

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

Yasuyuki Tsukada

(NTT Communication Science Laboratories,
Nippon Telegraph and Telephone Corporation)

Joint work with:

Ken Mano (NTT-CSL),

Hideki Sakurada (NTT-CSL), and

Yoshinobu Kawabe (Aichi Institute of Technology)

Motivation and Goal

The title of this session: "Privacy and Security".

1. What is "privacy"? What is "security"?

- You may say, "our new system perfectly ensures user privacy", but it is less appealing unless you clarify what "privacy" means.
- The definition of privacy/security is particularly important in **formal verification** of privacy/security.

2. What's the relationship between "privacy" and "security"?

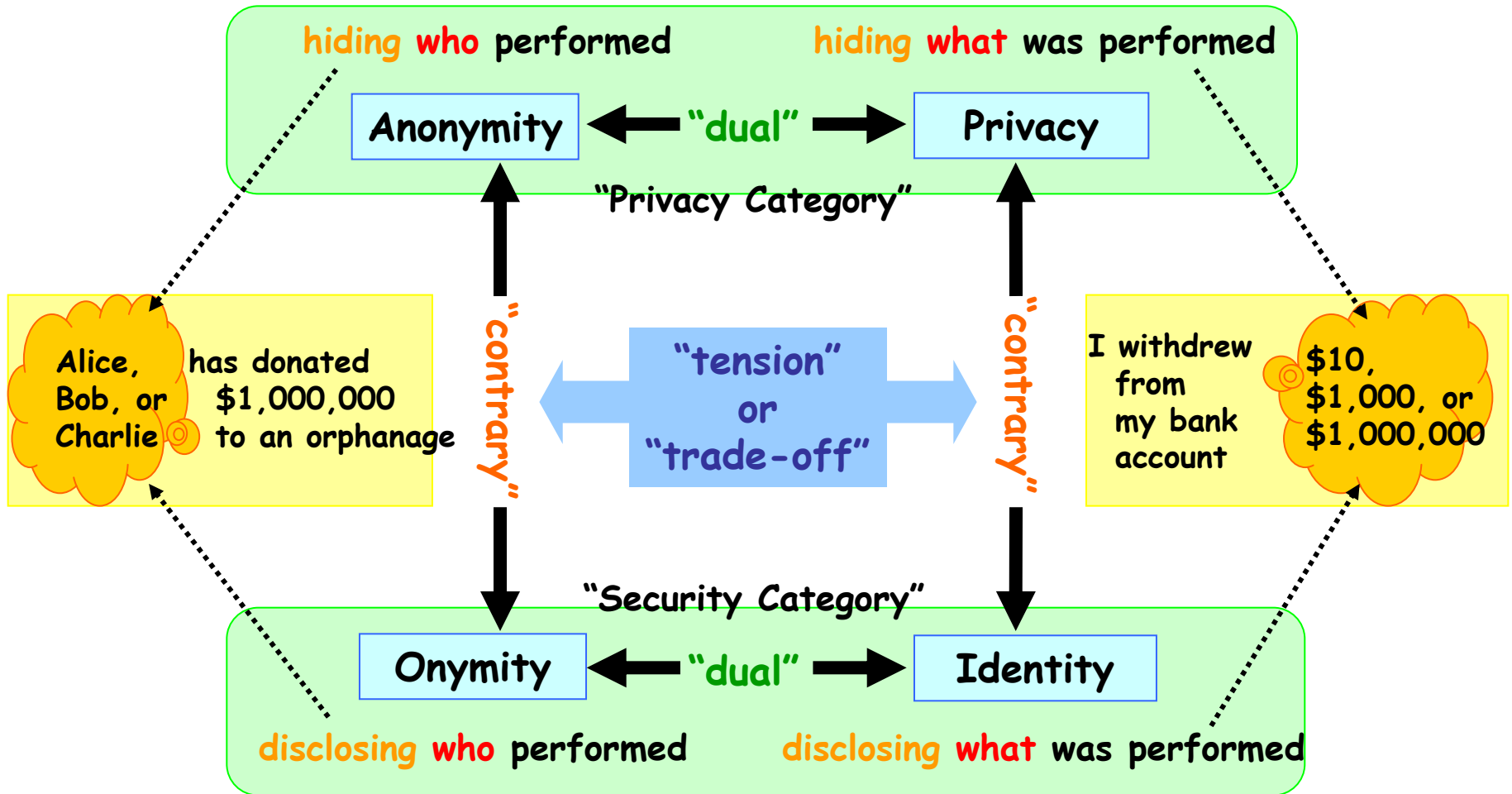
- It is often said that there is some "**tension**" or "**trade-off**" between "privacy" and "security", but it is rather informal and unclear.
- The **logical structure** underlying privacy/security will be helpful for understanding this "tension" or "trade-off".

Our Goal: to present a **taxonomy** of privacy and related properties including their **formal definitions** & **logical structure** underlying them.

Outline

1. Motivation and Goal
2. Taxonomy (Intuitive Version)
3. Approach---Modal Logic of Knowledge
4. Taxonomy (Formal Version)
 - Anonymity
 - Privacy
 - Onymity
 - Identity
5. Compatibility
 - Formal Analysis of "Tension" or "Trade-off"
6. Comparison with Pfitzmann-Hansen's Terminology
7. Conclusion and Future Work

Taxonomy (Intuitive Version)



"dual": operation of taking subject/object reversal "dual" by interchanging who with what

"contrary": operation of taking logical "contrary" by interchanging hiding with disclosure

Taxonomy (Formal Version)

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

role interchangeability

total anonymity

total privacy

$$\theta(i, a) \Rightarrow \bigwedge_{i' \in I \setminus \{j\}} P_j[\theta(i', a)]$$

$$\theta(i, a) \Rightarrow \bigwedge_{a' \in A} P_j[\theta(i, a')]$$

"dual"

(interchange I with A)

anonymity up to I_A

privacy up to A_I

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

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

minimal anonymity
= minimal privacy

$$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$$

"contrary"

"contrary"

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

partial onymity

role noninterchangeability

partial identity

$$\theta(i, a) \Rightarrow \bigvee_{i' \in I \setminus \{j\}} K_j[\neg\theta(i', a)]$$

$$\theta(i, a) \Rightarrow \bigvee_{a' \in A} K_j[\neg\theta(i, a')]$$

"dual"

(interchange I with A)

onymity down from I_A

identity down from A_I

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

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

maximal onymity
= maximal identity

$$\theta(i, a) \Rightarrow K_j[\theta(i, a)]$$

Two Formal Approaches

Computational Approach: based on Process Calculi

Schneider-Sidiropoulos 1996 (**CSP**) (seminal work on formal treatment of anonymity)

Delaune-Kremer-Ryan 2005-2006 (**applied pi calculus**)

Kawabe-Mano-Sakurada-Tsukada 2006-2007 (**I/O-automaton**)

powerful proof methods & practical support tools

-> many successful case studies of e-voting protocols:

anonymity for Fujioka-Okamoto-Ohta (1992), receipt freeness for Okamoto (1996), coercion resistance for Lee et al. (2003)

Logical Approach: based on **the Modal Logic of Knowledge**

Burrows-Abadi-Needham 1990 (seminal work on formal treatment of authentication)

Syverson-Stubblebine 1999

Halpern-O'Neill 2005

Mano-Kawabe-Sakurada-Tsukada 2006

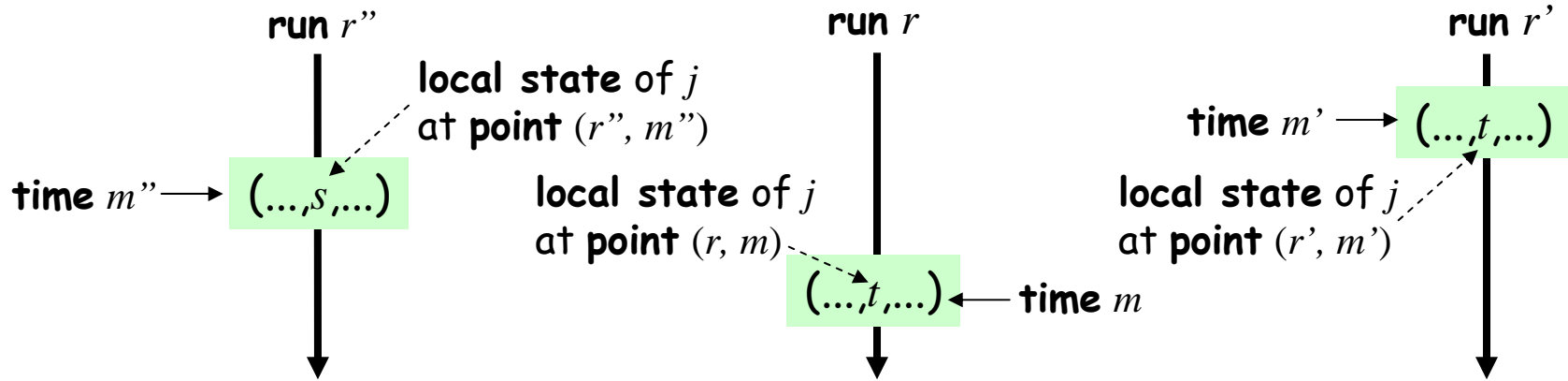
expressive power of the logic

& succinct specifications of variety of properties

-> indispensable for our goal of making a formal taxonomy

Modal Logic of Knowledge: Essence

(Fagin-Halpern-Moses-Vardi 1995)



(r'', m'') and (r, m) are **distinguishable** to j

(r, m) and (r', m') are **indistinguishable** to j
(possible worlds for j)

$$(r'', m'') \not\sim_j (r, m)$$

$$(r, m) \sim_j (r', m')$$

$$(r, m) \models K_j[\varphi] \Leftrightarrow \forall r' \forall m' ((r, m) \sim_j (r', m') \Rightarrow (r', m') \models \varphi)$$

j knows φ at (r, m) iff φ holds at every point indistinguishable to (r, m)

$$(r, m) \models P_j[\varphi] \Leftrightarrow \exists r' \exists m' ((r, m) \sim_j (r', m') \wedge (r', m') \models \varphi)$$

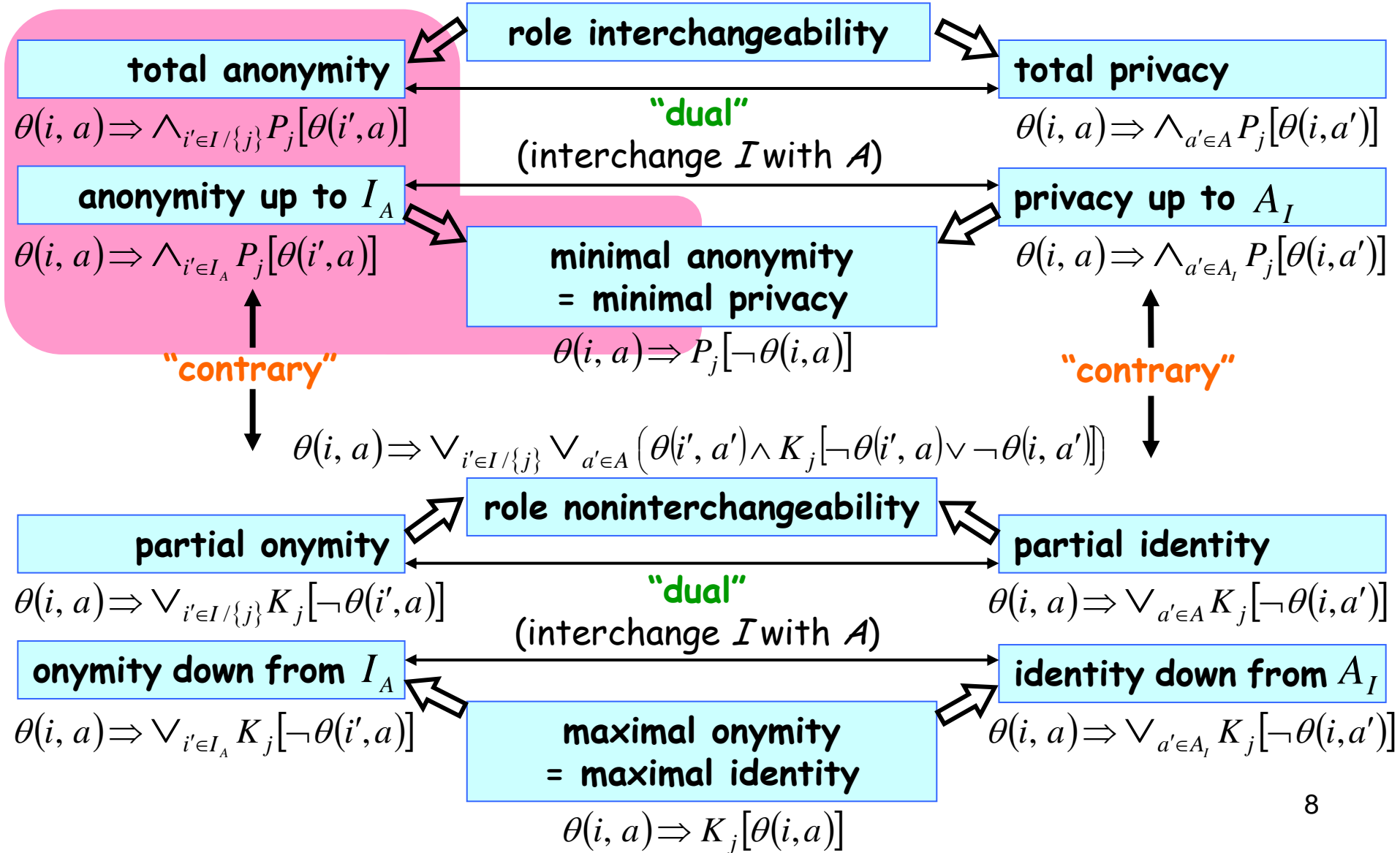
j thinks that φ is

possible at (r, m) iff φ holds at some point indistinguishable to (r, m)

$$(cf. r \models P_j[\varphi] \Leftrightarrow r \models \neg K_j[\neg \varphi])$$

Formal Taxonomy (Anonymity) (Halpern-O'Neill 2005)

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



Formal Taxonomy (Anonymity) (Halpern-O'Neill 2005)

total anonymity

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

anonymity up to I_A

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

minimal anonymity

$$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$$

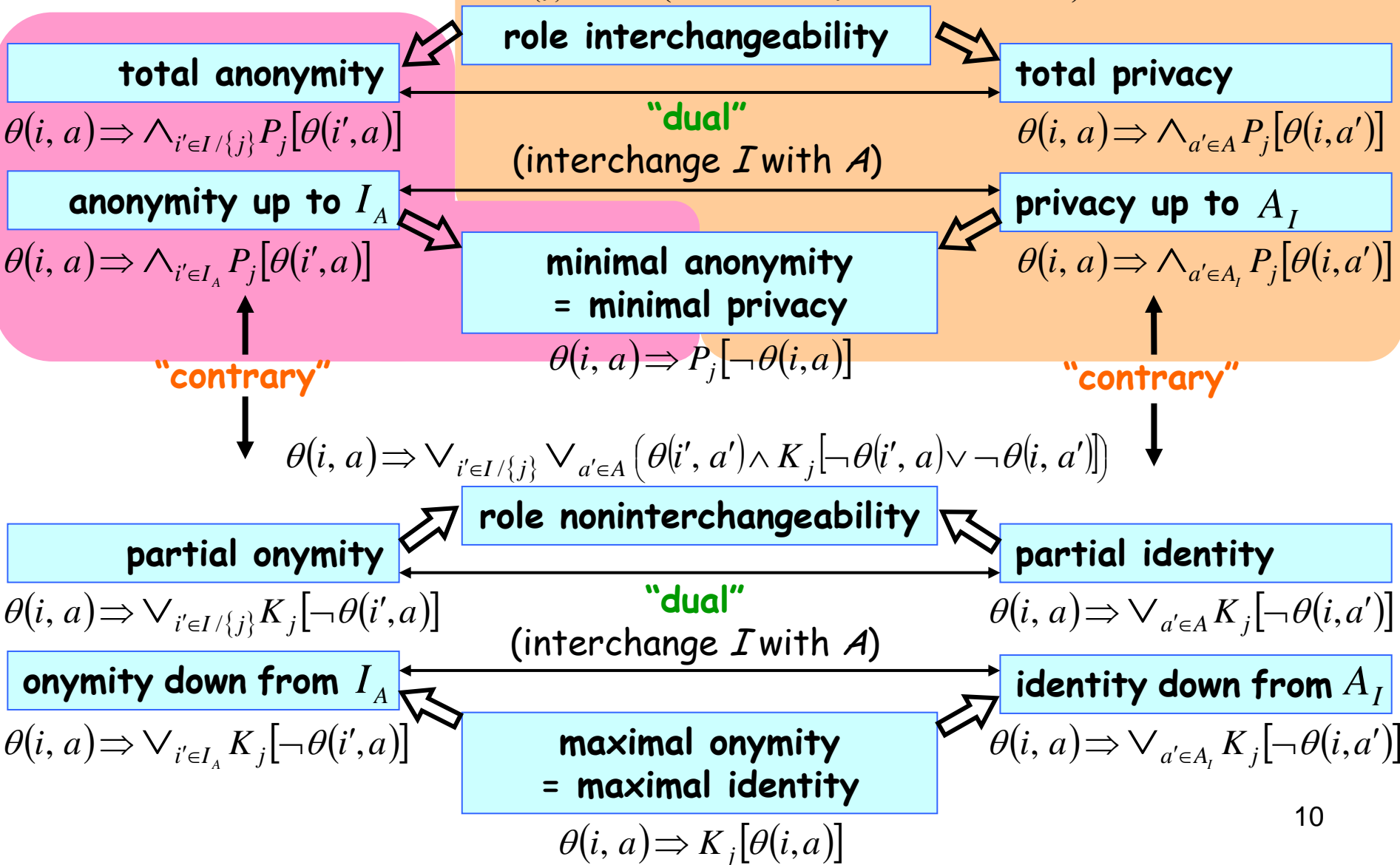
if an agent i
has performed
an action a

then for every agent i'
in an **anonymity set** I_A ,
 j thinks that
 a could have been
performed by i'

Anonymity = hiding who performed

Formal Taxonomy (Privacy) (Mano et al. 2006)

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



Formal Taxonomy (Privacy) (Mano et al. 2006)

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

role interchangeability

total anonymity

total privacy

"dual"

(interchange I with A)

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

$$\theta(i, a) \Rightarrow \bigwedge_{a' \in A} P_j[\theta(i, a')]$$

anonymity up to I_A

privacy up to A_I

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

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

minimal anonymity
= minimal privacy

$$\theta(i, a) \Rightarrow P_j[\neg \theta(i, a)]$$

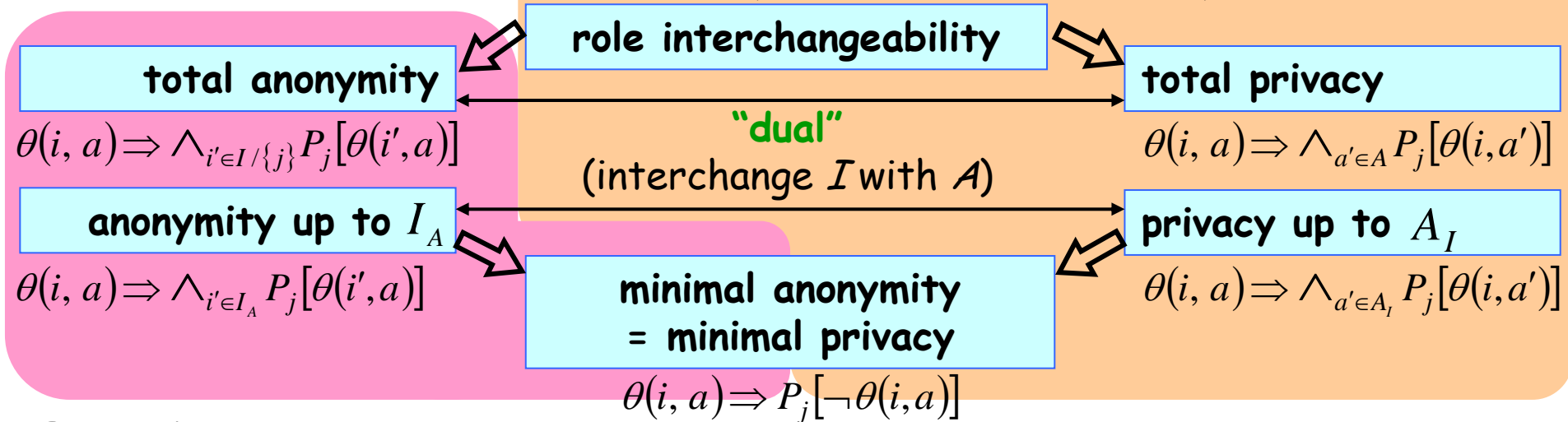
if an agent i
has performed
an action a

then for every action a'
in a **privacy set** A_I ,
 j thinks that
 i could have
performed a'

Privacy = **hiding what** was performed

Formal Taxonomy (Privacy) (Mano et al. 2006)

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



Examples

"Sender Anonymity" (Pfitzmann-Kohntopp 2001)

$$\theta(i, \text{send}(m)) \Rightarrow \bigwedge_{i' \in I_A} P_j[\theta(i', \text{send}(m))] \quad \wedge \quad \theta(i, \text{send}(m)) \Rightarrow \bigwedge_{a' \in \{\text{send}(m') | m'\}} P_j[\theta(i, a')]$$

= **Sender Anonymity**

+

Message Privacy

"Anonymity/Privacy of E-Voting" (Mano et al. 2006)

$$\theta(i, \text{vote}(k)) \Rightarrow \bigwedge_{i' \in \{i' | i' \text{ has a voting right}\}} P_j[\theta(i', \text{vote}(k))] \quad \wedge$$

$$\theta(i, \text{vote}(k)) \Rightarrow \bigwedge_{a' \in \{\text{vote}(k') | k' \text{ wins a vote}\}} P_j[\theta(i, a')]$$

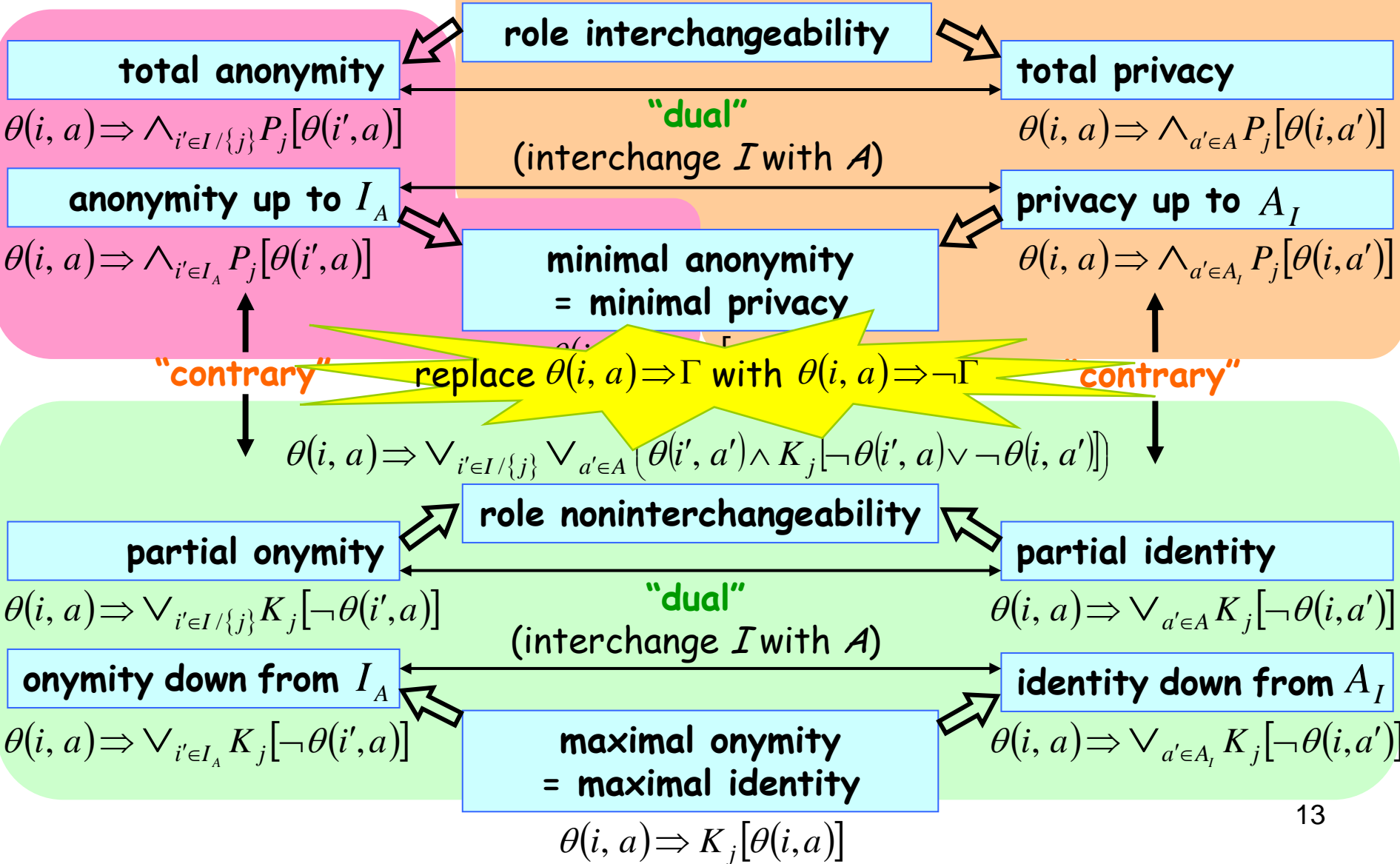
= **Voter Anonymity**

+

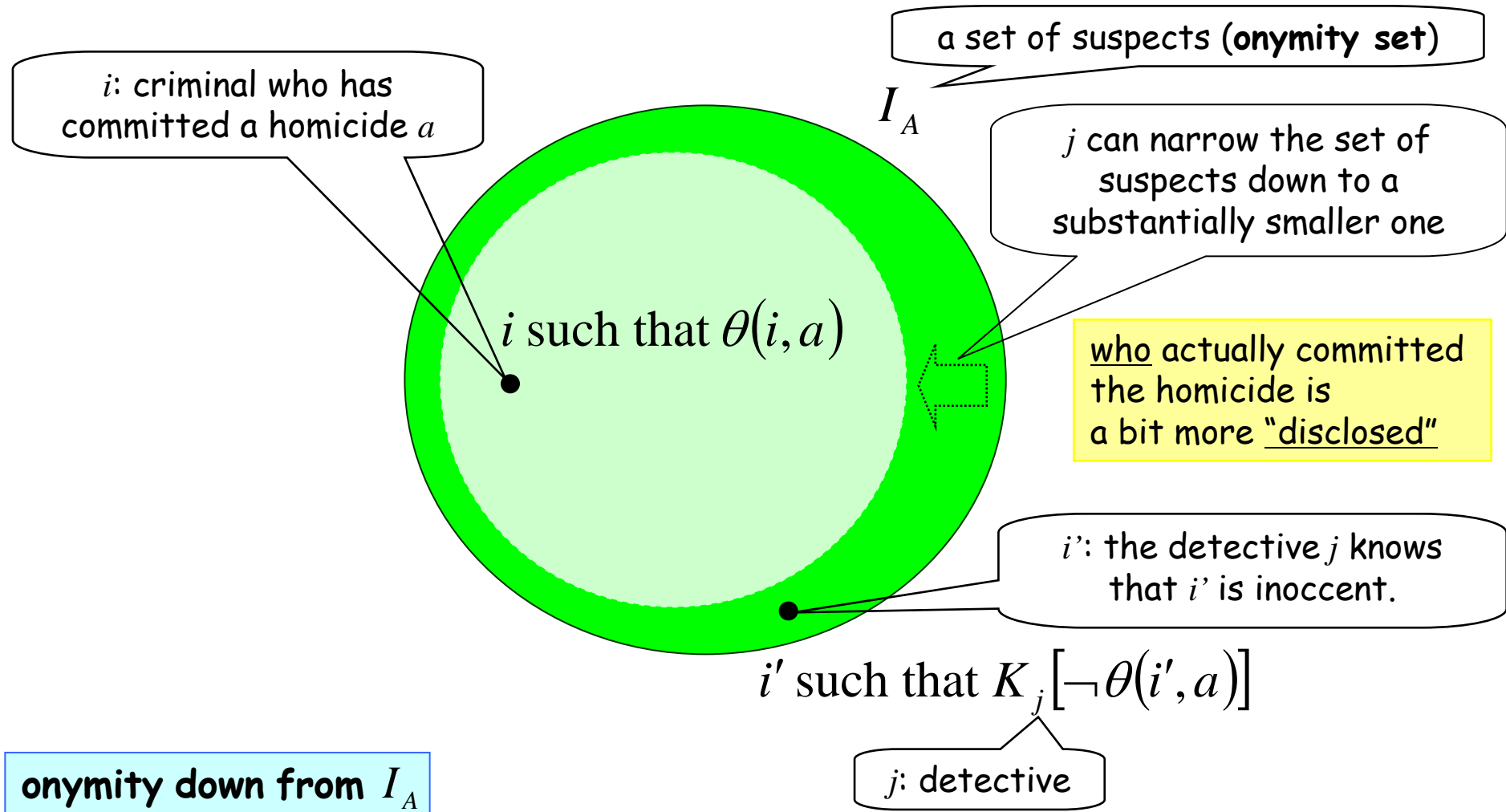
Vote Privacy

Formal Taxonomy (Onymity&Identity) (This Work)

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



Formal Taxonomy (Onymity&Identity) (This Work)



$$\theta(i, a) \Rightarrow \forall_{i' \in I_A} K_j [\neg \theta(i', a)]$$

Onymity = disclosing who performed

Compatibility (Formal Analysis of “Tension” or “Trade-off”)

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

role interchangeability

total anonymity

total privacy

$$\theta(i, a) \Rightarrow \bigwedge_{i' \in I \setminus \{j\}} P_j[\theta(i', a)]$$

$$\theta(i, a) \Rightarrow \bigwedge_{a' \in A} P_j[\theta(i, a')]$$

“dual”

(interchange I with A)

anonymity up to I_A

privacy up to A_I

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

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

minimal anonymity
= minimal privacy

$$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$$

“contrary”

“contrary”

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

partial onymity

role noninterchangeability

partial identity

$$\theta(i, a) \Rightarrow \bigvee_{i' \in I \setminus \{j\}} K_j[\neg\theta(i', a)]$$

$$\theta(i, a) \Rightarrow \bigvee_{a' \in A} K_j[\neg\theta(i, a')]$$

“dual”

(interchange I with A)

onymity down from I_A

identity down from A_I

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

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

maximal onymity
= maximal identity

$$\theta(i, a) \Rightarrow K_j[\theta(i, a)]$$

Compatibility (Formal Analysis of "Tension" or "Trade-off")

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

role interchangeability

total anonymity

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

anonymity up to I_A

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

minimal anonymity

$$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$$

"contrary"

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

partial onymity

role noninterchangeability

$$\theta(i, a) \Rightarrow \bigvee_{i' \in I / \{j\}} K_j[\neg\theta(i', a)]$$

onymity down from I_A

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

maximal onymity

$$\theta(i, a) \Rightarrow K_j[\theta(i, a)]$$

Properties A and B are **compatible** iff
A and B both hold in some possible world semantics

Apparent compatibility
induced by
logical implication

Compatibility (Formal Analysis of "Tension" or "Trade-off")

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

role interchangeability

total anonymity

$$\theta(i, a) \Rightarrow \bigwedge_{i' \in I \setminus \{j\}} P_j[\theta(i', a)]$$

anonymity up to I_A

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

minimal anonymity

$$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$$

"contrary"

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

partial anonymity

role noninterchangeability

$$\theta(i, a) \Rightarrow \bigvee_{i' \in I \setminus \{j\}} K_j[\neg\theta(i', a)]$$

anonymity down from I_A

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

maximal anonymity

$$\theta(i, a) \Rightarrow K_j[\theta(i, a)]$$

Properties A and B are **compatible** iff
A and B both hold in some possible world semantics

Trivial incompatibility
by definition

Compatibility (Formal Analysis of "Tension" or "Trade-off")

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

role interchangeability

total anonymity

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

anonymity up to I_A

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

minimal anonymity

$$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$$

"contrary"

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

partial onymity

$$\theta(i, a) \Rightarrow \bigvee_{i' \in I/\{j\}} K_j[\neg\theta(i', a)]$$

onymity down from I_A

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

role noninterchangeability

maximal onymity

$$\theta(i, a) \Rightarrow K_j[\theta(i, a)]$$

Properties A and B are **compatible** iff
A and B both hold in some possible world semantics

Incompatibility
resulting from
trivial incompatibility
and logical implication

Compatibility (Formal Analysis of "Tension" or "Trade-off")

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

role interchangeability

total anonymity

$$\theta(i, a) \Rightarrow \bigwedge_{i' \in I \setminus \{j\}} P_j[\theta(i', a)]$$

anonymity up to I_A

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

minimal anonymity

$$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$$

"contrary"

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

partial onymity

role noninterchangeability

$$\theta(i, a) \Rightarrow \bigvee_{i' \in I \setminus \{j\}} K_j[\neg\theta(i', a)]$$

onymity down from I_A

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

maximal onymity

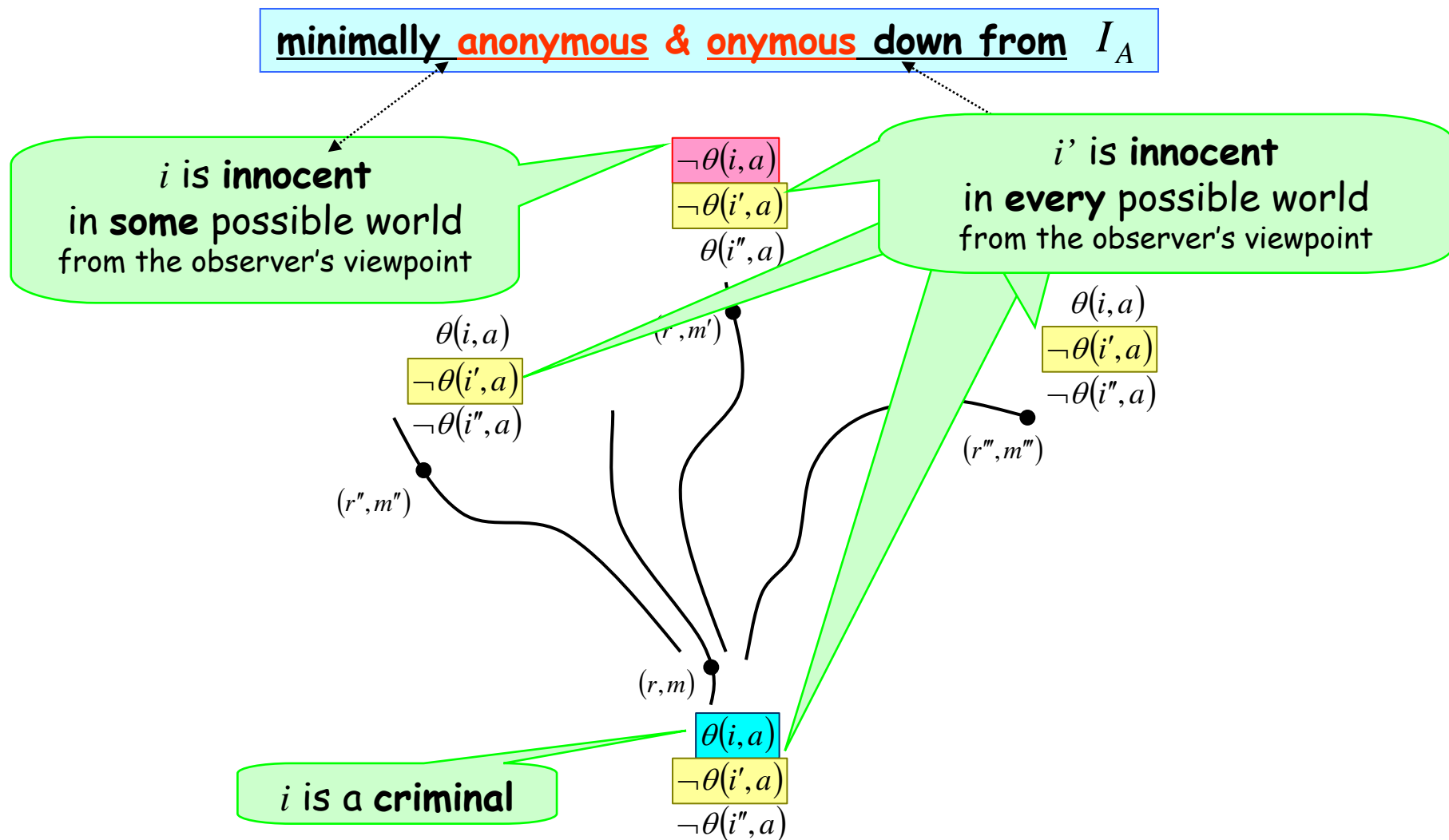
$$\theta(i, a) \Rightarrow K_j[\theta(i, a)]$$

Properties A and B are **compatible** iff
A and B both hold in some possible world semantics

Question:
Weak anonymity & Weak onymity: Compatible?

Answer: **Yes**

Compatibility (Formal Analysis of "Tension" or "Trade-off")



Comparison with Pfitzmann-Hansen

Pfitzmann-Hansen 2008 (Consistent but Informal)	This Work (Formal)
Anonymity Anonymity set	Anonymity up to I_A Anonymity set I_A
N/a N/a	Privacy up to A_I Privacy set A_I
Identifiability Identifiability set	Onymity down from I_A Onymity set I_A
Disclosure of a (PH-)identity Set of (PH-)identities	Identity down from A_I Identity set A_I
Unlinkability	Minimal anonymity/privacy
Undetectability, Unobservability, ...	N/a



Our duality viewpoint is helpful in understanding a structure of privacy-related information-hiding/disclosure properties

Conclusion and Future Work

- A formal taxonomy of anonymity/privacy/onymity/identity in terms of the modal logic of knowledge
 - The concepts of duality and contrary play important roles
- Formal analysis of "tension" or "trade-off"
 - Weak anonymity/privacy are compatible with weak onymity/identity, respectively
- Comparison with Pfitzmann-Hansen's Terminology
- * Our "qualitative" approach & other "quantitative" approaches
 - * The size of I_A / A_I
 - * Information-theoretic approach by Diaz et al. 2002
- * Formal specification and verification using our framework
 - * Current: voter-anonymity/vote-privacy of FOO e-voting
 - * Future: onymity/identity = authentication/non-repudiation?
cf. Zhou-Gollmann 1998
 - * Future: formal analysis in a compositional setting