of knowledge. The results are summarized in Fig. 3 at the end of Sect. 8.

The contributions of this paper can be summarized as follows. First, we believe this to be the first presentation of a taxonomy that comprehensively covers these four properties. In particular, the formal definitions of privacy, onymity, and identity that we give in Fig. 3 are novel.

Second, our taxonomy also reveals the logical structure underlying these properties, so that it can be used, for example, to consider a formal aspect of "tension" or "trade-off" between the privacy and security categories mentioned above. Since anonymity and privacy are respectively defined as contraries to onymity and identity, it is not surprising that strong forms of anonymity and privacy are incompatible with strong forms of onymity and identity, respectively. Our detailed taxonomy, however, enables us to consider a more subtle, marginal area between the privacy and security categories. That is, we can show that some weak forms of anonymity and privacy are compatible with some weak forms of onymity and identity, respectively. This means that there is an information system that is in some sense both anonymous and onymous.

Third, our formal taxonomy is simple, since we build on the fundamental work of Halpern and O'Neill, and also comprehensive, which means that it can serve as a logical "hub" for comparing and analyzing various previous concepts of privacy-related information-hiding/disclosure properties. More specifically, various concepts can be paraphrased or interpreted as the appropriate logical formulas or concepts shown in Fig. 3. In this paper, we are particularly interested in comparing our taxonomy and the existing standard terminology of Pfitzmann and Hansen [30, 29]. One can see that our duality viewpoint is particularly novel and plays an important role in refining the concepts that Pfitzmann and Hansen proposed. In addition, we are also concerned with the relationship between our formulation of onymity/identity and existing fundamental concepts of authentication/non-repudiation. Since onymity is the property of disclosing who, it is easy to see that it is closely related to (personal) authentication. Similarly, identity is closely related to attribute authentication. Non-repudiation can also be formulated naturally in terms of some forms of onymity or identity. We discuss these relationships between onymity/identity and authentication/non-repudiation.

## 1.1 Related Work

Formal approaches to privacy-related information-hiding properties go back to the seminal work of Schneider and Sidiropoulos [31], who proposed the concept of *strong anonymity*. Since then, this concept has been further developed and elaborated in various frameworks [1, 25, 8, 9, 2, 22, 21, 23, 15]. In these studies, properties are formulated in terms of computational languages such as CSP [31], applied $\pi$ calculus [1, 25, 8, 9, 2], and I/O-automata [22, 21, 23]. Another approach, which we call the logical approach here, has also been developed in [35, 14, 37, 13, 20, 39, 3, 38, 27, 26, 5], where properties are formulated in terms of the modal logic of knowledge for multiagent systems.

The two approaches—computational and logical—have been shown to have some interesting relationships. For example, Halpern and O'Neill showed that strong anonymity can be characterized by a logical counterpart that they defined in the modal logic of knowledge [14]. Mano *et al.* extended this to show that role interchangeability can be characterized by a computational counterpart that they defined in terms of traces of I/O-automata [27].

It is also recognized, however, that these two approaches have their own specific merits. The computational approach offers powerful proof methods and practical support tools, as demonstrated by the many successful case studies undertaken to prove several privacy-related information-hiding properties of quite complex electronic voting protocols [25, 21, 23, 8, 9, 2]. In contrast, the primary advantage of the logical approach is that the modal logic of knowledge is so expressive that we can use it to specify a variety of information-hiding properties succinctly. This is why we follow the logical approach in the present paper. In fact, we do not necessarily require the whole expressive power of the

modal logic of knowledge, because the properties and examples discussed in this paper do not involve any nested use of modal operators. However, as the summary of our results shown in Fig. 3 indicates, we should be able to consider the above-mentioned refinement (into anonymity/privacy and onymity/identity) and achieve some separation (between total/minimal and partial/maximal). Further, we also consider some combinations of the obtained properties to discuss more subtle properties such as weak/strong receipt-freeness (Example 5.4) and some form of unlinkability (Sect. 10.2). Thus, the expressiveness of the logical approach is important to the aim of the present paper.

### 1.2 Organization

This paper is organized as follows. Section 2 provides some technical preliminaries as regards the modal logic of knowledge for multiagent systems. Building on this logic, we give a formal account of the properties shown in Fig. 1 and also discuss their relationship (Sects. 3, 4, 5, 6, 7, and 8). Note that the material in Sects. 6, 7, and 8 is original, while the definitions and propositions in Sect. 3 and in Sects. 4 and 5 are derived from [14] and from [27], respectively, although some additional examples such as sender anonymity (Example 3.1), message privacy (Example 5.1), and receipt-freeness (Example 5.4) are also considered. The obtained taxonomy is used in Sect. 9 to consider the compatibility of anonymity, privacy, onymity, and identity. We can observe that some weak forms of anonymity and privacy are compatible with some weak forms of onymity and identity, respectively. Section 10 is devoted to discussions of our proposed taxonomy. We first discuss our proposal in relation to the standard terminology proposed by Pfitzmann and Hansen. We also discuss how our formulations of onymity and identity are related to authentication and non-repudiation. Finally, Sect. 11 summarizes the results of the paper.

## 2 Preliminaries

We briefly review the modal logic of knowledge for multiagent systems. Notions and terminologies are borrowed from [11, 14].

A *multiagent system* consists of $n$ *agents* with their *local states* and develops over time. We assume that an agent's local state encapsulates all the information to which the agent has access. Let $I = \{i_1, \ldots, i_n\}$ be the set of $n$ agents. A *global state* is defined as the tuple $(s_{i_1}, \ldots, s_{i_n})$ with all local states from $i_1$ to $i_n$. A *run* is a function from *time*, ranging over the natural numbers, to global states. A *point* is a pair $(r, m)$ comprising a run $r$ and a time $m$, and the global state at a point $(r, m)$ is denoted by $r(m)$. The function $r_x$ of $m$ is the projection of $r(m)$ to $x$'s component, so that $r_x(m) = s_x$ if $r(m) = (s_{i_1}, \ldots, s_{i_n})$ for $x = i_1, \ldots, i_n$. A *system* is a set of runs. The set of all points in a system $\mathcal{R}$ is denoted by $\mathcal{P}(\mathcal{R})$.

In a multiagent system, we can define the knowledge of an agent on the basis of the indistinguishability of the state for the agent. Given a system $\mathcal{R}$ and an agent $i$, let $\mathcal{K}_i(r, m)$ be the set of points in $\mathcal{P}(\mathcal{R})$ that $i$ thinks are possible at $(r, m)$; that is,

$$\mathcal{K}_i(r, m) = \{(r', m') \in \mathcal{P}(\mathcal{R}) \mid (r', m') \sim_i (r, m)\},$$

where $(r', m') \sim_i (r, m)$ means that $r'_i(m') = r_i(m)$. We can say that an agent $i$ "knows" $\phi$ at a point $(r, m)$ if $\phi$ is true at all points in $\mathcal{K}_i(r, m)$.

The *formulas* of the modal logic of knowledge are inductively constructed from a set $\Phi$ of *primitive propositions* (such as "the key is $k$" or "an agent $i$ sent a message $m$ to an agent $j$"),

the usual logical connectives, and a modal operator $K_i$ that represents the knowledge of agent $i$.

The meaning of each formula can be determined when each primitive proposition is given an interpretation. An *interpreted system* $\mathcal{I}$ consists of a pair $(\mathcal{R}, \pi)$ comprising a system $\mathcal{R}$ and an *interpretation* $\pi$ that maps each point to the truth-value assignment function for $\Phi$ for the point. In other words, $(\pi(r,m))(p) \in \{true, false\}$ for each $p \in \Phi$ and $(r,m) \in \mathcal{P}(\mathcal{R})$. Given an interpreted system $\mathcal{I} = (\mathcal{R}, \pi)$ and a point $(r,m)$ in $\mathcal{R}$, we define what it means for a formula $\phi$ to be true at $(r,m)$ in $\mathcal{I}$ by induction on the structure of formulas. Typical cases are as follows:

- $(\mathcal{I}, r, m) \models p$ if $(\pi(r,m))(p) = true$
- $(\mathcal{I}, r, m) \models \neg\phi$ if $(\mathcal{I}, r, m) \not\models \phi$
- $(\mathcal{I}, r, m) \models \phi \wedge \psi$ if $(\mathcal{I}, r, m) \models \phi$ and $(\mathcal{I}, r, m) \models \psi$
- $(\mathcal{I}, r, m) \models K_i\phi$ if $(\mathcal{I}, r', m') \models \phi$ for all $(r', m') \in \mathcal{K}_i(r, m)$

In addition to $K_i\phi$, which means that $i$ knows $\phi$, we also use $P_i\phi$ as an abbreviation of $\neg K_i \neg\phi$, which means that $i$ thinks that $\phi$ is possible. We also write $\mathcal{I} \models \phi$ if $(\mathcal{I}, r, m) \models \phi$ holds for every point $(r,m)$ in $\mathcal{I}$.

In the rest of the paper, we consider that the set $A$ of *actions* is also associated with each system. We assume that $i, i', j, j', \ldots$ range over agents while $a, a', b, b', \ldots$ range over actions. Following [14], we use primitive propositions of the form $\theta(i,a)$, which denotes that "an agent $i$ has performed an action $a$, or will perform $a$ in the future." Note that the truth value of $\theta(i,a)$ depends on the run, but not on the time; that is, if $(\mathcal{I}, r, m) \models \theta(i,a)$ holds for some $m$, then $(\mathcal{I}, r, m') \models \theta(i,a)$ also holds for every $m'$.

We introduce four additional conditions regarding the truth value of $\theta(i,a)$, which will be useful in proving some propositions. We say that an action $a$ is *exclusive* in the interpreted system $\mathcal{I}$ if $a$ is performed by at most one agent in each run, that is, $\mathcal{I} \models \bigwedge_{i \neq i'} \neg[\theta(i,a) \wedge \theta(i',a)]$ holds. We also say that an agent $i$ is *exclusive* in the interpreted system $\mathcal{I}$ if $i$ performs at most one action in each run, that is, $\mathcal{I} \models \bigwedge_{a \neq a'} \neg[\theta(i,a) \wedge \theta(i,a')]$ holds. (The exclusiveness of an action is assumed in Propositions 3.1, 4.2, 6.1, and 7.2; the exclusiveness of an agent is assumed in Propositions 5.2 and 5.3.) Let $j$ denote a special agent called an observer. Given an agent $i \in I/\{j\}$ and an action $a \in A$, we also say that $i$ performing $a$ is *nonsingular* with respect to $j$ if at least one agent other than $i$ and $j$ performs some action, that is, $\mathcal{I} \models \theta(i,a) \Rightarrow \bigvee_{i' \in I/\{j\}} \bigvee_{a' \in A}[i \neq i' \wedge \theta(i',a')]$ holds. We also say that $a$ performed by $i$ is *nonsingular* with respect to $j$ if at least one action other than $a$ is performed by some agent, that is, $\mathcal{I} \models \theta(i,a) \Rightarrow \bigvee_{a' \in A} \bigvee_{i' \in I/\{j\}}[a \neq a' \wedge \theta(i',a')]$ holds. (The nonsingularity of an agent is assumed in Propositions 4.2 and 7.2; the nonsingularity of an action is assumed in Proposition 5.3.)

# 3 Anonymity

**Definition 3.1.** An action $a$ performed by an agent $i$ is *minimally anonymous* with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i,a) \Rightarrow P_j[\neg\theta(i,a)].$$

In [14], this condition is described equivalently as $\mathcal{I} \models \neg K_j[\theta(i,a)]$.

Intuitively, minimal anonymity means that, from $j$'s viewpoint, $a$ could not have been performed by $i$.

**Remark 3.1.** Consider that our built-in proposition $\theta(i, a)$ expresses a specific form of "link" between an agent $i$ and an action $a$. Then, we can observe that minimal anonymity is similar to a specific form of the "unlinkability" property that was stipulated by Pfitzmann and Hansen [29]. This observation will be elaborated in Section 10.2.

**Definition 3.2.** An action $a$ performed by an agent $i$ is *anonymous up to* an *anonymity set* $I_A \subseteq I$ with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i, a) \Rightarrow \bigwedge_{i' \in I_A} P_j[\theta(i', a)].$$

In particular, an action $a$ performed by an agent $i$ is *totally anonymous* with respect to $j$ when the same condition holds for $I_A = I/\{j\}$.

Intuitively, anonymity up to $I_A$ means that, from $j$'s viewpoint, $a$ could have been performed by anybody in $I_A$. Taking the cardinality of $I_A$ into account straightforwardly, we can also obtain the definition of *k-anonymity* [14].

**Example 3.1.** In [30], Pfitzmann and Köhntopp defined *sender anonymity* as the property that (1) a particular message is not linkable to any sender and (2) to a particular sender, no message is linkable. The first part of the definition can be paraphrased in our formalism as follows:

$$\mathcal{I} \models \theta(i, send(m)) \Rightarrow \bigwedge_{i' \in I_A} P_j[\theta(i', send(m))].$$

Here, $\theta(i, send(m))$ means that $i$ sends a message $m$, and $I_A$ denotes the set of possible senders.

**Proposition 3.1** ([14, Proposition 3.3])**.** Suppose that an action $a$ is exclusive and that an anonymity set $I_A$ contains at least three agents. If $a$ performed by an agent $i$ is anonymous up to $I_A$ with respect to an agent $j$, then it is minimally anonymous as well.

*Proof.* Suppose that $a$ performed by $i$ is anonymous up to $I_A$ and that $(\mathcal{I}, r, m) \models \theta(i, a)$. Because there are at least three agents in $I_A$, there is some agent $i'$ other than $i$ and $j$ in $I_A$. Then, by anonymity up to $I_A$, $(\mathcal{I}, r, m) \models P_j[\theta(i', a)]$, that is, $\theta(i', a)$ holds at some point $(r', m')$ such that $(r', m') \sim_j (r, m)$. Then, by the exclusiveness assumption, $(\mathcal{I}, r', m') \models \neg\theta(i, a)$ because $i \neq i'$. Therefore, $(\mathcal{I}, r, m) \models P_j[\neg\theta(i, a)]$. □

# 4 Role Interchangeability

Role interchangeability [27] means that, as far as an agent $j$ is concerned, any two agents could interchange their *roles*, that is, the actions they performed.

**Definition 4.1.** A pair $(i, a)$ comprising an agent $i$ and an action $a$ is *totally role interchangeable* (or simply, *role interchangeable*) with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i, a) \Rightarrow \bigwedge_{i' \in I/\{j\}} \bigwedge_{a' \in A} (\theta(i', a') \Rightarrow P_j[\theta(i', a) \wedge \theta(i, a')]).$$

We also say that $(I, A)$ is *role interchangeable* with respect to an agent $j$ if every pair comprising $i \in I/\{j\}$ and $a \in A$ is role interchangeable with respect to $j$ in $\mathcal{I}$. This is the original definition of role interchangeability in [27].

**Example 4.1.** In [27], Mano *et al.* dealt with a practical electronic voting protocol called FOO [12] and discussed its role-interchangeability property. More specifically, let $I$ and $A$ be $\{1, \ldots, vmax\}$ and $\{vote(null), vote(1), \ldots, vote(cmax)\}$, respectively. Here, $vmax$ and $cmax$ denote the numbers of voters and candidates, respectively. Assume the intended interpretation of $\theta(i, vote(k))$ is that a voter $i$ voted for a candidate $k$. In particular, $null$ represents emptiness or namelessness, and $\theta(i, vote(null))$ means that $i$ received the right to vote (from a certain administrator) but did not actually cast a vote. Then, the role interchangeability of $(I, A)$ with respect to an agent $j$ means the following: for any $i$ and $i'$ and any $k$ and $k'$, if $i$ voted for $k$ and $i'$ voted for $k'$, then $j$ thinks that it is possible that $i$ voted for $k'$ and $i'$ voted for $k$.

Despite the similarity between role interchangeability and anonymities, they are not equi-expressive [27]. We first observe that we can derive total anonymity and minimal anonymity from role interchangeability by assuming certain appropriate conditions.

**Proposition 4.1** ([27, Theorem 2.9])**.** Let $I_A$ be the set of agents that perform some action in every run in $\mathcal{I}$, that is, the set $\{i \in I/\{j\} \mid \mathcal{I} \models \bigvee_{a \in A} \theta(i, a)\}$. If a pair comprising $i \in I/\{j\}$ and $a \in A$ is role interchangeable with respect to $j$ in $\mathcal{I}$, then $a$ performed by $i$ is anonymous up to $I_A$.

*Proof.* Suppose $(\mathcal{I}, r, m) \models \theta(i, a)$. Let $i'$ be any agent in $I_A$. Then, there is an action $a'$ such that $(\mathcal{I}, r, m) \models \theta(i', a')$. By role interchangeability, we have $(\mathcal{I}, r, m) \models P_j[\theta(i', a) \wedge \theta(i, a')]$. Thus, $(\mathcal{I}, r, m) \models \bigwedge_{i' \in I_A} P_j[\theta(i', a)]$. □

**Example 4.2.** Assume that the role-interchangeability property explained in Example 4.1 holds for the FOO electronic voting protocol. Then, by virtue of Proposition 4.1, we can deduce that the *voter anonymity* property holds for FOO. More specifically, it is true that every action $vote(k)$ performed by $i$ is anonymous up to $I_A$ (with respect to the observer $j$), where $I_A$ is the set of all voters who obtain the right to vote.

**Corollary 4.1** ([27, Corollary 2.10])**.** Suppose that every agent in $I/\{j\}$ performs some action in $A$ in every run in $\mathcal{I}$. If a pair comprising $i \in I/\{j\}$ and $a \in A$ is role interchangeable with respect to $j$ in $\mathcal{I}$, then $a$ performed by $i$ is totally anonymous.

**Proposition 4.2** ([27, Theorem 2.7])**.** Given $i \in I/\{j\}$ and $a \in A$, assume that $i$ performing $a$ is nonsingular and that $a$ is exclusive. If the pair comprising $i$ and $a$ is role interchangeable with respect to $j$ in $\mathcal{I}$, then $a$ performed by $i$ is minimally anonymous.

*Proof.* Suppose $(\mathcal{I}, r, m) \models \theta(i, a)$. By the nonsingularity assumption, there exist $i' \in I/\{j\}$ and $a' \in A$ such that $i \neq i'$ and $\theta(i', a')$ hold at $(r, m)$.

By role interchangeability, $(\mathcal{I}, r, m) \models P_j[\theta(i, a') \wedge \theta(i', a)]$, so $(\mathcal{I}, r, m) \models P_j[\theta(i', a)]$, that is, $\theta(i', a)$ holds at some point $(r', m')$ such that $(r', m') \sim_j (r, m)$. Then, by the exclusiveness assumption, $(\mathcal{I}, r', m') \models \neg\theta(i, a)$. Therefore, $(\mathcal{I}, r, m) \models P_j[\neg\theta(i, a)]$. □

There are two practical merits of role interchangeability. First, role interchangeability can be characterized by a computational counterpart that is defined in terms of traces of I/O-automata, thereby constituting a useful simulation proof method [27]. More specifically, the role interchangeability of $(I, A)$ with respect to an observer $j$ holds if and only if for every trace $t$ such that $i.a$ and $i'.a'$ occur in $t$, there exists a trace $t'$ such that $i'.a$ and $i.a'$ occur in $t'$ and the observer $j$ thinks that $t$ and $t'$ are equivalent. Here, $i.a$ and $i'.a'$ are called *trace actions* and their occurrence in a trace $t$ means that the propositions $\theta(i, a)$ and $\theta(i', a')$ are true in the run $r$ corresponding to $t$. The existence of such an equivalent trace

$t'$ can be proved with the proposed simulation method. (For full details, see [27].) This characterization enables us to adopt a "hybrid" approach to anonymity verification; the relationship between each specific anonymity property and role interchangeability is proved "logically" in our framework of the modal logic of knowledge (as shown in Proposition 4.1, Corollary 4.1, and Proposition 4.2), and the role interchangeability itself is proved "computationally" by the simulation proof method, which is capable of being (partially) automated with the assistance of verification tools.

Second, from role interchangeability, we can systematically derive the "privacy" property as well as anonymity. In other words, we can establish both anonymity and privacy simultaneously via only one simulation proof of role interchangeability. Indeed, these two merits have been shown to be useful in demonstrating the anonymity and privacy properties of the FOO electronic voting protocol. These remarks are elaborated in the following section.

# 5 Privacy

In [27], Mano *et al.* considered the operation of taking the subject/object reversal (or agent/action reversal) dual, that is, the operation that replaces $I$ with $A$ and $A$ with $I$. Applying this duality operation to the anonymity properties given in Sect. 3, they obtained the properties that they called *privacy*.

**Definition 5.1.** An agent $i$ performing an action $a$ is *private up to* a *privacy set* $A_I \subseteq A$ with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i,a) \Rightarrow \bigwedge_{a' \in A_I} P_j[\theta(i,a')].$$

In particular, an agent $i$ performing an action $a$ is *totally private* with respect to $j$ when the same condition holds for $A_I = A$.

Intuitively, privacy up to $A_I$ means that, from $j$'s viewpoint, $i$ could have performed any action in $A_I$. This definition certainly corresponds to our observation that hiding *who* has performed the action is anonymity while hiding *what* has been performed by the agent is privacy.

**Example 5.1.** Recall the definition of sender anonymity proposed by Pfitzmann and Köhntopp [30] and given in Example 3.1. The second part of the definition can be paraphrased in our formalism as follows:

$$\mathcal{I} \models \theta(i, send(m)) \Rightarrow \bigwedge_{a' \in A_I} P_j[\theta(i,a')],$$

where $A_I = \{send(m') \mid m' \text{ is a possible message}\}$. The property paraphrased above can therefore be called *message privacy* according to our terminology.

**Example 5.2.** In [28], Mauw *et al.* proposed the concept of an *attribution set* and used it to analyze the FOO electronic voting protocol [12]. The attribution set $AS(i)$ of a voter $i$ for FOO is defined as the set of votes that can possibly be attributed to $i$. Thus, $AS(i)$ can be regarded as an example of a privacy set. The concept of an attribution set has been extended to a case where more active adversaries are present [19].

The following is the dual of Proposition 4.1. Note that role interchangeability is equivalent to its dual.

**Proposition 5.1** ([27, Theorem 2.13])**.** Let $A_I$ be the set of actions that is performed by some agent in every run in $\mathcal{I}$, that is, the set $\{a \in A \mid \mathcal{I} \models \bigvee_{i \in I/\{j\}} \theta(i,a)\}$. If a pair comprising $i \in I/\{j\}$ and $a \in A$ is role interchangeable with respect to $j$ in $\mathcal{I}$, then $i$ performing $a$ is private up to $A_I$.

*Proof.* Suppose $(\mathcal{I}, r, m) \models \theta(i,a)$. Let $a'$ be any action in $A_I$. Then, there is an agent $i'$ in $I/\{j\}$ such that $(\mathcal{I}, r, m) \models \theta(i', a')$. By role interchangeability, we have $(\mathcal{I}, r, m) \models P_j[\theta(i', a) \wedge \theta(i, a')]$. Thus, $(\mathcal{I}, r, m) \models \bigwedge_{a' \in A_I} P_j[\theta(i, a')]$. □

**Example 5.3.** Assume that the role-interchangeability property explained in Example 4.1 holds for the FOO electronic voting protocol. Then, by virtue of Proposition 5.1, we can deduce that the *vote privacy* property holds for FOO. More specifically, it is true that every voter $i$ who performs $vote(k)$ is private up to $A_I$ (with respect to the observer $j$), where $A_I$ is the set of actions $vote(k')$ such that $k'$ is a candidate who wins a vote.

**Remark 5.1.** In other words, Propositions 4.1 and 5.1 guarantee that by proving role interchangeability, we obtain both anonymity up to $I_A$ and privacy up to $A_I$ simultaneously for appropriate $I_A$ and $A_I$. Indeed, Mano *et al.* [27] demonstrated the role-interchangeability property of FOO by using a simulation proof method in a computational model based on I/O-automata, thereby showing the voter anonymity and vote privacy properties of FOO.

Besides role interchangeability, minimal anonymity is also equivalent to its dual:

**Definition 5.2.** An agent $i$ performing an action $a$ is *minimally private* with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i,a) \Rightarrow P_j[\neg\theta(i,a)].$$

**Example 5.4.** In [20], Jonker and Pieters formulated *receipt-freeness* in terms of what we call minimal privacy. It can be regarded as an extension of vote privacy and has also been commonly sought for electronic voting protocols. This property means that a voter does not gain any information (a *receipt*) that can be used to prove to a coercer that the voter voted in a certain way. Their definition of *weak receipt-freeness* can be paraphrased in our formalism as follows:

$$(\mathcal{I}, r.(i \to j : x), m) \models \theta(i, vote(k)) \Rightarrow P_j[\neg\theta(i, vote(k))]$$

holds for every run $r$, time $m$, and message $x$ that $i$ possesses. Here, the notation $r.(i \to j : x)$ is borrowed from [20] and not defined formally here. Intuitively, the above definition means that some minimal privacy property holds even after the current run $r$ is extended by concatenating it with a new global state that indicates that the voter $i$ supplies an arbitrary message (a receipt) $x$ to the coercer $j$. Actually, they also defined *strong receipt-freeness* as the conjunction of minimal privacy and privacy up to a certain privacy set $A_I$:

$$\begin{aligned}(\mathcal{I}, r.(i \to j : x), m) \;\models\; & \theta(i, vote(k)) \\ & \Rightarrow (P_j[\neg\theta(i, vote(k))] \wedge \bigwedge_{a \in A_I} P_j[\theta(i,a)]),\end{aligned}$$

where $A_I$ denotes the set $\{vote(k') \mid k' \text{ is a possible candidate}\}$.

The following is the dual of Proposition 3.1, which shows a relationship between minimal privacy and privacy up to $A_I$. In particular, it indicates that the former conjunct occurring

in the definition of strong receipt-freeness above turns out to be redundant, provided that certain conditions are satisfied. Hereafter, the proof of the dual of a proved proposition will be omitted, because it can be straightforwardly obtained from the original proof via duality, as the proof of Proposition 5.1 exemplifies.

**Proposition 5.2.** Suppose that an agent $i$ is exclusive and that a privacy set $A_I$ contains at least two actions. If $i$ performing an action $a$ is private up to $A_I$ with respect to an agent $j$, then it is minimally private as well.

The following also holds, which is the dual of Proposition 4.2:

**Proposition 5.3** ([27, Remark 2.15])**.** Given $i \in I/\{j\}$ and $a \in A$, assume that $a$ performed by $i$ is nonsingular and that $i$ is exclusive. If the pair comprising $i$ and $a$ is role interchangeable with respect to $j$ in $\mathcal{I}$, then $i$ performing $a$ is minimally private.

**Remark 5.2.** Since minimal anonymity is equivalent to its dual, that is, minimal privacy, Proposition 5.3 also indicates that, to derive minimal anonymity from role interchangeability, we can assume the nonsingularity of $a$ and the exclusiveness of $i$ (as described in Proposition 5.3) instead of the nonsingularity of $i$ and the exclusiveness of $a$ (as described in Proposition 4.2).

**Example 5.5.** Let $I$ and $A$ be the same as those in Example 4.1. Then, the exclusiveness of an action means that no two voters vote for the same candidate, which is quite unnatural as regards normal voting. On the other hand, the exclusiveness of an agent seems to be a much more adequate condition, namely, that a voter does not vote for two candidates. Although this adequacy depends on the interpretation, the example shows that our duality is useful in terms of obtaining appropriate premises for the problem to be solved.

# 6 Onymity

By the "contrary" of a formula of the form $\theta(i,a) \Rightarrow \Gamma$, we mean the formula $\theta(i,a) \Rightarrow \neg\Gamma$. The hypothesis $\theta(i,a)$ is to be preserved because we want to confine ourselves to a consideration of the epistemic properties of runs where $i$ has actually performed $a$. By taking the contrary of the anonymity properties formulated in Sect. 3, we can obtain the definitions of the properties that we call *onymity*.

**Definition 6.1.** An action $a$ performed by an agent $i$ is *maximally onymous* with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i,a) \Rightarrow K_j[\theta(i,a)]. \tag{1}$$

Intuitively, maximal onymity means that $j$ knows that $i$ has performed $a$. This definition corresponds to our observation that onymity generally means that the agent who performs the action is disclosed.

**Claim 6.1.** The formula (1) is equivalent to

$$\mathcal{I} \models P_j[\theta(i,a)] \Rightarrow \theta(i,a). \tag{2}$$

*Proof.* Assume (1) and $(\mathcal{I}, r, m) \models P_j[\theta(i,a)]$. Then, there exists a point $(r', m')$ such that $(r', m') \sim_j (r, m)$ and $(\mathcal{I}, r', m') \models \theta(i,a)$. By virtue of (1), $(\mathcal{I}, r', m') \models K_j[\theta(i,a)]$ holds. Since $(r', m') \sim_j (r, m)$, this means that $(\mathcal{I}, r, m) \models \theta(i,a)$.

Conversely, assume (2) and $(\mathcal{I}, r, m) \models \theta(i, a)$. Let $(r', m')$ be an arbitrary point such that $(r', m') \sim_j (r, m)$. By definition, $(\mathcal{I}, r', m') \models P_j[\theta(i, a)]$. By virtue of (2), $(\mathcal{I}, r', m') \models \theta(i, a)$ holds. Since $(r', m')$ is an arbitrary point such that $(r', m') \sim_j (r, m)$, this means that $(\mathcal{I}, r, m) \models K_j[\theta(i, a)]$. This concludes the proof. □

**Example 6.1.** Consider an anonymous authentication scheme based on *group signatures* [6]. In such a scheme, a legitimate agent can be authorized only as a group member, being granted anonymity up to a certain anonymity set, but will be maximally onymous once it is considered illegitimate. Specifically, let $G$ be a group of agents and $k$ a distinct agent called a group authority. Also assume the intended interpretation of $\theta(i, gsign_G(m))$ is that an agent $i$ in $G$ sends a message $m$ with a group signature on it. Then, the anonymity requirement can be specified as

$$\mathcal{I} \models \theta(i, gsign_G(m)) \Rightarrow \bigwedge_{i' \in G} P_j[\theta(i', gsign_G(m))],$$

where an observer $j$ is assumed not to belong to $G \cup \{k\}$. Further, in case of a dispute, the group authority $k$ can trace the sender of a message. This can be specified, in terms of maximal onymity, as

$$\mathcal{I} \models \theta(i, gsign_G(m)) \Rightarrow K_k[\theta(i, gsign_G(m))].$$

**Definition 6.2.** An action $a$ performed by an agent $i$ is *onymous down from* an *onymity set* $I_A \subseteq I$ with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i, a) \Rightarrow \bigvee_{i' \in I_A} K_j[\neg\theta(i', a)].$$

In particular, an action $a$ performed by an agent $i$ is *partially onymous* with respect to $j$ when the same condition holds for $I_A = I/\{j\}$.

Intuitively, onymity down from $I_A$ means that, from $j$'s viewpoint, some agent in $I_A$ except $j$ itself has not performed $a$. The following example shows that the above definition also corresponds to our general observation that onymity is the property of disclosing who has performed the action.

**Example 6.2.** Suppose that a detective $j$ is using network forensic analysis tools and searching for a criminal, say $i$, who has committed a homicide $a$. (As a technical note, $a$ can be regarded as an exclusive action.) Let $I_A$ be a set of suspects. Then, onymity down from $I_A$ means that there is a suspect $i'$ in $I_A$ such that the detective $j$ knows that $i'$ has not performed $a$ (Fig. 2). This means that $j$ can narrow the set of suspects down to a substantially smaller one. (This is similar to *identification by elimination* referred to in [17].) In other words, who actually committed the homicide is closer to being "disclosed." This contrasts with the idea that anonymity up to $I_A$ generally means that $j$ regards the set as remaining large.

**Remark 6.1.** In their consolidated terminology paper [29], Pfitzmann and Hansen defined the concept of *identifiability* as the "negation" of anonymity. The definition accompanies the concept of an *identifiability set*. We can see that identifiability and identifiability sets are similar to onymity and onymity sets in our formulation, respectively.

The following is the contrary of Proposition 3.1:

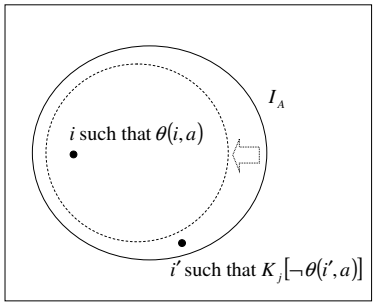


Figure 2: Onymity down from $I_A$

**Proposition 6.1.** Suppose that an action $a$ is exclusive and that an onymity set $I_A$ contains at least three agents. If $a$ performed by an agent $i$ is maximally onymous with respect to an agent $j$, then it is onymous down from $I_A$ as well.

*Proof.* Suppose that $a$ performed by $i$ is maximally onymous and that $(\mathcal{I}, r, m) \models \theta(i, a)$. Because there are at least three agents in $I_A$, there is some agent $i'$ other than $i$ and $j$ in $I_A$. Let $(r', m')$ be any point such that $(r', m') \sim_j (r, m)$. By maximal onymity, $(\mathcal{I}, r', m') \models \theta(i, a)$, that is, $(\mathcal{I}, r', m') \models \neg\theta(i', a)$ by the exclusiveness assumption because $i \neq i'$. Therefore, $(\mathcal{I}, r, m) \models K_j[\neg\theta(i', a)]$. □

# 7 Role Noninterchangeability

Since role interchangeability is a quite strong information-hiding property, its contrary becomes a rather weak information-disclosure property.

**Definition 7.1.** A pair $(i, a)$ consisting of an agent $i$ and an action $a$ is *partially role noninterchangeable* (or simply, *role noninterchangeable*) with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i, a) \Rightarrow \bigvee_{i' \in I/\{j\}} \bigvee_{a' \in A} (\theta(i', a') \wedge K_j[\neg\theta(i', a) \vee \neg\theta(i, a')]).$$

The following are the contraries of Propositions 4.1 and 4.2, respectively. Hereafter, the proof of the contrary of a proved proposition will be omitted, because it can be straightforwardly obtained from the original proof via the contrary, as the proof of Proposition 6.1 exemplifies.

**Proposition 7.1.** Let $I_A$ be the set of agents that perform some action in every run in $\mathcal{I}$, that is, the same set as described in Proposition 4.1. If an action $a \in A$ performed by an agent $i \in I/\{j\}$ is onymous down from $I_A$ with respect to $j$ in $\mathcal{I}$, then the pair comprising $i$ and $a$ is role noninterchangeable.

**Proposition 7.2.** Given $i \in I/\{j\}$ and $a \in A$, assume that $i$ performing $a$ is nonsingular and that $a$ is exclusive. If $a$ performed by $i$ is maximally onymous with respect to $j$ in $\mathcal{I}$, then the pair comprising $i$ and $a$ is role noninterchangeable.

# 8 Identity

Either by taking the dual of the onymity properties shown in Sect. 6 or by taking the contrary of the privacy properties shown in Sect. 5, we can easily obtain the definitions of properties that we call *identity*. By identity we mean the properties of disclosing what the agent *does* or, in case of the be verb, what the agent *is*.

Below we only give the definitions and brief explanations of identity properties; relevant propositions can also be shown in a similar way to the propositions in the previous sections.

**Definition 8.1.** An agent $i$ performing an action $a$ is *maximally identified* with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i,a) \Rightarrow K_j[\theta(i,a)].$$

Note that maximal identity is equivalent to its dual, that is, maximal onymity.

**Definition 8.2.** An agent $i$ performing an action $a$ is *identified down from* an *identity set* $A_I \subseteq A$ with respect to an agent $j$ in the interpreted system $\mathcal{I}$ if

$$\mathcal{I} \models \theta(i,a) \Rightarrow \bigvee_{a' \in A_I} K_j[\neg\theta(i,a')].$$

In particular, an agent $i$ performing an action $a$ is *partially identified* with respect to $j$ when the same condition holds for $A_I = A$.

**Example 8.1.** Consider four attribute values—"stomach cancer (S)," "other cancers (O)," "early stage (E)," and "later stage (L)"—of cancer sufferers. Let the set of possible combinations of these attribute values be denoted by the identity set $A_I = \{is\_S\&E,\ is\_S\&L,\ is\_O\&E,\ is\_O\&L,\ is\_S\&O\&E,\ is\_S\&O\&L\}$. Suppose that a drug seller $j$ is analyzing online medical care transaction data extracted from an e-medicine system and contacting a sufferer $i$ in order to advertise a new drug that is effective only for early-stage stomach cancer without metastasis. Then, the first thing $j$ should do is to narrow the identity set $A_I$ for $i$ to a smaller one. (As a technical note, we assume here that $i$ is exclusive.) That is, $j$'s initial goal can be specified as

$$\mathcal{I} \models \theta(i, is\_S\&E) \Rightarrow \bigvee_{a' \in A_I} K_j[\neg\theta(i,a')].$$

**Remark 8.1.** Besides the identifiability mentioned in Remark 6.1, Pfitzmann and Hansen [29] also defined the concept of an identity, which we hereafter refer to as a *PH-identity*. They stipulated that a PH-identity is "any subset of attribute values of an individual person which sufficiently identifies this individual person within any set of persons." Example 8.1 indicates that each member of $A_I$ can be regarded as a PH-identity. That is, our concept of an identity set can be regarded as a set of possible PH-identities. (In fact, they also defined a weaker concept, a partial identity, which may not sufficiently identify an individual person. To be precise, we should say that an identity set can be viewed as a set of possible *partial PH-identities*.)

The results that we have described so far in this paper are summarized in Fig. 3, which can be regarded as a detailed, formal version of Fig. 1.

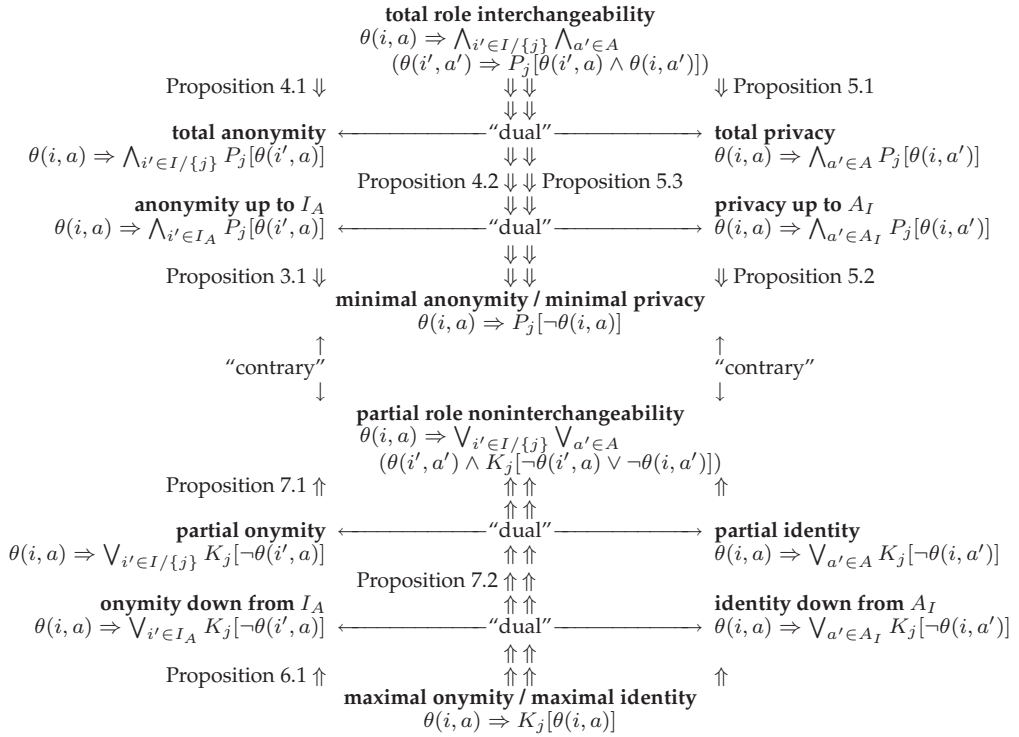


Figure 3: A formal taxonomy of privacy-related information-hiding/disclosure properties

# 9 Compatibility

Instead of having a single property of anonymity, privacy, onymity, or identity, each system sometimes has multiple properties. For example, some requirements of an anonymous authentication scheme based on group signatures can be specified as anonymity up to a certain group and maximal onymity (Example 6.1). While this example system involves these "contrary" properties in its different phases, some more subtle combinations of "contrary" properties might be co-resident in some system. This section is devoted to discussions of this kind of co-residence.

Let $P_1$ and $P_2$ be any of the anonymity or onymity properties that we have formulated so far. We say that $P_1$ and $P_2$ are *compatible* if there exist an interpreted system $\mathcal{I}$, an action $a$, and agents $i$ and $j$ such that

1. $a$ performed by $i$ has the property $P_1$ with respect to $j$ in $\mathcal{I}$,
2. $a$ performed by $i$ has the property $P_2$ with respect to $j$ in $\mathcal{I}$, and
3. $(\mathcal{I}, r, m) \models \theta(i,a)$ holds for some $r$ and $m$.

Known results related to the compatibility of the six anonymity or onymity properties are summarized in Table 1. The compatibility between privacy and identity is similar.

Apparently, $P_1$ and $P_2$ are compatible if they are both in the same category (that is, either the privacy or the security category) and if $P_1$ implies $P_2$. The six $\circ$'s in Table 1 indicate compatibility of this kind. For example, role interchangeability and anonymity up to

Table 1: Compatibility of Anonymity and Onymity

| | Role interchangeability | Anonymity up to $I_A$ | Minimal anonymity | Role noninterchangeability | Onymity down from $I_A$ | Maximal onymity |
|---|---|---|---|---|---|---|
| Role interchangeability | - | ○[a] | ○ | ×[c] | ∗[d] | ∗ |
| Anonymity up to $I_A$ | - | - | ○ | ⊕[b] | × | ∗ |
| Minimal anonymity | - | - | - | ⊕ | ⊕ | × |
| Role noninterchangeability | - | - | - | - | ○ | ○ |
| Onymity down from $I_A$ | - | - | - | - | - | ○ |
| Maximal onymity | - | - | - | - | - | - |

[a] ○: apparent compatibility induced by logical implication. [b] ⊕: compatibility in "marginal" area.
[c] ×: trivial incompatibility by definition. [d] ∗: conditional incompatibility.

$I_A$ are compatible, because Proposition 4.1 guarantees that role interchangeability implies anonymity up to $I_A$ if we take $I_A$ as the set of agents that perform some action in every run. The three $\times$'s indicate incompatibility that is trivial by definition. Role interchangeability and role noninterchangeability, for example, are expressed as "contrary" formulas, so that they are never compatible. The three $*$'s indicate conditional incompatibility. Consider, for example, the case for role interchangeability and onymity down from $I_A$. By Proposition 7.1 and the trivial incompatibility between role interchangeability and role noninterchangeability, role interchangeability and onymity down from $I_A$ are incompatible as long as we assume that $I_A$ is the set of agents that perform some action in every run. Note that they are compatible if we abandon the assumption, that is, if we allow some $i' \in I_A$ such that $i'$ never performs any action in some run.

We can see that some weak forms of anonymity are compatible with some weak forms of onymity.

**Claim 9.1.** Every pair of properties marked $\oplus$ in Table 1 is a compatible pair.

*Proof.* Consider the interpreted system $\mathcal{I}_1$ described in Fig. 4. This system consists of four runs, and here we assume that $(r, m) \sim_j (r', m') \sim_j (r'', m'') \sim_j (r''', m''')$ and $I_A = \{i, i', i''\}$. The primitive propositions that are true in each run are also described. In this system, $a$ performed by $i$ is minimally anonymous as well as onymous down from $I_A$ with respect to $j$, and $\theta(i, a)$ is true at $(r, m)$. In view of Proposition 7.1, we can also see that $\mathcal{I}_1$ is an example of a role noninterchangeable system.

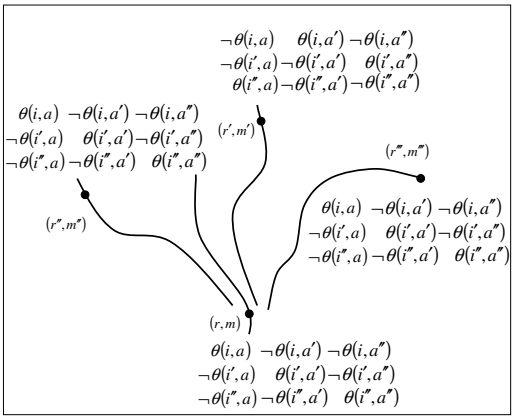


Figure 4: Minimally anonymous but onymous down from $I_A$ system $\mathcal{I}_1$

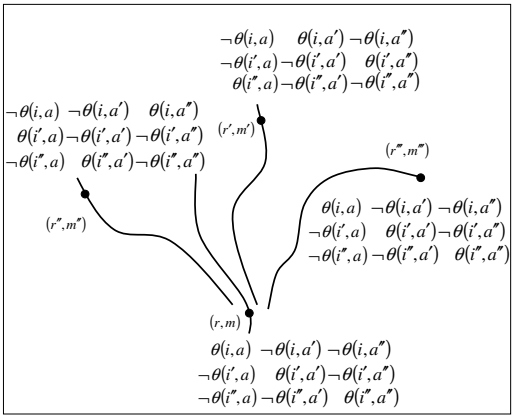


Figure 5: Anonymous up to $I_A$ but role noninterchangeable system $\mathcal{I}_2$

Also consider the interpreted system $\mathcal{I}_2$ described in Fig. 5. This system only differs from $\mathcal{I}_1$ in having a different set of primitive propositions that are true at $(r'', m'')$. It is easy to see that this is an example of a system that is anonymous up to $I_A$ but role noninterchangeable. In view of Proposition 3.1, we can also see that $a$ performed by $i$ is minimally anonymous with respect to $j$ in $\mathcal{I}_2$. □

**Example 9.1.** To see more intuitively what the system $\mathcal{I}_1$ described in Fig. 4 represents, assume that $I_A = \{i, i', i''\}$ denotes a set of voters, let $a$, $a'$, and $a''$ be $vote(k)$, $vote(k')$, and $vote(k'')$, respectively, and suppose that the intended interpretation of $\theta(i, vote(k))$ is that a voter $i$ voted for a candidate $k$. Then, the minimally anonymous but onymous down from $I_A$ system $\mathcal{I}_1$ indicates that from the observer $j$'s viewpoint, $i$ could not have voted for $k$ but some other voter in $I_A$, specifically, $i'$, has never voted for $k$.

**Remark 9.1.** In Table 1, we state that anonymity up to $I_A$ and onymity down from $I_A$ are incompatible for each same set $I_A$. However, for different anonymity/onymity sets, they could be compatible. For example, it is possible to state both that everyone in $I_A$ might have performed $a$ and that $a$ is known to not have been performed by anyone in ${I_A}' - I_A$, where $I_A$ is a proper subset of ${I_A}'$. In this case, $a$ performed by $i$ is anonymous up to $I_A$ and onymous down from ${I_A}'$.

# 10 Discussion

## 10.1 Comparison with the Work of Pfitzmann and Hansen

One of the main differences between our proposal and the standard terminology proposed by Pfitzmann and Hansen [30, 29] is that our approach is formal whereas theirs is consistent but informal. A more important, technical difference between them is the (non)existence of the subject/object reversal duality. By this duality, we can refine anonymity and privacy from the category of privacy-related information-hiding properties. This view of refinement was explained in Examples 3.1 and 5.1, where the definition of sender anonymity given in [30] was analyzed and refined into what we call sender anonymity and message

Table 2: Correspondence between Pfitzmann-Hansen's [29] and Our Concepts

| Pfitzmann-Hansen [29] | This Paper |
|---|---|
| Anonymity | Anonymity up to $I_A$ |
| Anonymity set | Anonymity set $I_A$ |
| N/a | Privacy up to $A_I$ |
| N/a | Privacy set $A_I$ |
| Identifiability | Onymity down from $I_A$ |
| Identifiability set | Onymity set $I_A$ |
| Disclosure of a partial (PH-)identity | Identity down from $A_I$ |
| Set of partial (PH-)identities | Identity set $A_I$ |

privacy. (Similar examples can also be found in Examples 4.2 and 5.3, where a refinement into voter anonymity and vote privacy is explained.) In newer versions including [29], Pfitzmann and Hansen redefined anonymity in a more succinct manner, so that it coincides with what we call anonymity up to a certain anonymity set; however, its dual, that is, privacy up to a privacy set, was beyond the scope of their formulation (Table 2).

Similarly, by this duality, we can also distinguish onymity and identity in the category of identity-related information-disclosure properties. As Remarks 6.1 and 8.1 show, our concepts of onymity and identity are related to those that Pfitzmann and Hansen defined in their consolidated terminology paper [29]. Specifically, onymity, that is, the disclosure of who, corresponds to identifiability and its dual, identity, means the disclosure of a partial PH-identity (Table 2). Thus, our duality viewpoint is also helpful in understanding the structure of the identity category.

On the other hand, several important privacy-related properties dealt with in [30, 29] have not been discussed in our framework. These include *unlinkability*, *undetectability*, *unobservability*, and *pseudonymity*. Although a general logical treatment of these properties is important future work, below we simply provide some observations with respect to unlinkability.

## 10.2 Unlinkability

In [29], Pfitzmann and Hansen stipulated that "unlinkability of two or more items of interest (e.g., subjects, messages, and actions) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these items of interest are related or not." As an immediate remark, they also explained that unlinkability might be a more "fine-grained" property than anonymity, since unlinkability might be concerned with relations between various types of items whereas anonymity is simply concerned with relationships between specific types of items, that is, between agents and actions. Considering that our built-in primitive proposition $\theta(i, a)$ can be regarded as expressing a specific form of "link" between $i$ and $a$, we will here focus on the unlinkability of this specific form.

Our first observation is that minimal anonymity (or equivalently, minimal privacy) is close to the unlinkability property stipulated by Pfitzmann and Hansen. Minimal anonymity, like unlinkability, is fundamental, as Halpern and O'Neill mentioned in [14], where they stated that the definition of minimal anonymity "illustrates the basic intuition behind any definition of anonymity." Technically, Definition 3.1 states that minimal anonymity $\mathcal{I} \models \theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$ means that for every $(r, m)$ such that $(\mathcal{I}, r, m) \models \theta(i, a)$, there exists some $(r', m')$ such that $(\mathcal{I}, r', m') \models \neg\theta(i, a)$ and $(r', m') \sim_j (r, m)$. In other words, minimal anonymity roughly means that the attacker $j$ cannot sufficiently distinguish a point $(r, m)$ where $i$ and $a$ are related (that is, $(\mathcal{I}, r, m) \models \theta(i, a)$ holds) from another point $(r', m')$

where $i$ and $a$ are not related (that is, $(\mathcal{I}, r', m') \models \neg\theta(i, a)$ holds). We can see that this interpretation of minimal anonymity is close to the stipulation of unlinkability provided by Pfitzmann and Hansen.

In a similar but stronger form of this approach, Garcia *et al.* [13] gave a formal definition of unlinkability between a sender $i$ and a message $m$ from an attacker $j$'s viewpoint. Their definition can be paraphrased in our formalism as follows:

$$\mathcal{I} \models \theta(i, send(m)) \Rightarrow (P_j[\neg\theta(i, send(m))] \wedge \bigwedge_{i' \in I_A} P_j[\theta(i', send(m))]).$$

In other words, they defined unlinkability as the conjunction of minimal anonymity and anonymity up to a certain anonymity set. The latter conjunct can be used to exclude the case where $j$ does know that $i$ does not send $m$. (As shown in Proposition 3.1, the latter conjunct can also imply the former, provided that certain conditions are satisfied.)

The above observation can be extended from the duality/contrary view of our taxonomy. For example, we can say that the contrary of minimal anonymity, that is, maximal onymity (or equivalently, maximal identity), is close to linkability. We can also consider the dual of Garcia *et al.*'s formulation, which means the unlinkability property on the privacy side.

As a final remark in this subsection, we note that role interchangeability also refers to a property related to unlinkability. This is because role interchangeability can be roughly interpreted as meaning that the attacker $j$ cannot sufficiently distinguish a point $(r, m)$ where two "links" are present (that is, $(\mathcal{I}, r, m) \models \theta(i, a)$ and $(\mathcal{I}, r, m) \models \theta(i', a')$ hold) from another point $(r', m')$ where the two "links" are interchanged (that is, $(\mathcal{I}, r', m') \models \theta(i', a)$ and $(\mathcal{I}, r', m') \models \theta(i, a')$ hold). However, as we see above, it is minimal anonymity (and equivalently, minimal privacy) that closely corresponds to the unlinkability property stipulated by Pfitzmann and Hansen. Further, our formal framework shows that role interchangeability conditionally implies minimal anonymity (Propositions 4.2 and 5.3). To sum up, building on our formal framework, we can say that role interchangeability is related to but stronger than unlinkability.

## 10.3 Onymity/Identity versus Authentication/Non-Repudiation

The classification and analysis of real-world examples based on our taxonomy are important. So far, however, our intensive case study [27] of real protocols has only treated anonymity and privacy. With respect to onymity and identity, authentication and non-repudiation protocols will be relevant examples to be discussed.

Indeed, onymity is closely related to (personal) *authentication* because it is the property of disclosing who. Similarly, identity is closely related to *attribute authentication*. Consider a set of runs of a certain authentication protocol where $i$ is the initiator and $j$ the responder. Further, suppose that $\theta(i, says(m))$ and $\theta(j, says(n))$ respectively mean that $i$ says an initiating message $m$ and that $j$ says a responding message $n$. Then, the mutual authentication property of the protocol seems to be expressed as the maximal onymity of the action $says(m)$ performed by $i$ with respect to $j$ and the maximal onymity of the action $says(n)$ performed by $j$ with respect to $i$.

*Non-repudiation* can be regarded as a variant of authentication. Non-repudiation of origin (NRO) is the property that protects against the originator's false denial of having sent a specific message, and non-repudiation of receipt (NRR) is the property that protects against the recipient's false denial of having received the specific message. NRO and NRR have been formulated in the literature in the form of maximal onymity, or equivalently, maximal identity. For example, in [41, 42], Zhou and Gollmann used a BAN ([4, 7])-like logic, the SVO

logic [34], to specify and verify NRO and NRR of a certain fair non-repudiation protocol. Their specifications of NRO and NRR can be paraphrased, in the form of maximal identity, as

$$\theta(i, says(m)) \Rightarrow K_k[\theta(i, says(m))]$$

and

$$\theta(j, sees(m)) \Rightarrow K_k[\theta(j, sees(m))],$$

respectively. Here, we assume that $i$, $j$, and $k$ are the originator, the recipient, and the judge, respectively.

The above discussion is intended to explain that our formulation of maximal onymity/identity is closely related to authentication and non-repudiation. However, this explanation is still informal and needs further elaboration. Some additional discussions are offered below.

We first observe that maximal onymity $\mathcal{I} \models \theta(i,a) \Rightarrow K_j[\theta(i,a)]$ means, by definition, that for every $(r,m)$ such that $(\mathcal{I},r,m) \models \theta(i,a)$ and for every $(r',m')$ such that $(\mathcal{I},r',m') \models \neg\theta(i,a)$, $(r',m') \not\sim_j (r,m)$. In other words, from an algorithmic or computational viewpoint, maximal onymity means that $j$ can distinguish such $(r,m)$ and $(r',m')$ with "non-negligible" probability. This contrasts with the ordinary authentication property that requires $j$ to distinguish such $(r,m)$ and $(r',m')$ with "overwhelming" probability.

On the basis of this observation, we could say that authentication requires more than maximal onymity, and we could provide an alternative, stronger definition of maximal onymity as

$$\mathcal{I} \models \theta(i,a) \Rightarrow K_j^+[\theta(i,a)].$$

Here, $(\mathcal{I},r,m) \models K_j^+[\theta(i,a)]$ means that $(\mathcal{I},r',m') \models \theta(i,a)$ for every $(r',m')$ such that $\neg((r',m') \nsim_j (r,m))$, where $\nsim_j$ denotes a "strong" distinguishability that corresponds to the distinguishability with "overwhelming" probability mentioned above and should be additionally introduced into our multiagent systems. Note that $(r',m') \sim_j (r,m)$ should imply $\neg((r',m') \nsim_j (r,m))$, but the converse of this would not necessarily hold. Thus, the new form of maximal onymity means that for every $(r,m)$ such that $(\mathcal{I},r,m) \models \theta(i,a)$ and for every $(r',m')$ such that $(\mathcal{I},r',m') \models \neg\theta(i,a)$, $(r',m') \nsim_j (r,m)$. In other words, from a computational viewpoint again, this maximal onymity means that $j$ can distinguish such $(r,m)$ and $(r',m')$ with "overwhelming" probability. This seems to be closer to the ordinary authentication property. We are thus led to an alternative taxonomy framework by replacing all explicit occurrences of $K$ in Fig. 3 with $K^+$.

# 11 Conclusion

In this paper, we have proposed a novel taxonomy of privacy-related information-hiding/disclosure properties in information systems. Specifically, we have formulated anonymity, privacy, onymity, and identity in terms of the modal logic of knowledge for multiagent systems and have investigated their logical relationship. In particular, we have shown that some weak forms of anonymity and privacy are compatible with some weak forms of onymity and identity, respectively. Furthermore, we have discussed the relationships between our taxonomy and existing standard terminology. We believe that these results contribute to a better understanding of logical foundations for privacy and related concepts.

Of course, there are a number of issues that should be worked out. In addition to the points raised in Sect. 10, the following are considered particularly important. First, our approach based on logic can be regarded as "qualitative." In contrast to this, "quantitative" approaches have also been reported. Typically, the size of an anonymity set or a privacy set can give the measure of anonymity or privacy. Furthermore, there is also a well-known, information-theoretic approach using the concept of entropy [10, 32]. It is interesting to study how these approaches differ and how they can be combined. Second, formal analysis in a compositional setting should constitute interesting future work. In general, each information system consists of several subsystems. If some subsystems have anonymity properties and some others privacy properties, then there is some question as to how we can infer that the total system has a certain anonymity or privacy property. Or, more complicatedly, the system may possibly consist of a variety of subsystems that have various degrees of anonymity, privacy, onymity, or identity properties. Our framework might be useful for reasoning about properties in such compositional cases.

In closing, we should note that different views of privacy-related properties can be found in the literature. For example, Weitzner *et al.* proposed an *information-accountability* perspective on privacy [40]. They mentioned that privacy is the claim of individuals, groups, and institutions to determine for themselves when, how, and to what extent information about them is used lawfully and appropriately by others. This contrasts with our view of privacy as an instance of *information-hiding* properties. The information-accountability perspective would produce a different picture of privacy-related properties. This is also a future direction for research.

## Acknowledgements

We thank our colleagues, Koji Chida, Akiko Fujimura, Kunihiko Fujita, Eisaku Maeda, Yoshifumi Manabe, and Kenji Takahashi, for their valuable comments on earlier versions of this work. We are also grateful to the anonymous referees for their constructive criticism and suggestions.

## References

[1] Abadi, M., Fournet, C.: Private authentication. *Theoret. Comput. Sci.* **322**(3) (2004) 427–476.

[2] Backes, M., Hritcu, C., Maffei, M.: Automated verification of remote electronic voting protocols in the applied pi-calculus. In *Proc. 21st IEEE CSF* (2008) 195–209.

[3] Baskar, A., Ramanujam, R., Suresh, S. P.: Knowledge-based modelling of voting protocols. In *Proc. TARK'07* (2007) 62–71.

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

[5] Chadha, R., Delaune, S., Kremer, S.: Epistemic logic for the applied pi calculus. In *Proc. FMOODS/FORTE'09*, Springer LNCS, Vol. 5522 (2009) 182–197.

[6] Chaum, D., van Heyst, E.: Group signatures. In *Proc. Eurocrypt'91*, Springer LNCS, Vol. 547 (1991) 257–265.

[7] Cohen, M., Dam, M.: A completeness result for BAN logic. *J. Logic, Language and Inform.* (to appear).

[8] Delaune, S., Kremer, S., Ryan, M.: Coercion-resistance and receipt-freeness in electronic voting. In *Proc. 19th IEEE CSFW* (2006) 28–42.

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

[10] Díaz, C., Seys, S., Claessens, J., Preneel, B.: Towards measuring anonymity. In *Proc. PET'02*, Springer LNCS, Vol. 2482 (2002) 54–68.

[11] Fagin, R., Halpern, J. Y., Moses, Y., Vardi, M. Y.: *Reasoning About Knowledge*. The MIT Press (1995).

[12] Fujioka, A., Okamoto, T., Ohta, K.: A practical secret voting scheme for large scale elections. In *Proc. AUSCRYPT'92*, Springer LNCS, Vol. 718 (1993) 244–251.

[13] Garcia, F. D., Hasuo, I., Pieters, W., van Rossum, P.: Provable anonymity. In *Proc. ACM FMSE'05* (2005) 63–72.

[14] Halpern, J. Y., O'Neill, K. R.: Anonymity and information hiding in multiagent systems. *J. Comput. Security* **13**(3) (2005) 483–512.

[15] Hasuo, I., Kawabe, Y.: Probabilistic anonymity via coalgebraic simulations. In *Proc. ESOP'07*, Springer LNCS, Vol. 4421 (2007) 379–394.

[16] Hevia, A., Micciancio, D.: An indistinguishability-based characterization of anonymous channels. In *Proc. PETS'08*, Springer LNCS, Vol. 5134 (2008) 24–43.

[17] Hogben, G., Wilikens, M., Vakalis, I.: On the ontology of digital identification. In *Proc. OTM 2003 Workshops*, Springer LNCS, Vol. 2889 (2003) 579–593.

[18] Hughes, D., Shmatikov, V.: Information hiding, anonymity and privacy: a modular approach. *J. Comput. Security* **12**(1) (2004) 3–36.

[19] Jonker, H., Mauw, S., Pang, J.: Measuring voter-controlled privacy. In *Proc. ARES'09* (2009) 289–298.

[20] Jonker, H., Pieters, W.: Receipt-freeness as a special case of anonymity in epistemic logic. In *WOTE'06* (2006).

[21] Kawabe, Y., Mano, K., Sakurada, H., Tsukada, Y.: Backward simulations for anonymity. In *Proc. Sixth IFIP WG 1.7 WITS* (2006) 206–220.

[22] Kawabe, Y., Mano, K., Sakurada, H., Tsukada, Y.: Theorem-proving anonymity of infinite-state systems. *Inform. Process. Lett.* **101**(1) (2007) 46–51.

[23] Kawabe, Y., Mano, K., Sakurada, H., Tsukada, Y.: On backward-style anonymity verification. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.* **E91-A**(9) (2008) 2597–2606.

[24] Kelly, D.: *A Taxonomy for and Analysis of Anonymous Communications Networks*. Ph. D. Thesis, Air Force Institute of Technology (2009).

[25] Kremer, S., Ryan, M.: Analysis of an electronic voting protocol in the applied pi calculus. In *Proc. ESOP'05*, Springer LNCS, Vol. 3444 (2005) 186–200.

[26] Küsters, R., Truderung, T.: An epistemic approach to coercion-resistance for electronic voting protocols. In *Proc. IEEE S&P'09* (2009) 251–266.

[27] Mano, K., Kawabe, Y., Sakurada, H., Tsukada, Y.: Role interchange for anonymity and privacy of voting. *J. Logic and Comput.* (in press). doi:10.1093/logcom/exq013

[28] Mauw, S., Verschuren, J., de Vink, E. P.: Data anonymity in the FOO voting scheme. In *Proc. VODCA'06*, ENTCS, Vol. 168 (2007) 5–28.

[29] Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management (Ver. v0.34) (2010).

[30] Pfitzmann, A., Köhntopp, M.: Anonymity, unobservability, and pseudonymity—A proposal for terminology. In *Designing Privacy Enhancing Technologies*, Springer LNCS, Vol. 2009 (2001) 1–9.

[31] Schneider, S., Sidiropoulos, A.: CSP and anonymity. In *Proc. ESORICS'96*, Springer LNCS, Vol. 1146 (1996) 198–218.

[32] Serjantov, A., Danezis, G.: Towards an information theoretic metric for anonymity. In *Proc. PET'02*, Springer LNCS, Vol. 2482 (2002) 41–53.

[33] Solove, D. J.: A taxonomy of privacy. *University of Pennsylvania Law Review* **154**(3) (2006) 477–560.

[34] Syverson, P. F., van Oorschot, P. C.: On unifying some cryptographic protocol logics. In *Proc. IEEE S&P'94* (1994) 14–28.

[35] Syverson, P. F., Stubblebine, S. G.: Group principals and the formalization of anonymity. In *Proc. FM'99*, Springer LNCS, Vol. 1708 (1999) 814–833.

[36] Tsukada, Y., Mano, K., Sakurada, H., Kawabe, Y.: Anonymity, privacy, onymity, and identity: A modal logic approach. In *Proc. IEEE PASSAT'09* (2009) 42–51.

[37] van der Meyden, R., Su, K.: Symbolic model checking the knowledge of the dining cryptographers. In *Proc. 17th IEEE CSFW* (2004) 280–291.

[38] van der Meyden, R., Wilke, T.: Preservation of epistemic properties in security protocol implementations. In *Proc. TARK'07* (2007) 212–221.

[39] van Eijck, J., Orzan, S.: Epistemic verification of anonymity. In *Proc. VODCA'06*, ENTCS, Vol. 168 (2007) 159–174.

[40] Weitzner, D. J., Abelson, H., Berners-Lee, T., Feigenbaum, J., Hendler, J., Sussman, G. J.: Information accountability. *Commun. ACM* **51**(6) (2008) 82–87.

[41] Zhou, J., Gollmann, D.: A fair non-repudiation protocol. In *Proc. IEEE S&P'96* (1996) 55–61.

[42] Zhou, J., Gollmann, D.: Towards verification of non-repudiation protocols. In *Proc. IRW/FMP'98*, Springer DMTCS (1998) 370–380.