ANONYMITY, UNLINKABILITY, UNDETECTABILITY, UNOBSERVABILITY, PSEUDONYMITY, AND IDENTITY MANAGEMENT

– A CONSOLIDATED PROPOSAL FOR TERMINOLOGY

Andreas Pfitzmann and
Marit Hansen
Version v0.31, Feb. 15, 2008

Fall 2009

Presented by Shirin Nilizadeh

Outline

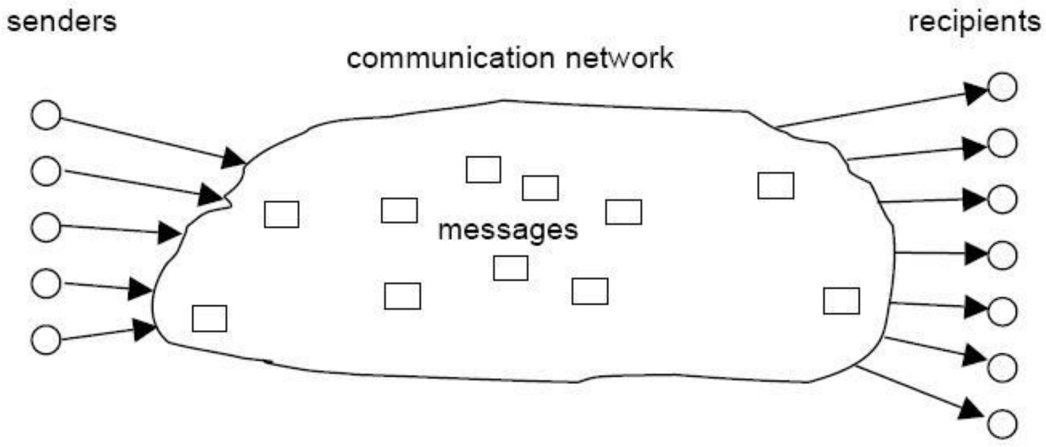
- Introduction and Setting
- Definitions of anonymity, unlinkability, undetectability, and unobservability
- Relationships between these terms
- Known mechanisms
- Pseudonymity
  - Properties and Known mechanisms of pseudonyms
- Identity management
- Overview

Introduction

- Goal: show relationships between the anonymity, … terms and develop a consistent terminology.

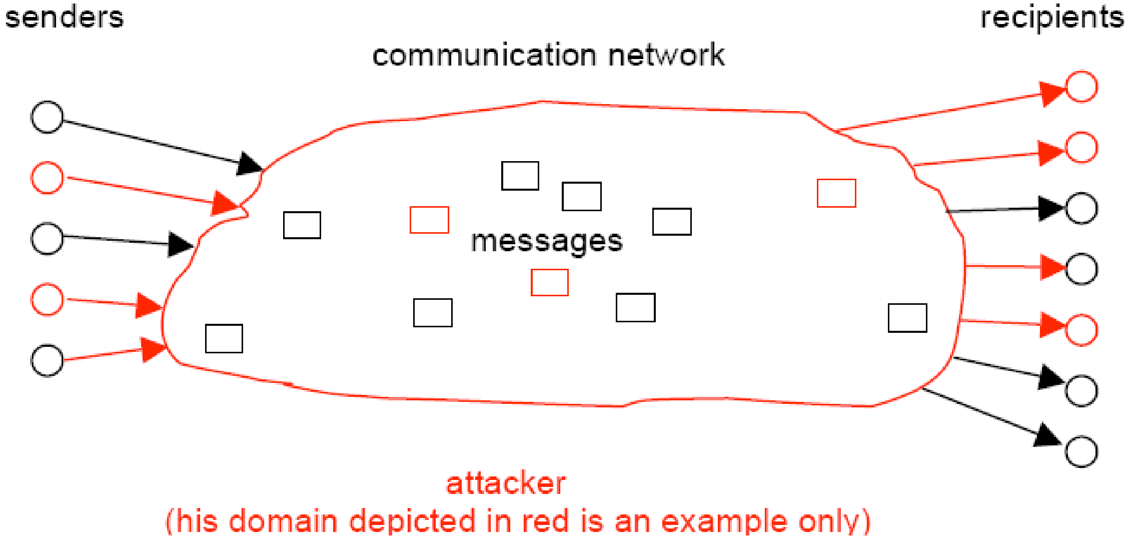
Setting:

- Senders send messages to recipients using a communication network.
- A *subject (Sender/ Receiver)*: *a human being*, a legal person, or a computer.
- Setting >> System
  - has a surrounding
  - The state of the system may change by actions within the system.



Setting: Attacker

- Outsider/ insider
- Uses all information to infer *items of interests (IOIs)*.
    - Attributes may be *IOIs*/ Attributes' observation may give information on IOIs.
- Attacker is not able to get information from the message content.
- The knowledge of the attacker only increases.

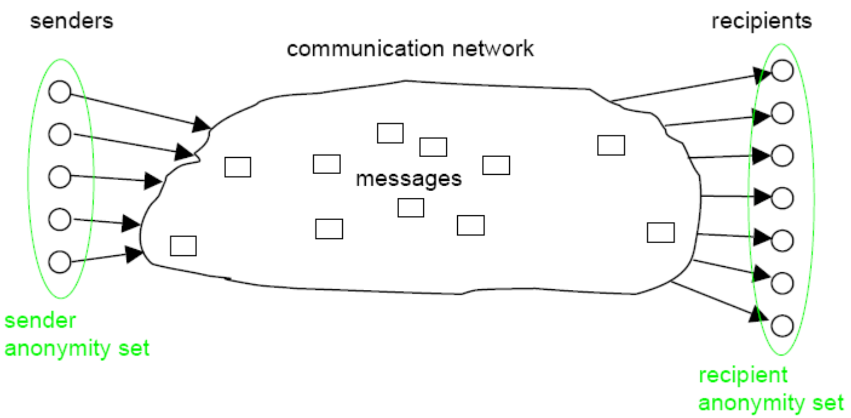


Anonymity

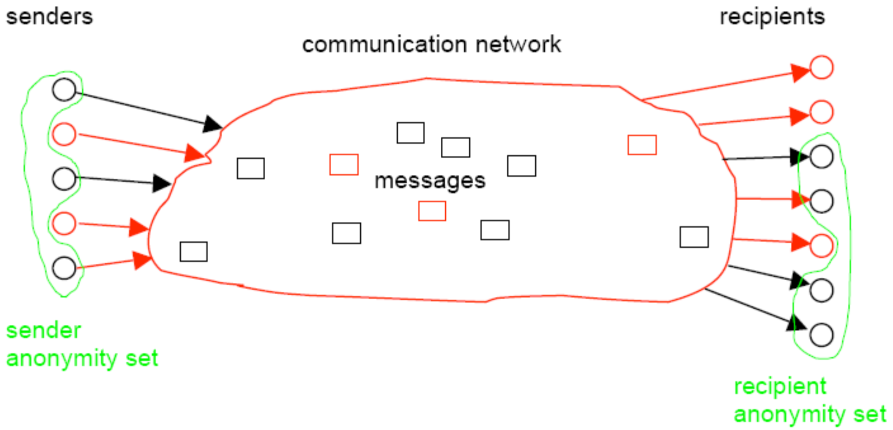
1. *Anonymity of a subject means that the subject is not identifiable within a set of subjects, the anonymity set.*

>> Defines a binary property! >> need quantify anonymity & underlining that all statements are made from the perspective of an attacker

2. *Anonymity of a subject from an attacker's perspective means that the attacker cannot* sufficiently identify the subject within a set of subjects, the *anonymity set.*



largest possible anonymity sets



largest possible anonymity sets w.r.t. attacker

Anonymity (2)

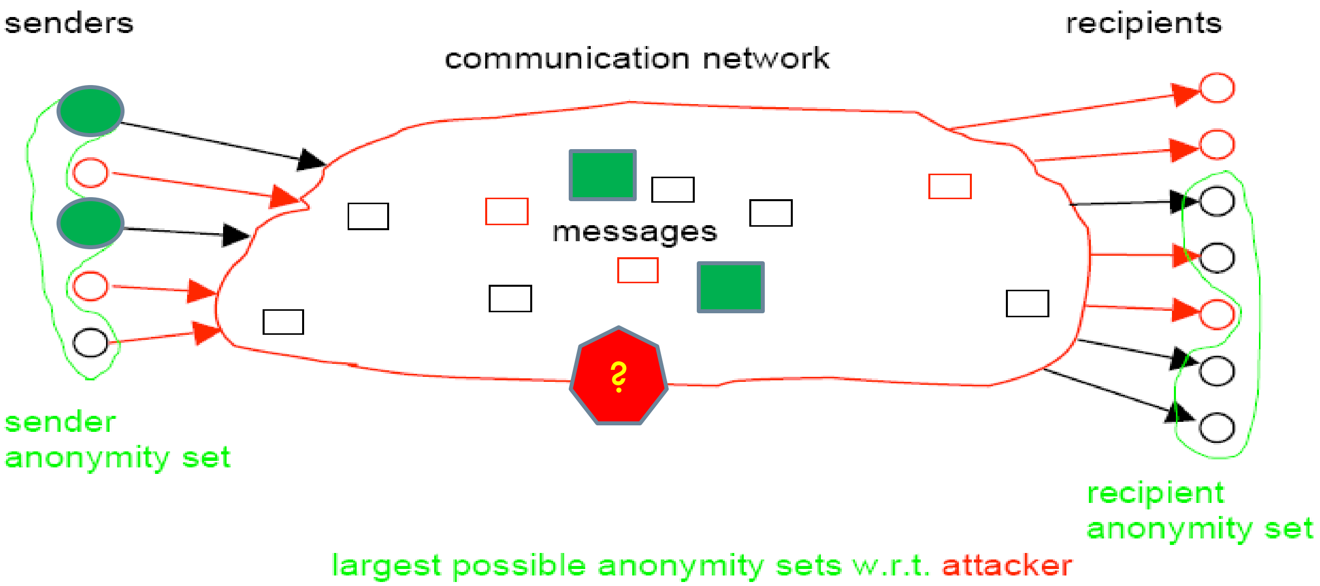
- *Individual anonymity and global anonymity*
- Global anonymity is the stronger, the larger the respective anonymity set is.
- *Global anonymity is maximal iff all* subjects within the anonymity set are equally likely. >> impossible!
- Strong global anonymity does not imply strong individual anonymity.

- Another aspect of anonymity: *Robustness of anonymity:* how stable the quantity of anonymity is against changes in the particular setting.

3. ***An anonymity delta (regarding a subject's anonymity) from an attacker's perspective specifies the difference between the subject's anonymity taking into account the attacker's observations (i.e., the attacker's a-posteriori knowledge) and the subject's anonymity given the attacker's a-priori knowledge only.***

Unlinkability

1. **Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.**



Unlinkability (2)

2. ***An unlinkability delta of two or more items of interest (IOIs, e.g., subjects, messages,* actions, …) from an attacker's perspective specifies the difference between the unlinkability of these IOIs taking into account the attacker's observations and the unlinkability of these IOIs given the attacker's a-priori knowledge only.**

- The same as anonymity the unlinkability cannot increase.
- The unlinkability delta the same as Anonymity delta can never be positive.

Anonymity in terms of unlinkability

- Consider sending and receiving of messages as attributes; the items of interest (IOIs) are “who has sent or received which message”.

- *Anonymity of a subject w.r.t. an attribute may be defined as unlinkability of this subject and this* attribute.

- *Sender anonymity of a subject means that to this potentially sending subject, each* message is unlinkable.
- *Recipient anonymity of a subject means that to this potentially receiving subject,* each message is unlinkable.
- *Relationship anonymity of a pair of subjects, the potentially sending subject and the potentially* receiving subject, means that to this potentially communicating pair of subjects, each message is unlinkable.

Undetectability

- In undetectability, the IOIs are protected not its relationship to subjects or other IOIs.

1. ***Undetectability of an item of interest (IOI) from an attacker's perspective means that the* attacker cannot sufficiently distinguish whether it exists or not.**

- This means that messages are not sufficiently distinguishable from "random noise".

2. ***An undetectability delta of an item of interest (IOI) from an attacker's perspective* specifies the difference between the undetectability of the IOI taking into account the attacker's observations and the undetectability of the IOI given the attacker's a-priori knowledge only.**

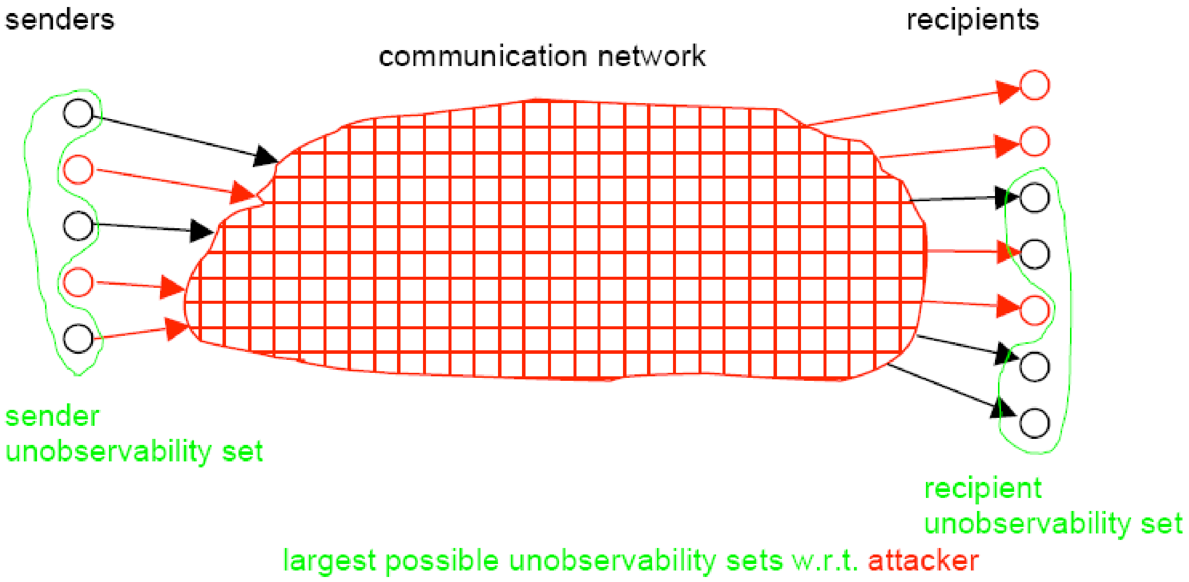
- The definition of undetectability has nothing to do with anonymity – it does not mention any relationship between IOIs and subjects.

Unobservability

1. **Unobservability of an item of interest (IOI) means**
   - **Undetectability of the IOI against all subjects uninvolved in it.**
   - **Anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.**

- Unobservability ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

Unobservability (2)



senders

communication network

recipients

sender
unobservability set

recipient
unobservability set

largest possible unobservability sets w.r.t. attacker

2. **An unobservability delta of an item of interest (IOI) means**
   - □ **Undetectability delta of the IOI against all subjects uninvolved in it.**
   - □ **Anonymity delta of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.**

□ Unobservability cannot increase. The unobservability delta can never be positive.

Relationships between terms

- (⇒ reads “implies”)

- unobservability ⇒ anonymity
- sender unobservability ⇒ sender anonymity
- recipient unobservability ⇒ recipient anonymity
- relationship unobservability ⇒ relationship anonymity

- sender anonymity ⇒ relationship anonymity
- recipient anonymity ⇒ relationship anonymity
- sender unobservability ⇒ relationship unobservability
- recipient unobservability ⇒ relationship unobservability

- unobservability ⇒ undetectability

Known mechanisms

- DC-net [Chau85, Chau88] and MIX-net [Chau81] >> sender anonymity and relationship anonymity

  + dummy traffic >> unobservability!

- Broadcast [Chau85, PfWa86, Waid90] and private information retrieval [CoBi95] >> recipient anonymity

  + dummy traffic >> recipient unobservability!

- dummy traffic alone makes the message undetectable.

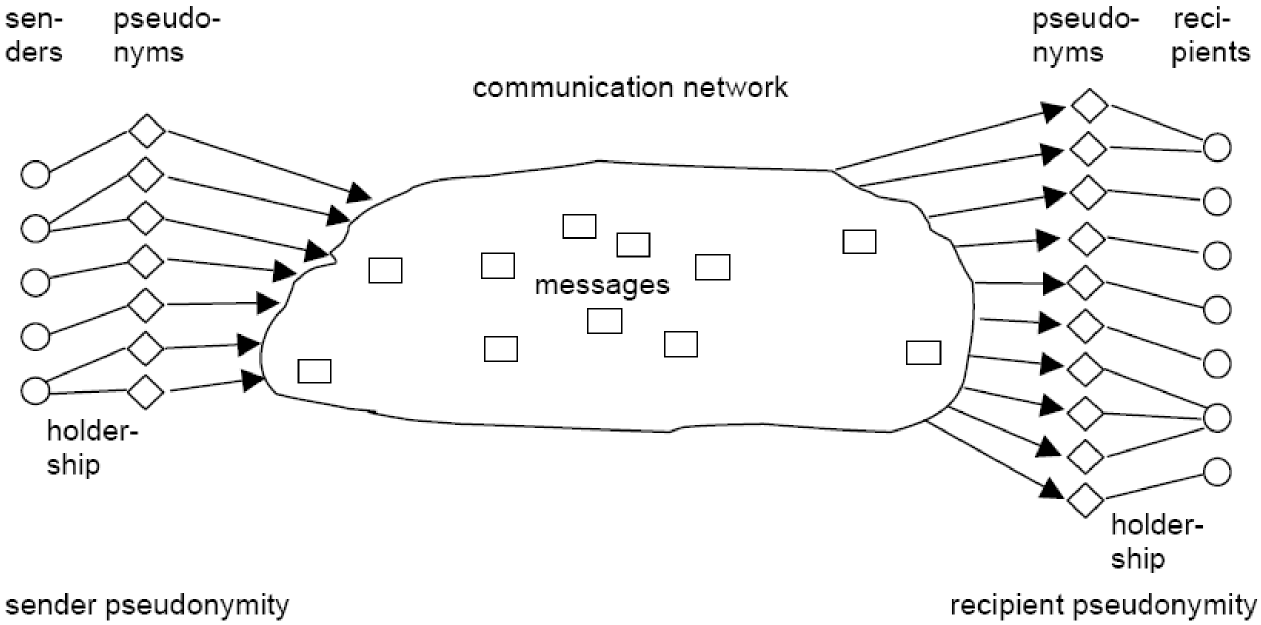
Pseudonymity

- Many applications need appropriate kinds of identifiers.

- ***A pseudonym is an identifier of a subject other than one of the subject's real names.***
- ***The subject which the pseudonym refers to is the holder of the pseudonym.***
- ***A subject is pseudonymous if a pseudonym is used as identifier instead of one of its real names.***
- ***Pseudonymity is the use of pseudonyms as identifiers.***

Pseudonymity (2)

- Assumption: Each pseudonym refers to exactly one specific holder.
- A *group pseudonym refers to a set of* holders.
- A *transferable pseudonym is transferred from* one holder to another subject becoming its holder.
- >> both of them induce an anonymity set.



Pseudonymity with respect to accountability and authorization

- Digital pseudonyms to authenticate messages
- A *digital pseudonym:*
  - Unique as identifier,
  - Used to authenticate the holder's IOIs

- To authenticate IOIs relative to pseudonyms usually is not enough to achieve accountability for IOIs.
  - Attach funds to digital pseudonyms to cover claims,
  - Let identity brokers authenticate digital pseudonyms,
  - both.

Pseudonymity with respect to linkability

- Ongoing use of the same pseudonym allows the holder to establish a reputation.

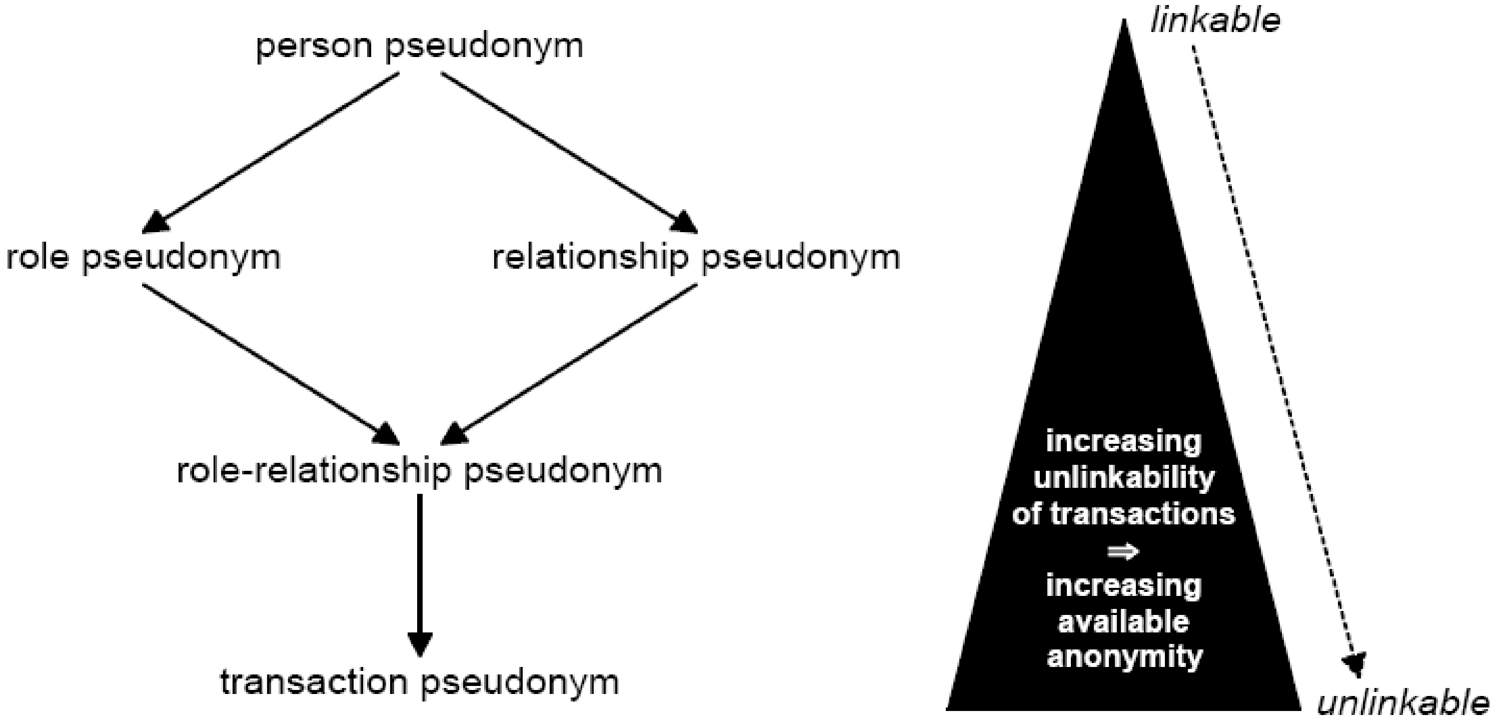
- Some kinds of pseudonyms enable dealing with claims in case of abuse of unlinkability to holders:
  - Identity brokers may have the possibility to reveal the civil identity of the holder in order to provide means for investigation.
  - Third parties may act as liability brokers of the holder to clear a debt or settle a claim.

Typical kinds of pseudonyms are:

- *public pseudonym.*
  - The linking between a public pseudonym and its holder may be publicly known even from the very beginning.
- *initially non-public pseudonym.*
  - The linking between an initially non-public pseudonym and its holder may be known by certain parties, but is not public at least initially.
- *initially unlinked pseudonym.*
  - The linking between an initially unlinked pseudonym and its holder is – at least initially – not known to anybody.
- The strength of anonymity decreases with increasing knowledge of the pseudonym linking.

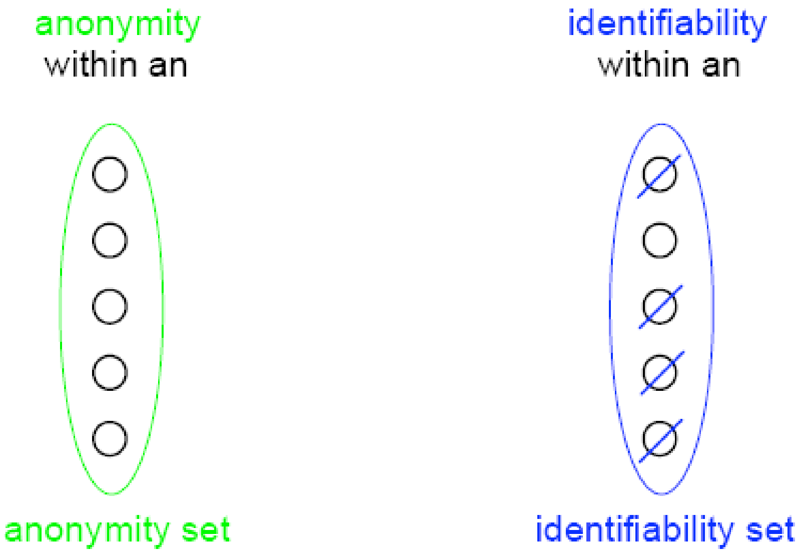
Lattice of pseudonyms according to their use in different contexts:

- A → B stands for “B enables stronger anonymity than A”.


person pseudonym
role pseudonym
relationship pseudonym
role-relationship pseudonym
transaction pseudonym
linkable
increasing unlinkability of transactions
⇒
increasing available anonymity
unlinkable

Identity management

- ***Identifiability of a subject from an attacker’s perspective means that the attacker can*** **sufficiently identify the subject within a set of subjects, the** ***identifiability set.***
- Anonymity is the stronger, the smaller the respective identifiability set is.
- **An** ***identity is any subset of attributes of an individual person which sufficiently*** **identifies this individual person within any set of persons. So usually there is no such thing as “the identity”, but several of them.**



Identity-related terms

- ***Role***: a set of connected actions.

- ***Partial identity***: each *partial identity* represents the person in a specific context or role.

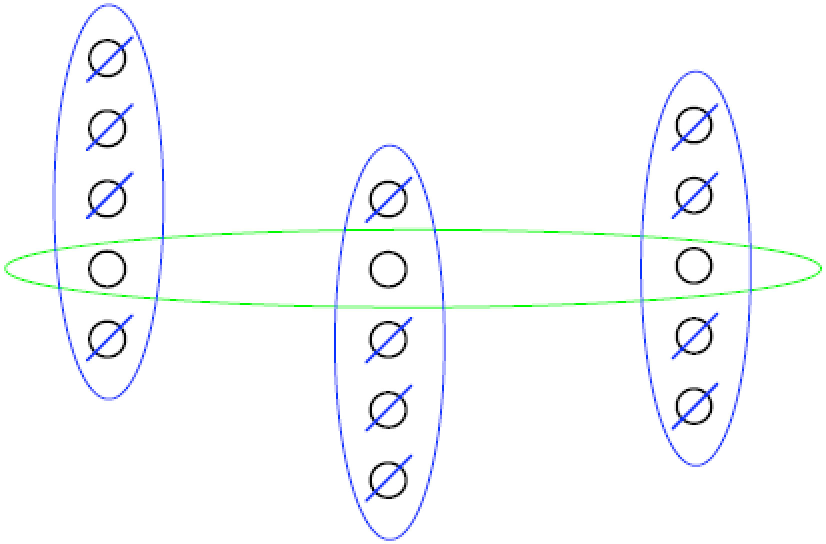
- A *pseudonym might be an identifier for a partial identity.*

- ***Digital identity***: denotes attribution of attributes to an individual person, which are immediately operationally accessible by technical means.

- ***Virtual identity***: The same meaning as digital identity, is mainly applied to characters in a MUD, MMORPG or to avatars.

Relation between anonymity set and identifiability set

- Anonymity set of a partial identity given that the set of all possible subjects can be partitioned into the three disjoint identifiability sets of the partial identity shown.



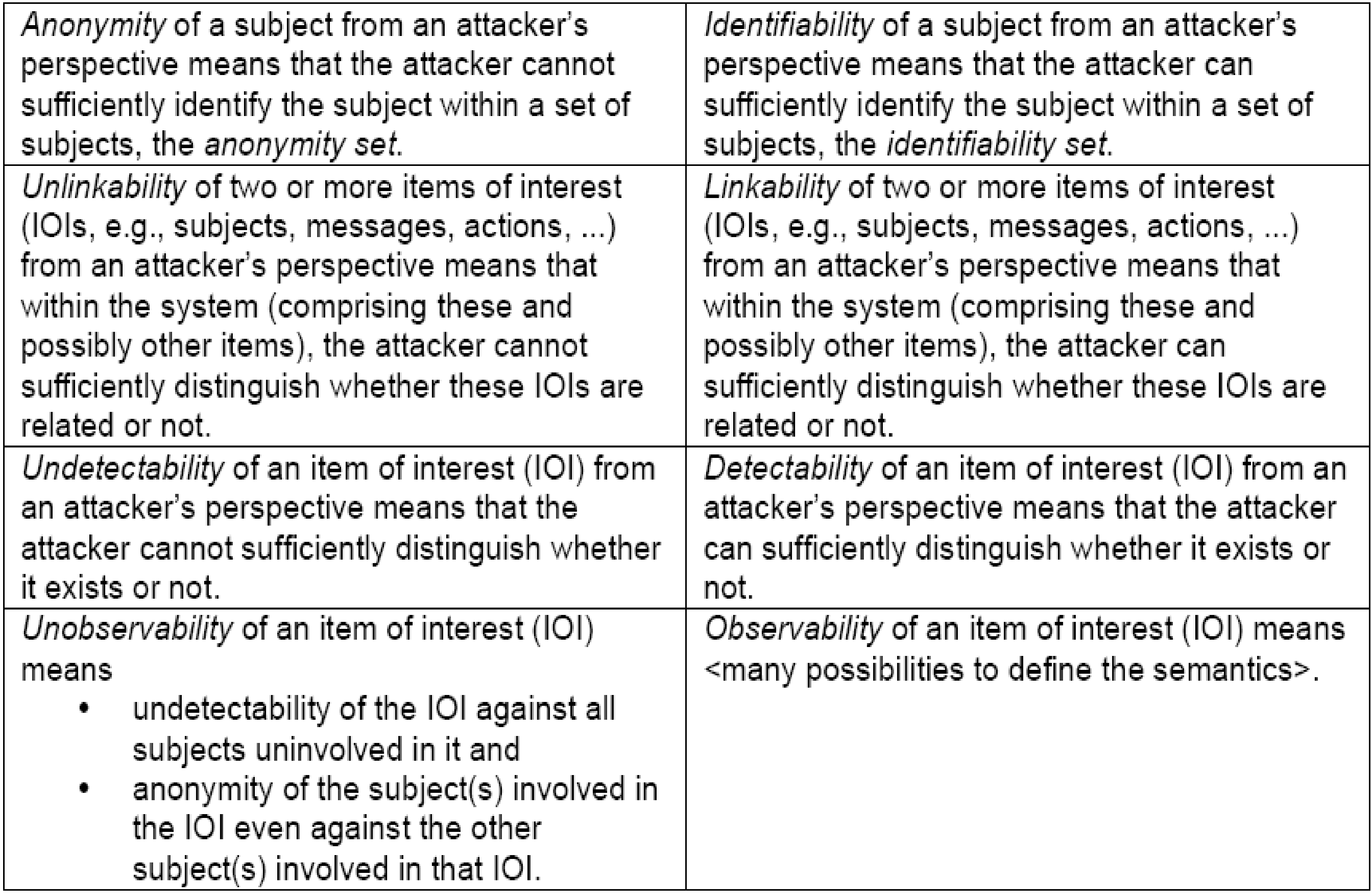
Identity management-related terms

- ***Identity management***: Development and choice of the partial identity and pseudonym to be (re-)used in a specific context or role.
- ***Privacy-enhancing identity management***: Identity management that sufficiently preserves unlinkability between the partial identities.

- ***Privacy-enhancing identity management enabling application design***: A design that neither the pattern of sending/receiving messages nor the attributes given to entities organizations, reduce unlinkability.
- ***Identity management system (IMS):*** refers to technology-based administration of identity attributes.

- ***Privacy-enhancing identity management system (PE-IMS):*** A Privacy-Enhancing IMS that sufficiently preserves unlinkability between the partial identities and corresponding pseudonyms.
- ***User-controlled identity management system:*** an IMS gives its user a large degree of control.

Overview



Anonymity of a subject from an attacker's perspective means that the attacker cannot sufficiently identify the subject within a set of subjects, the *anonymity set*.	*Identifiability* of a subject from an attacker's perspective means that the attacker can sufficiently identify the subject within a set of subjects, the *identifiability set*.
Unlinkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker cannot sufficiently distinguish whether these IOIs are related or not.	*Linkability* of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not.
Undetectability of an item of interest (IOI) from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not.	*Detectability* of an item of interest (IOI) from an attacker's perspective means that the attacker can sufficiently distinguish whether it exists or not.
Unobservability of an item of interest (IOI) means • undetectability of the IOI against all subjects uninvolved in it and • anonymity of the subject(s) involved in the IOI even against the other subject(s) involved in that IOI.	*Observability* of an item of interest (IOI) means <many possibilities to define the semantics>.

Discussion

- Is this terminology complete? Does it consider all terms and all aspects of the terms related to anonymity?