

# 匿名性とプライバシーの合成可能性について

塚田恭章 櫻田英樹 真野健 真鍋義文

日本電信電話(株) NTT コミュニケーション科学基礎研究所

# 研究の動機

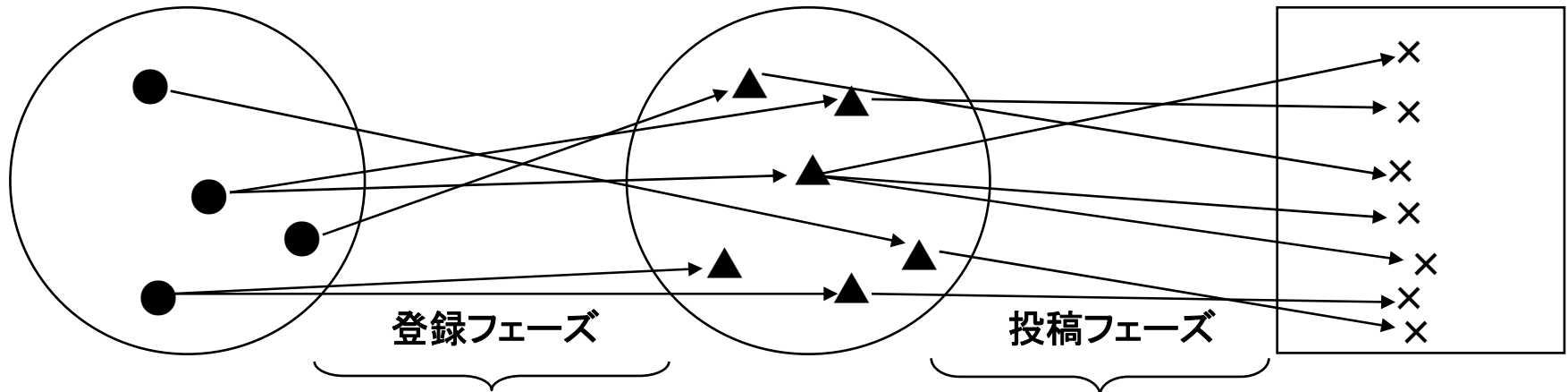
部分システムの性質から全体システムの性質を導くモジュラーなアプローチを匿名性やプライバシーといった個人情報の秘匿に関する性質の検証にも適用したい

## 【例】会員制匿名掲示板システム

実名(real names)の集合

仮名(pseudonyms)の集合

投稿記事の集合



①匿名性(リンク不能性)成立

②プライバシー(リンク不能性)成立

$$x \neq y$$

$$y \neq z$$

⇒ ③匿名性/プライバシー(リンク不能性)成立?

アナロジー?

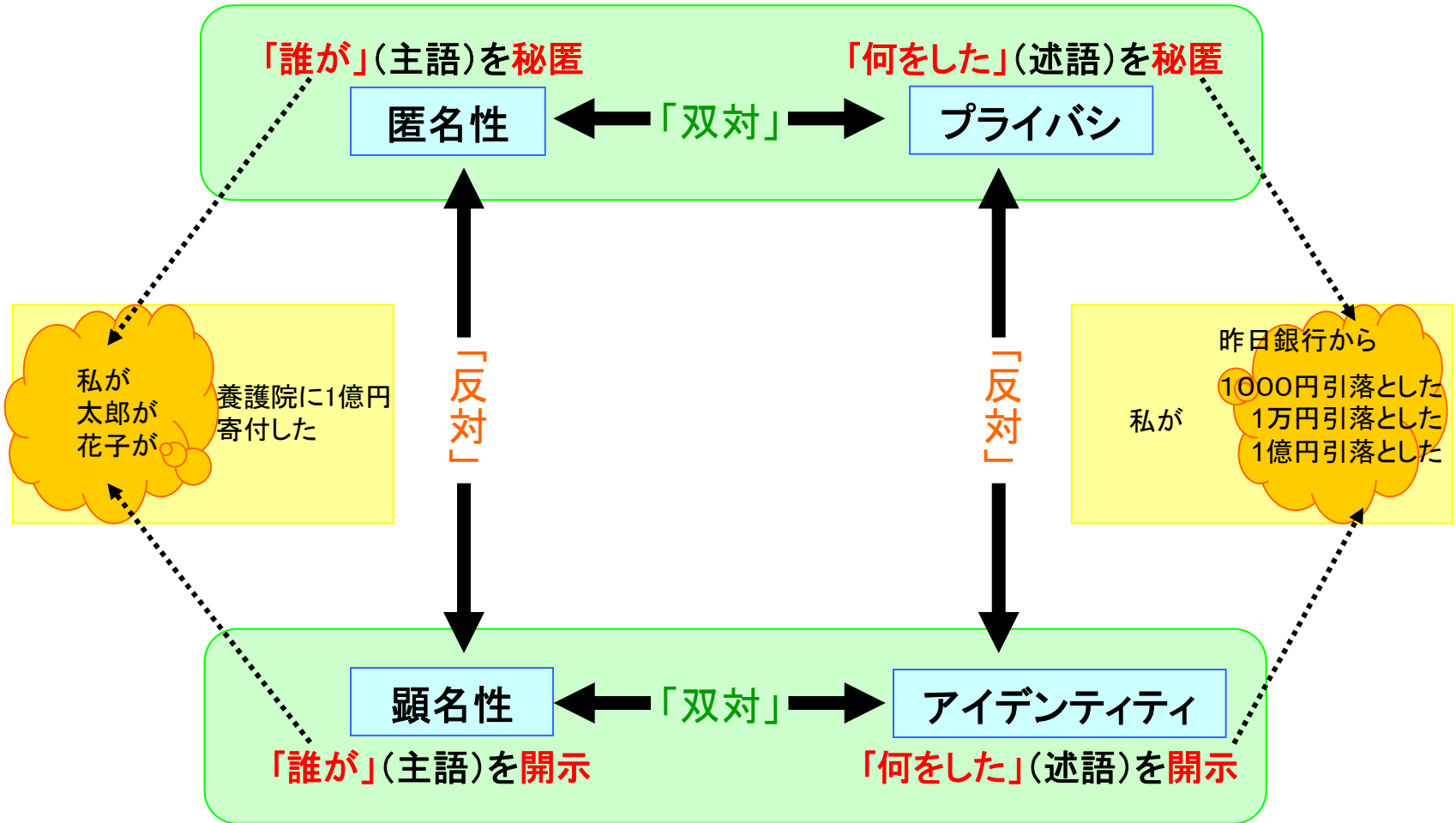
$$x \neq z ?$$

# 本発表の構成

1. 匿名性・プライバシー(+顕名性・アイデンティティ)の知識論理を用いた定式化
2. 会員制匿名掲示板モデルの導入
3. 匿名性・プライバシーの合成不可能性
4. 独立性条件
5. 匿名性・プライバシーが合成可能となるための十分条件
6. 簡単な応用例(電子投票プロトコル)
7. 逐次合成から並列合成へ
8. まとめと今後の課題

# 匿名性・プライバシー・顕名性・アイデンティティ(直観的バージョン)

個人情報の秘匿／開示の視点から



# 匿名性・プライバシー・顕名性・アイデンティティ(フォーマルバージョン)

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

役割交換可能性

全匿名性

全プライバシー

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

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

「双対」

(I と A を入替)

$I_A$  中の匿名性

$A_I$  中のプライバシー

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

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

極小匿名性=極小プライバシー

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

↑「反対」

↑「反対」

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

役割交換不能性

部分顕名性

部分アイデンティティ

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

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

「双対」

(I と A を入替)

$I_A$  からの顕名性

$A_I$  からのアイデンティティ

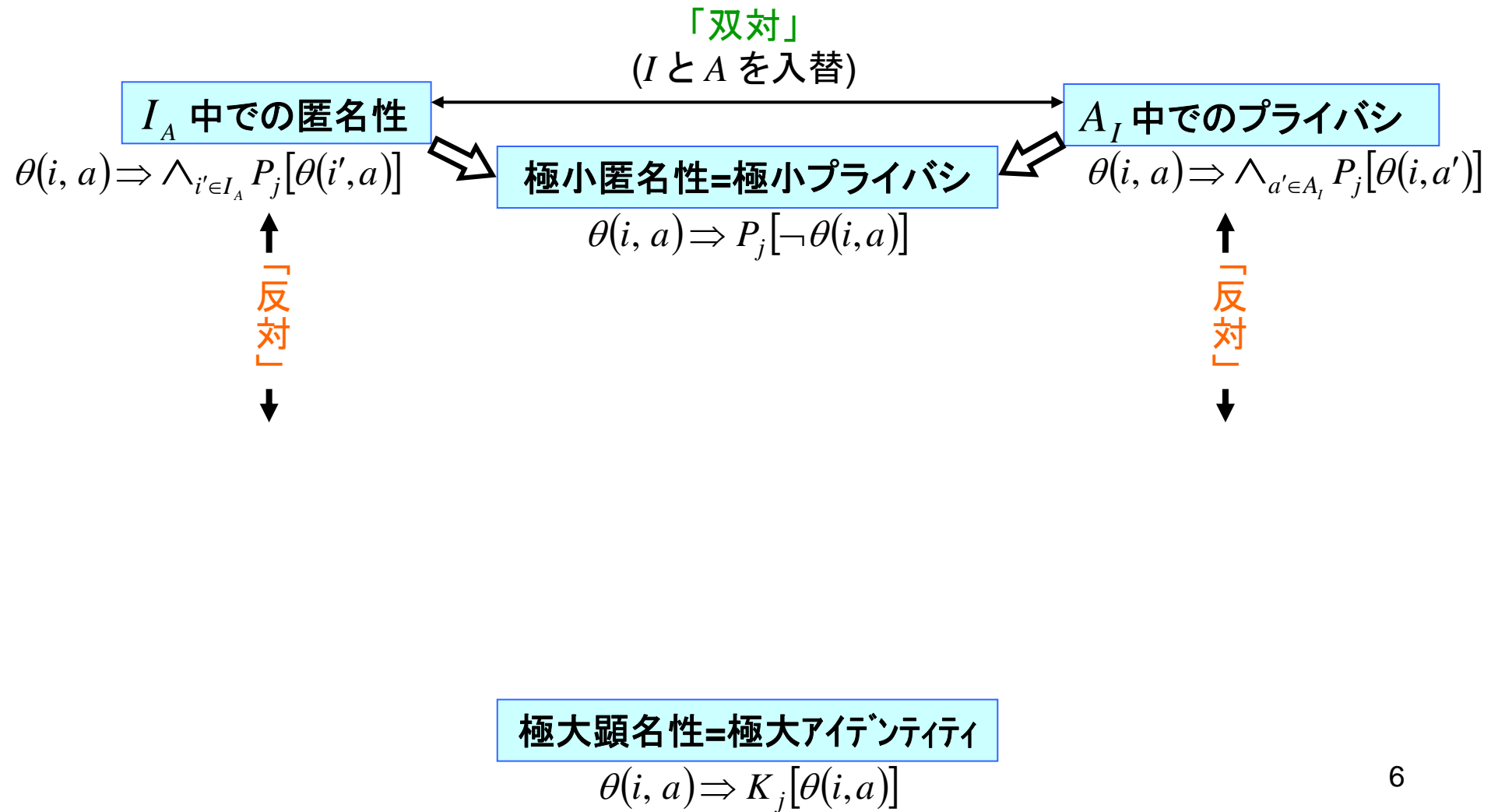
$$\theta(i, a) \Rightarrow \bigvee_{i' \in I_A} K_j[\neg\theta(i', a)]$$

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

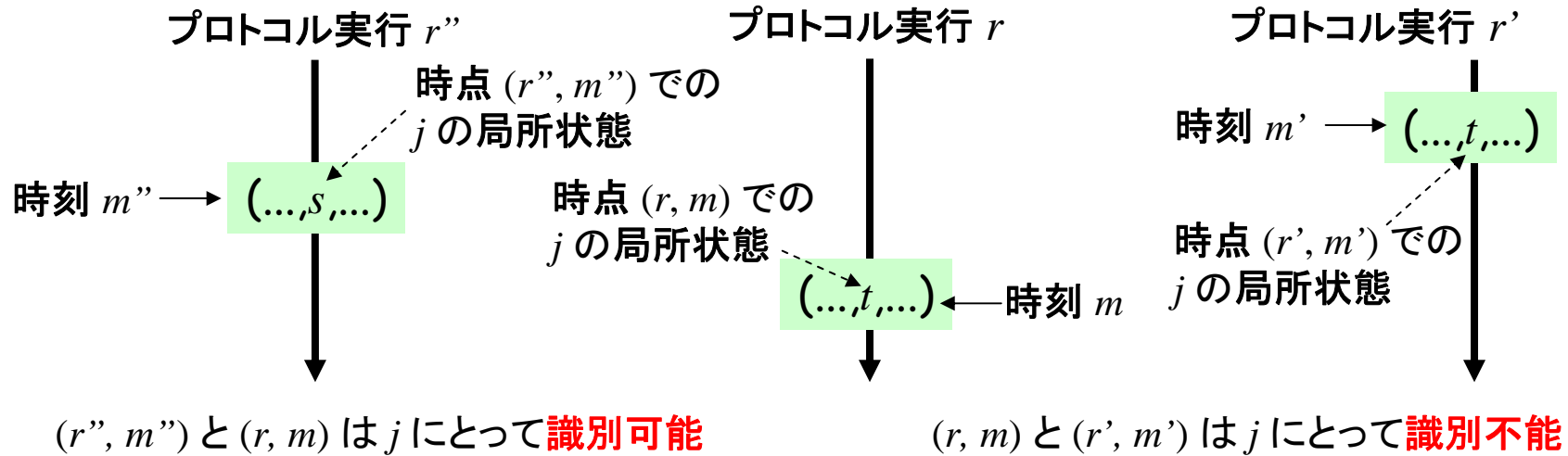
極大顕名性=極大アイデンティティ

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

# 匿名性・プライバシー・顕名性・アイデンティティ(抜粋)



# 知識論理の「肝」 (Fagin-Halpern-Moses-Vardi 1995)



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

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

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

$(r, m)$  において  $j$  が  $\varphi$  を知っている

iff  $j$  にとって  $(r, m)$  と識別不能な任意の時点上で  $\varphi$  が成立

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

$(r, m)$  において  $j$  が  $\varphi$  かもしれないと思っている

iff  $j$  にとって  $(r, m)$  と識別不能なある時点上で  $\varphi$  が成立

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

# 匿名性・プライバシー・顕名性・アイデンティティ(抜粋)

「双対」  
(I と A を入替)

$I_A$  中の匿名性

$A_I$  中のプライバシー

極小匿名性=極小プライバシー

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

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

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

参加者  $i$  が  
アクション  $a$  を  
実行したならば

匿名集合  $I_A$  中の任意の  $i'$  について,  $j$  は,  
 $i'$  が  $a$  を実行したかもしれないと思っている

匿名性 = 「誰が」(主語)を秘匿

極大顕名性=極大アイデンティティ

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



# 匿名性・プライバシー・顕名性・アイデンティティ(抜粋)

「双対」  
(I と A を入替)

$I_A$  中の匿名性

$A_I$  中のプライバシー

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

極小匿名性=極小プライバシー

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

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

参加者  $i$  が  
アクション  $a$  を  
実行したならば

プライバシー集合  $A_I$  中の  
任意の  $a'$  について,  $j$  は,  
 $i$  が  $a'$  を実行したかもしれない  
と思っている

プライバシー = 「何をした」(述語)を秘匿

極大顕名性=極大アイデンティティ

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

# 匿名性・プライバシー・顕名性・アイデンティティ(抜粋)

「双対」

(I と A を入替)

$I_A$  中での匿名性

$A_I$  中でのプライバシー

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

極小匿名性=極小プライバシー

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

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

双対性により、匿名性とプライバシーに切り分けた詳細な仕様記述が可能

“送信者匿名性” (Pfitzmann-Kohntopp 2001)

$$\theta(i, \text{send}(m)) \Rightarrow \bigwedge_{i' \in I_A} P_j[\theta(i', \text{send}(m))] \quad \wedge \quad \theta(i, \text{send}(m)) \Rightarrow \bigwedge_{a' \in \{\text{send}(m') \mid m'\}} P_j[\theta(i, a')] \\ = \quad \text{送信者匿名性} \quad + \quad \text{メッセージプライバシー}$$

“電子投票の匿名性/プライバシー” (真野ら 2010)

$$\theta(i, \text{vote}(k)) \Rightarrow \bigwedge_{i' \in \{i' \mid i' \text{ は投票権を獲得}\}} P_j[\theta(i', \text{vote}(k))] \quad \wedge \\ \theta(i, \text{vote}(k)) \Rightarrow \bigwedge_{a' \in \{\text{vote}(k') \mid k' \text{ は1票以上得票}\}} P_j[\theta(i, a')] \\ = \quad \text{投票者匿名性} \quad + \quad \text{投票プライバシー}$$

極大顕名性=極大アイデンティティ

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

# 匿名性・プライバシー・顕名性・アイデンティティ(抜粋)

$i$ と $a$ の間の  
リンク不能性

$I_A$  中の匿名性

$A_I$  中のプライバシー

極小匿名性=極小プライバシー

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

「反対」

$\theta(i, a) \Rightarrow \Gamma$  を  
 $\theta(i, a) \Rightarrow \neg\Gamma$  に置換

「反対」

$i$ と $a$ の間の  
リンク可能性

極大顕名性=極大アイデンティティ

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

## ここまでの話

### 【匿名性、確率的匿名性】

Halpern, O'Neill: *Journal of Computer Security* **13**(3) 483-512 (2005)

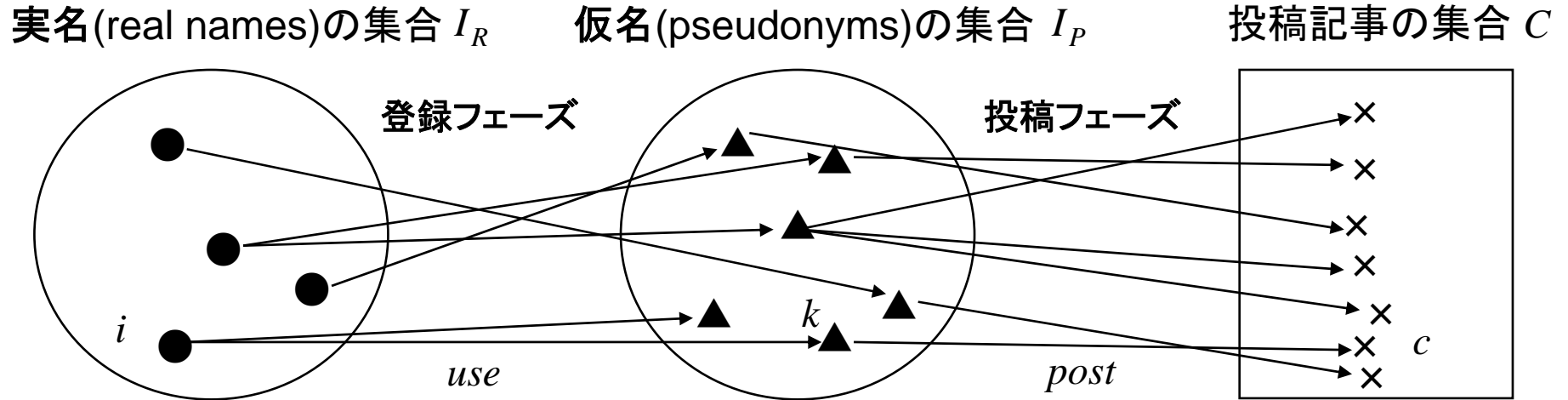
### 【プライバシー、双対、役割交換、電子投票プロトコルFOO検証】

Mano, Kawabe, Sakurada, Tsukada: *Journal of Logic and Computation* **20**(6) 1251-1288 (2010)

### 【顕名性、アイデンティティ、Pfitzmann-Hansen 2010との比較】

Tsukada, Mano, Sakurada, Kawabe: *Transactions on Data Privacy* **3**(3) 177-198 (2010)

# 会員制匿名掲示板モデルの導入



$use$  と  $post$  の逐次合成

$$|= \theta(i, submit(c)) \Leftrightarrow \bigvee_{k \in I_P} (\theta(i, use(k)) \wedge \theta(k, post(c)))$$

会員制匿名掲示板モデルの一般性

【再解釈その1】 $i$ : 投票者,  $k$ : 投票ID,  $c$ : 投票内容  $\Rightarrow$  電子投票

【再解釈その2】 $use$ : 1段目 mix サーバ,  $post$ : 2段目 mix サーバ  $\Rightarrow$  多段 mix サーバ

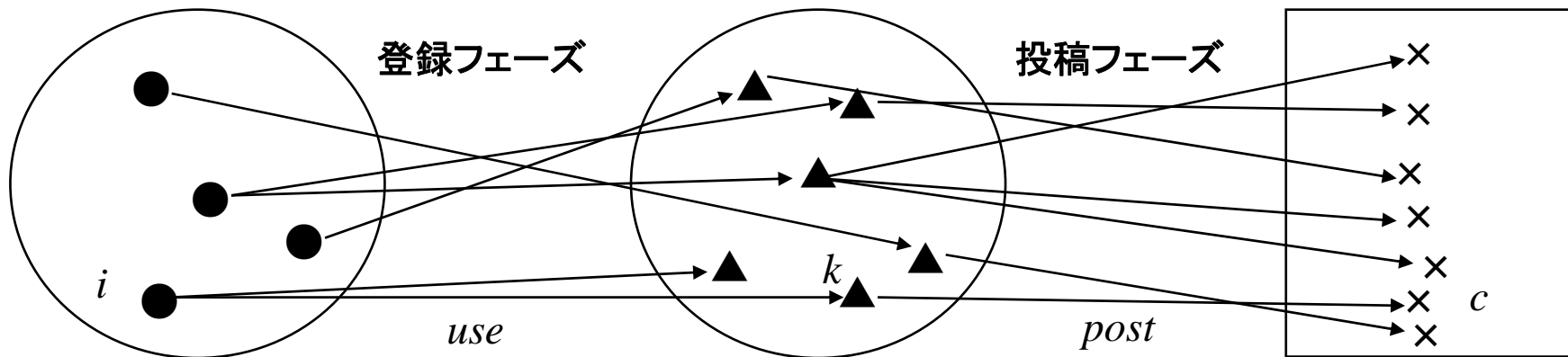
(注: 多少の付加条件は必要)

# 匿名性・プライバシーの合成不可能性

実名(real names)の集合  $I_R$

仮名(pseudonyms)の集合  $I_P$

投稿記事の集合  $C$



$use$  に関する匿名性

$$\theta(i, use(k)) \Rightarrow \bigwedge_{i' \in I_R} P_j[\theta(i', use(k))]$$

+

$post$  に関するプライバシー

$$\theta(k, post(c)) \Rightarrow \bigwedge_{c' \in C} P_j[\theta(k, post(c'))]$$

$submit$  に関する匿名性 or プライバシ ???

⇒成り立たない!

反例:

$r_1$   
 $i_1$  ———  $k_1$  ———  $c_1$

$r_1$

$i_2$  ———  $k_2$  ———  $c_2$

**説明1:** 観測者が「 $i_1$  は絶対  $c_2$  を  $submit$  なんかしない」という前提知識を持っていることと、 $use$  に関する匿名性・ $post$  に関するプライバシーは相反しない

$r_2$   
 $i_1$  ———  $k_2$  ———  $c_1$

$r_2$

$i_2$  ———  $k_1$  ———  $c_2$

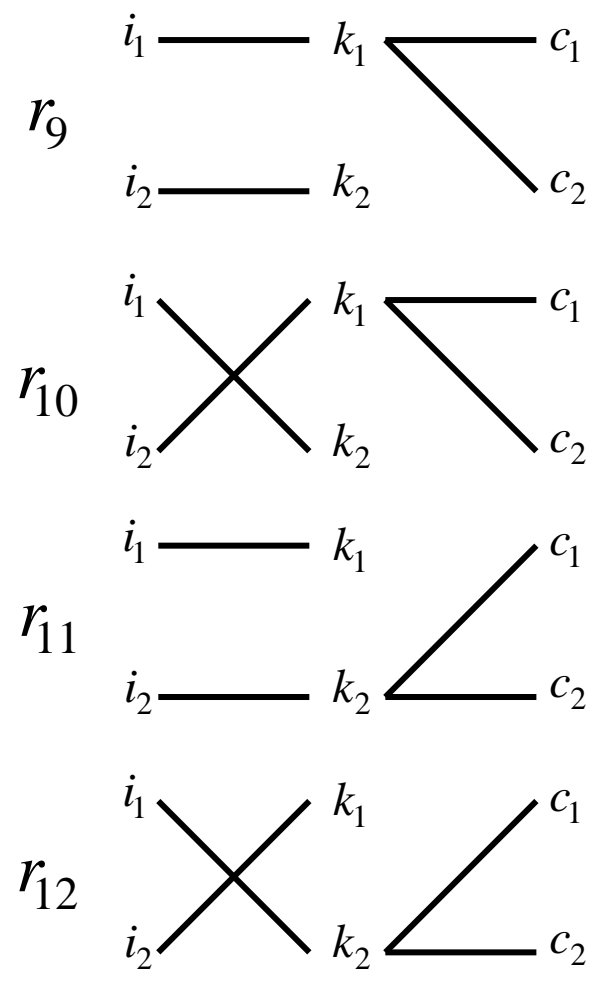
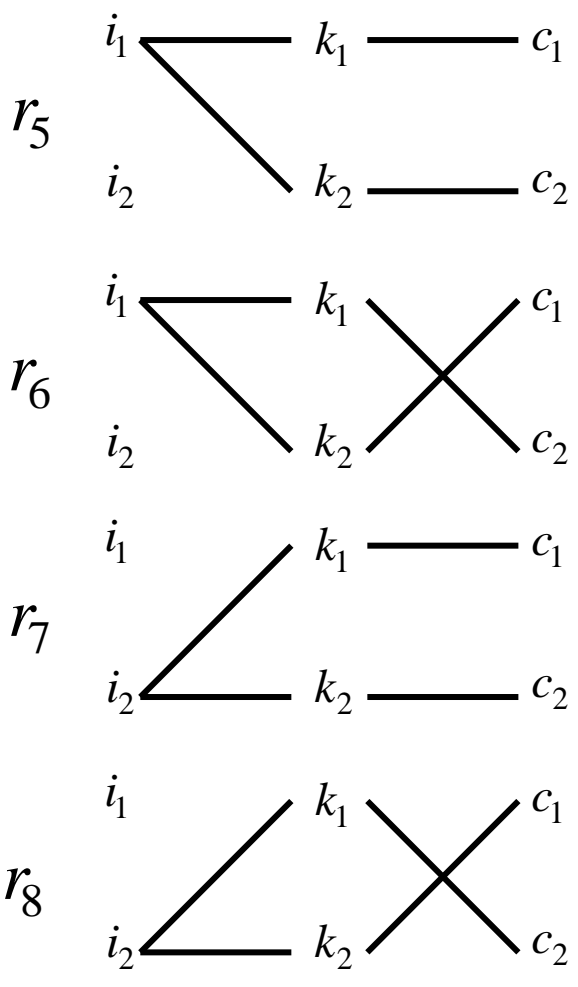
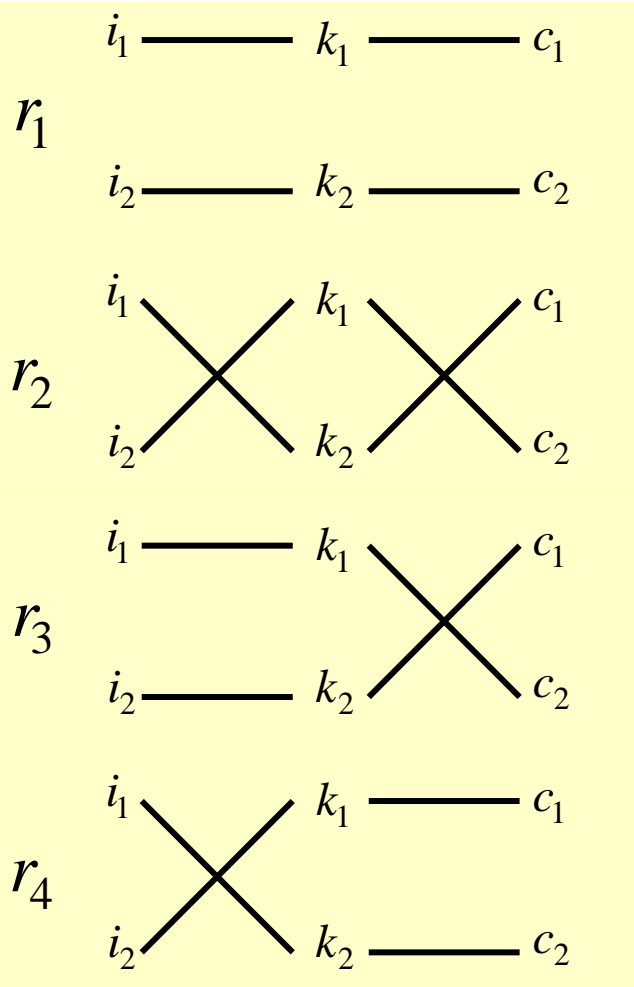
**説明2:**  $use = M$ ,  $post = M^{-1}$ ,  $submit = M * M^{-1} = Id$

**観察:**  $use$  と  $post$  が「独立」ならば合成可能か?

# 独立性条件

$$\begin{array}{c}
 P_j[\theta(i, use(k))] \wedge P_j[\theta(k', post(c))] \\
 \Downarrow \\
 P_j[\theta(i, use(k)) \wedge \theta(k', post(c))]
 \end{array}$$

$$\begin{array}{c}
 \equiv \Pr(A) * \Pr(B) \\
 \parallel \\
 \Pr(A \cap B)
 \end{array}$$

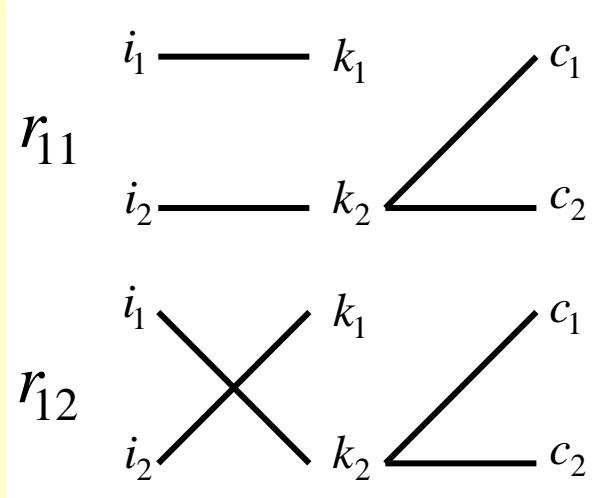
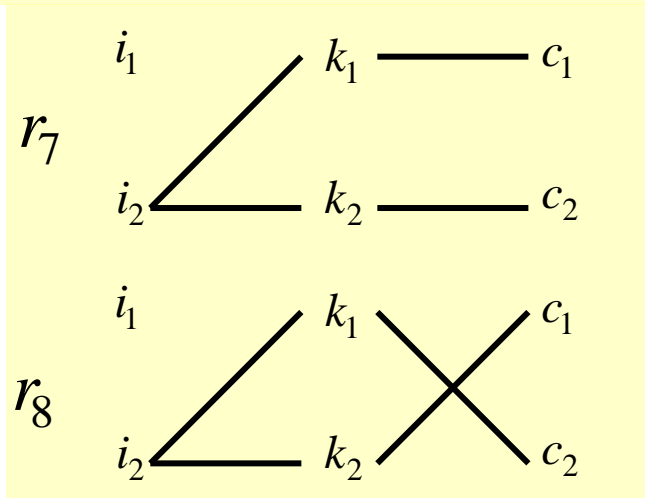
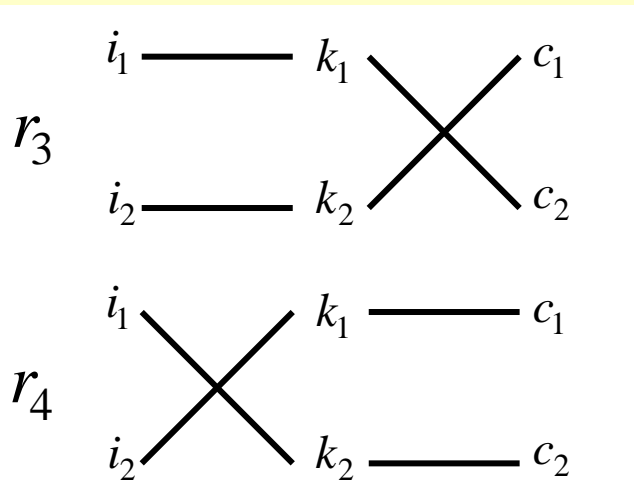
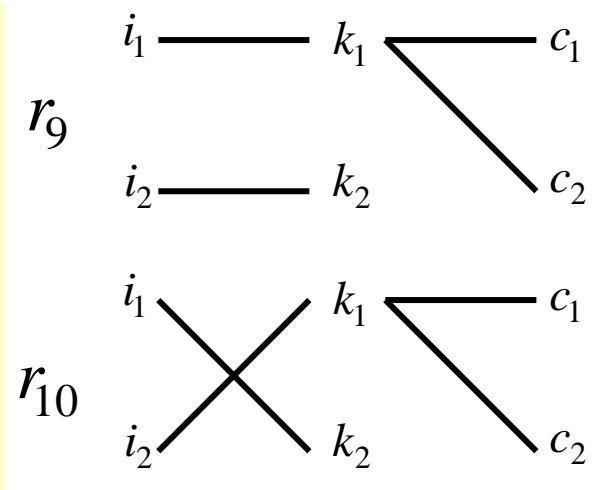
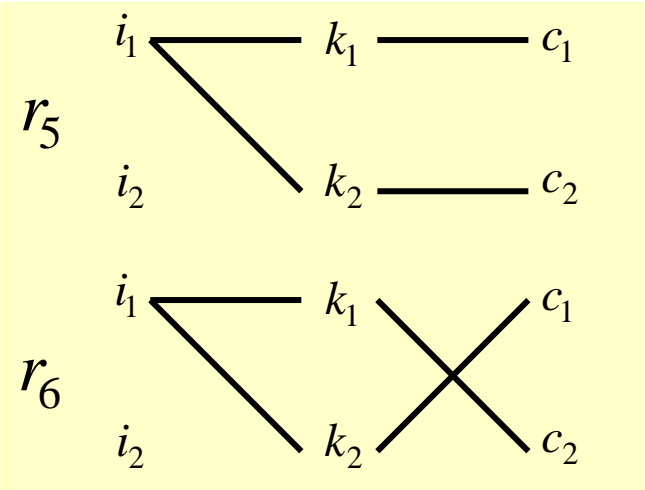
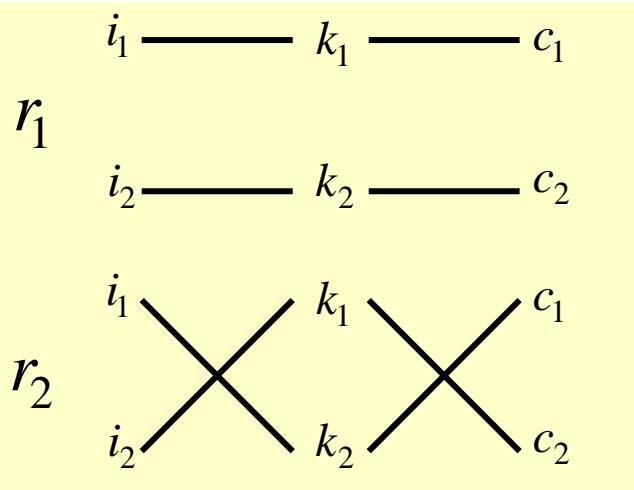


独立性条件自体が「メタレベル」のある種の匿名性・プライバシー

# 独立性条件

$$\begin{aligned}
 &P_j[\theta(i, use(k))] \wedge P_j[\theta(k', post(c))] \\
 &\quad \Downarrow \\
 &P_j[\theta(i, use(k)) \wedge \theta(k', post(c))]
 \end{aligned}$$

$$\begin{aligned}
 &\equiv \Pr(A) * \Pr(B) \\
 &\quad \parallel \\
 &\Pr(A \cap B)
 \end{aligned}$$



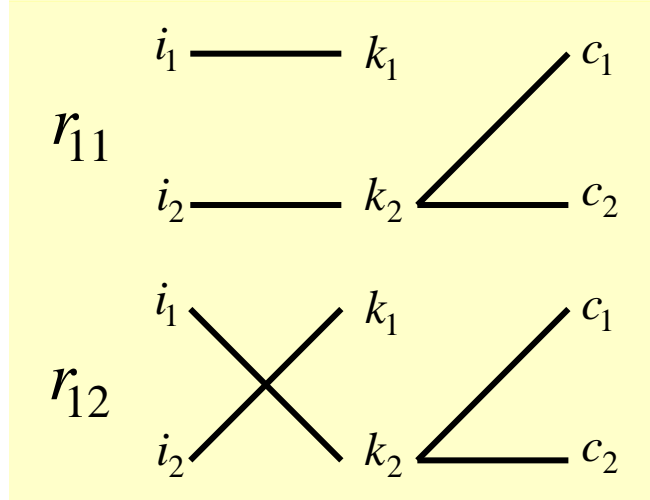
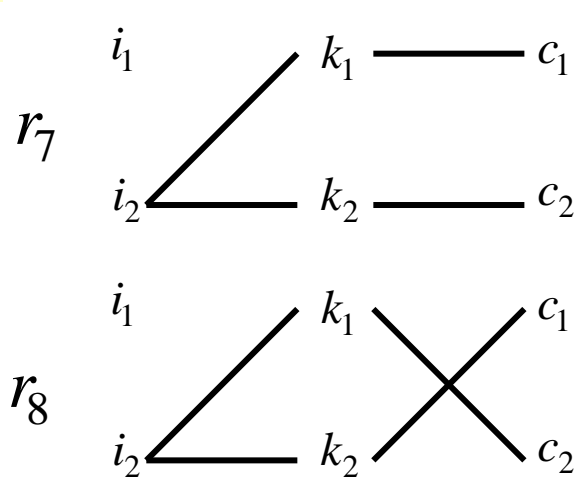
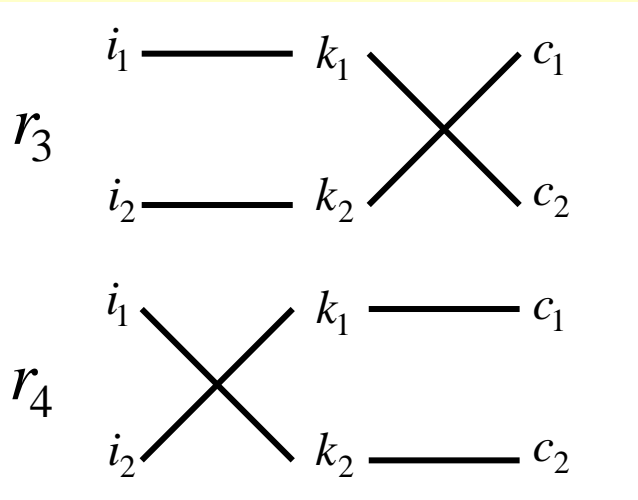
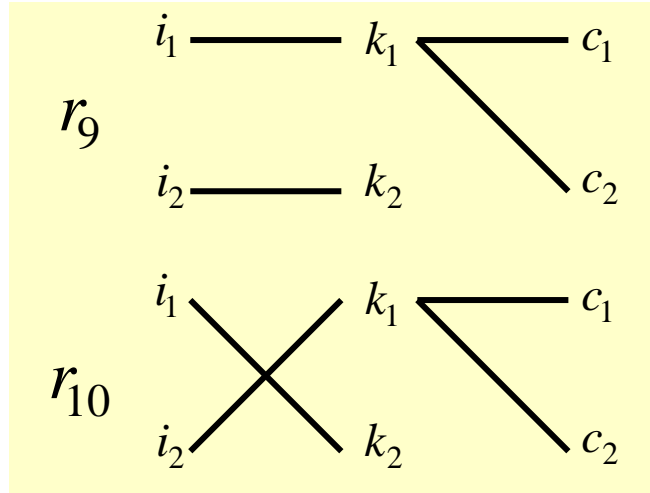
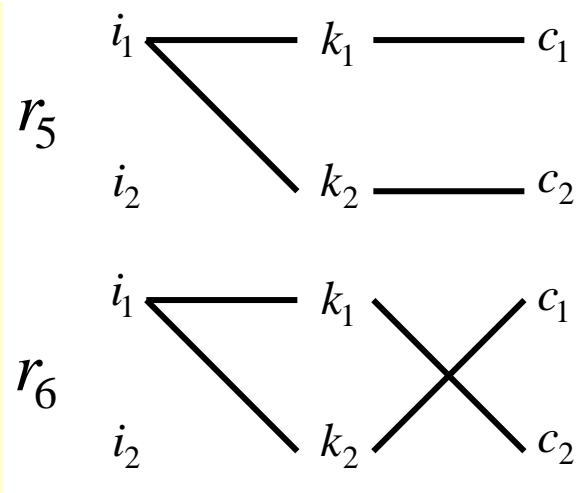
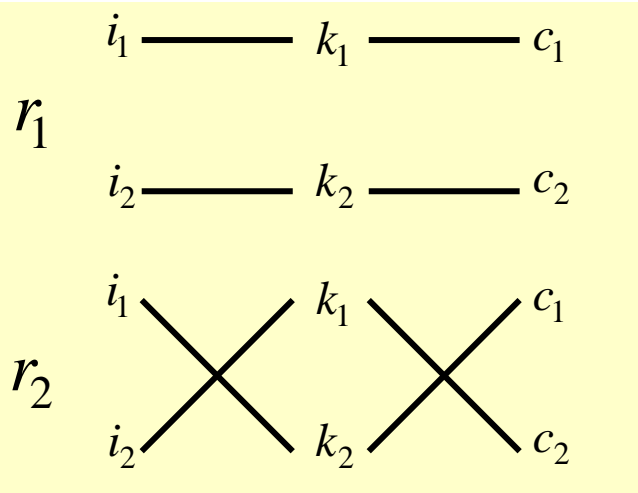
独立性条件自体が「メタレベル」のある種の匿名性・プライバシー



# 独立性条件

$$\begin{aligned}
 &P_j[\theta(i, use(k))] \wedge P_j[\theta(k', post(c))] \\
 &\quad \Downarrow \\
 &P_j[\theta(i, use(k)) \wedge \theta(k', post(c))]
 \end{aligned}$$

$$\begin{aligned}
 &\equiv \Pr(A) * \Pr(B) \\
 &\quad \parallel \\
 &\Pr(A \cap B)
 \end{aligned}$$



独立性条件自体が「メタレベル」のある種の匿名性・プライバシー

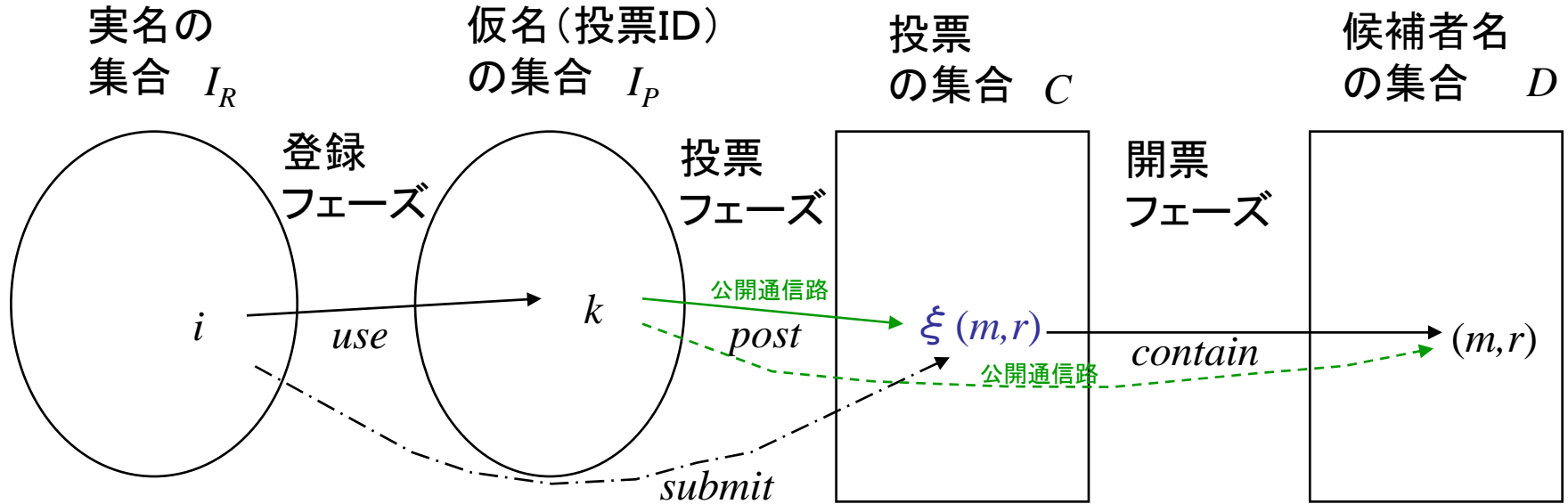
# 匿名性・プライバシーが合成可能となるための十分条件

ケース	仮定	登録フェーズ( <i>use</i> )	投稿フェーズ( <i>post</i> )	全体( <i>submit</i> )
①		$I_R$ 中で匿名	$A_P$ 中でプライベート	—
②	独立	—	$A_P$ 中でプライベート	$A_S$ 中でプライベート
③	独立	$I_R$ 中で匿名	—	$I_R$ 中で匿名
④	—	極大顕名	$A_P$ 中でプライベート	$A_S$ 中でプライベート
⑤	—	$I_R$ 中で匿名	極大アイデンティティ	$I_R$ 中で匿名
⑥	pairwise独立		役割交換可能	役割交換可能
⑦	pairwise独立	役割交換可能		役割交換可能
⑧	独立 投稿:全域, 登録・投稿:排他的	—	極小プライベート	極小プライベート
⑨	独立 登録:全域, 登録・投稿:排他的	極小匿名	—	極小匿名
⑩	投稿:全域, 登録・投稿:排他的	極大顕名	極小プライベート	極小プライベート
⑪	登録:全域, 登録・投稿:排他的	極小匿名	極大アイデンティティ	極小匿名
⑫	—	極大顕名	極大アイデンティティ	極大顕名 / 極大アイデンティティ

【補題】極大顕名 / 極大アイデンティティ  $\Rightarrow$  独立

①匿名 + プライバシ  $\leq$  ④プライバシ

# 簡単な応用例(電子投票プロトコル)



*submit* と *contain* の逐次合成

$$|= \theta(i, \text{vote}(d)) \Leftrightarrow \forall c \in C (\theta(i, \text{submit}(c)) \wedge \theta(c, \text{contain}(d)))$$

前提	登録フェーズ( <i>use</i> )	投票フェーズ( <i>post</i> )	開票フェーズ( <i>contain</i> )	全体( <i>vote</i> )
1	$I_R$ 中で匿名	極大アイデンティティ	極大アイデンティティ	$I_R$ 中で匿名(ケース⑤&⑤)
2 秘密通信路→	$I_R$ 中で匿名	$A_p$ 中でプライベート	極大アイデンティティ	合成的な推論不可(ケース①)
3 独立 秘密通信路→	$I_R$ 中で匿名	$A_p$ 中でプライベート	極大アイデンティティ	$I_R$ 中で匿名(ケース②&⑤)
4 $\xi((m,i),r)$	極大顕名	極大アイデンティティ	極大アイデンティティ	極大顕名(ケース⑫&⑫)

$k$  と  $i$  の間のリンク可能性

## まとめ

- ・匿名性・プライバシーの合成不可能性
- ・独立性条件
- ・匿名性・プライバシーが合成可能となるための十分条件
- ・簡単な応用例(電子投票プロトコル)
- ・並列合成

## 今後の課題

1. 確率知識論理を用いた合成可能性の議論 (cf. Halpern-O'Neill 2005)
2. 合成可能性推論の計算論的健全性
3. 実システムの合成的検証