匿名性とプライバシの合成可能性について

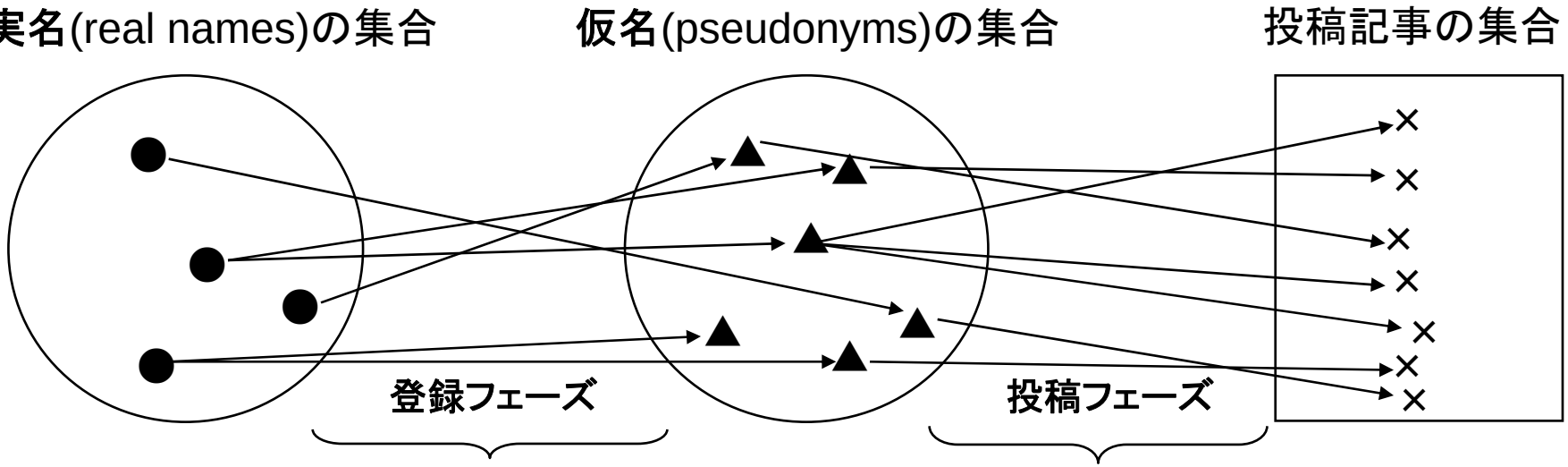
塚田恭章　　櫻田英樹　　真野健　　真鍋義文

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



①匿名性(リンク不能性)成立　②プライバシ(リンク不能性)成立

$x \neq y$　　$y \neq z$

⇒ ③匿名性／プライバシ(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（＋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・プライバシの合成不可能性

4. 独立性条件

5. 匿名性・プライバシが合成可能となるための十分条件

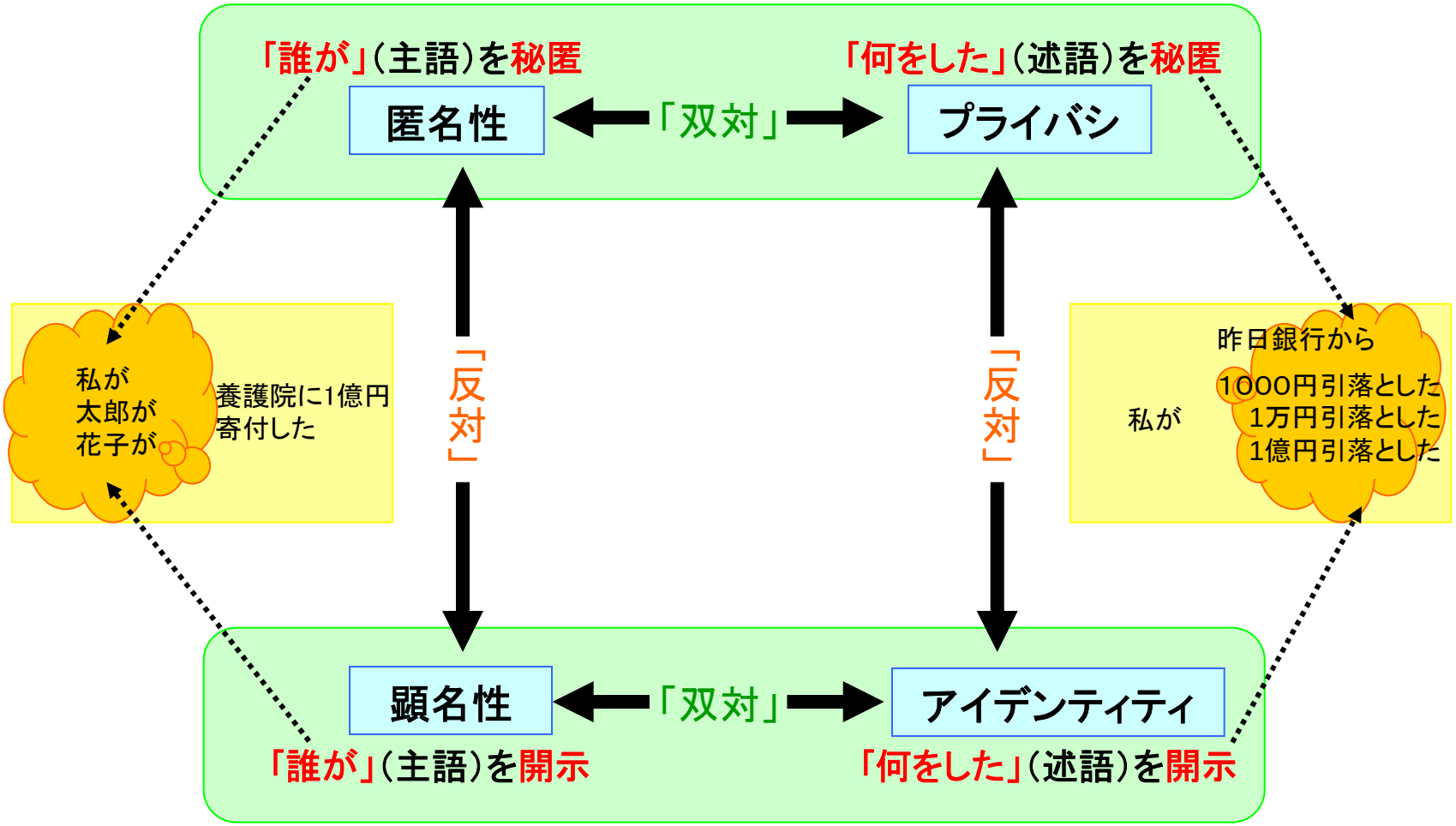
6. 簡単な応用例（電子投票プロトコル）

7. 逐次合成から並列合成へ

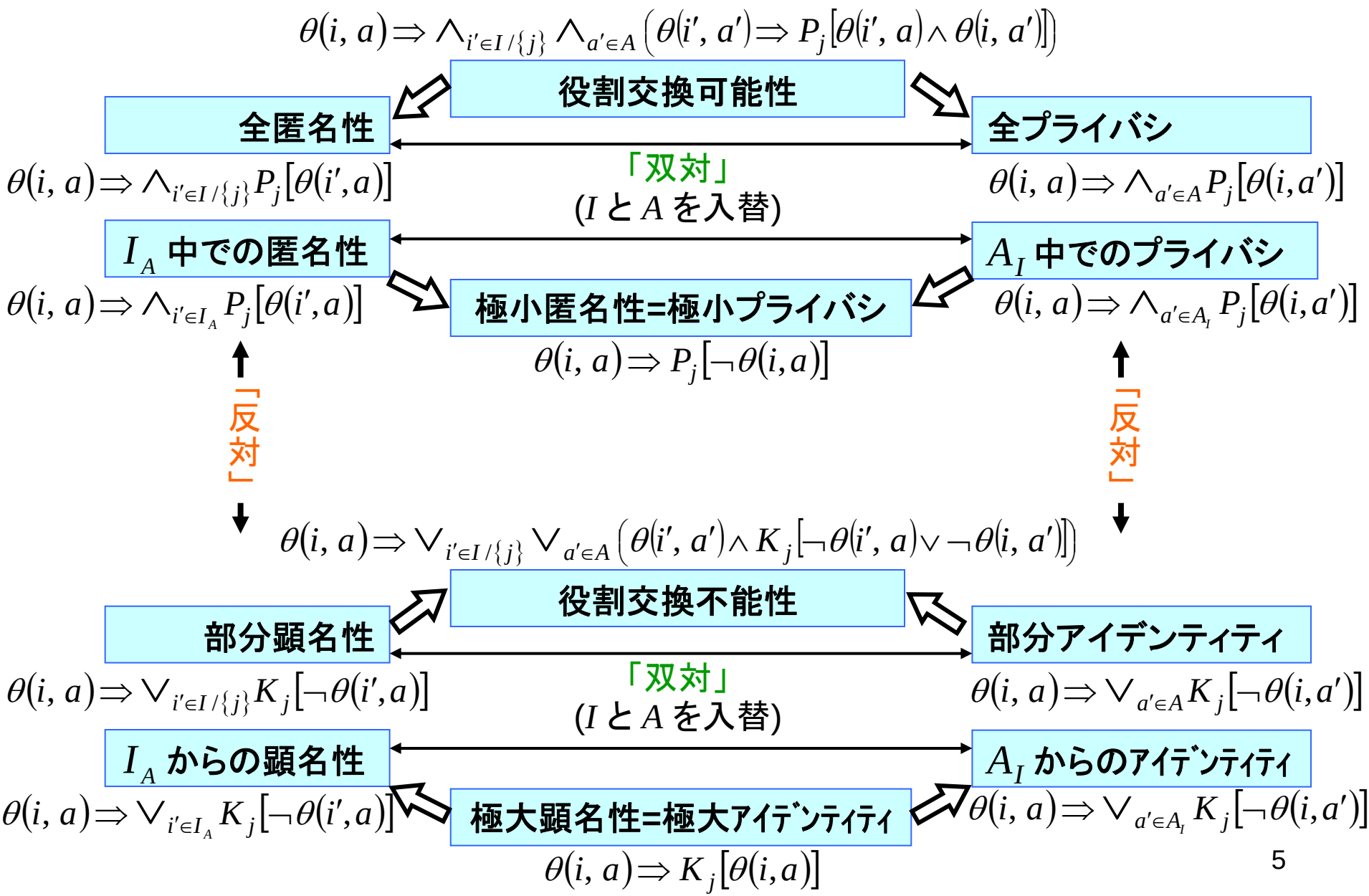
8. まとめと今後の課題

匿名性・プライバシ・顕名性・アイデンティティ（直観的バージョン）

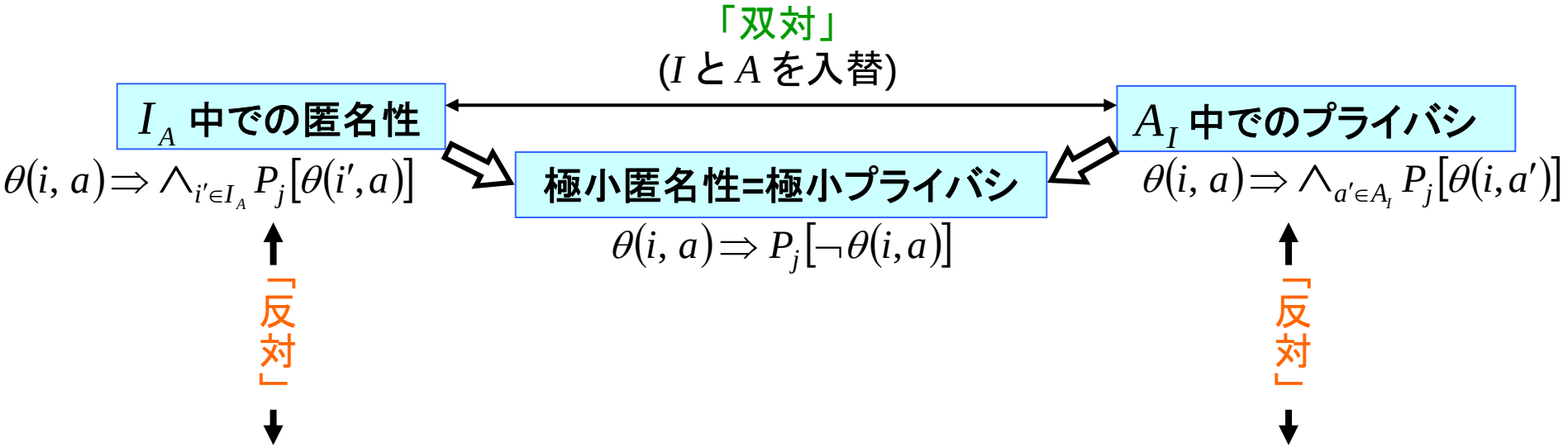
個人情報の秘匿／開示の視点から



匿名性・プライバシ・顕名性・アイデンティティ（フォーマルバージョン）



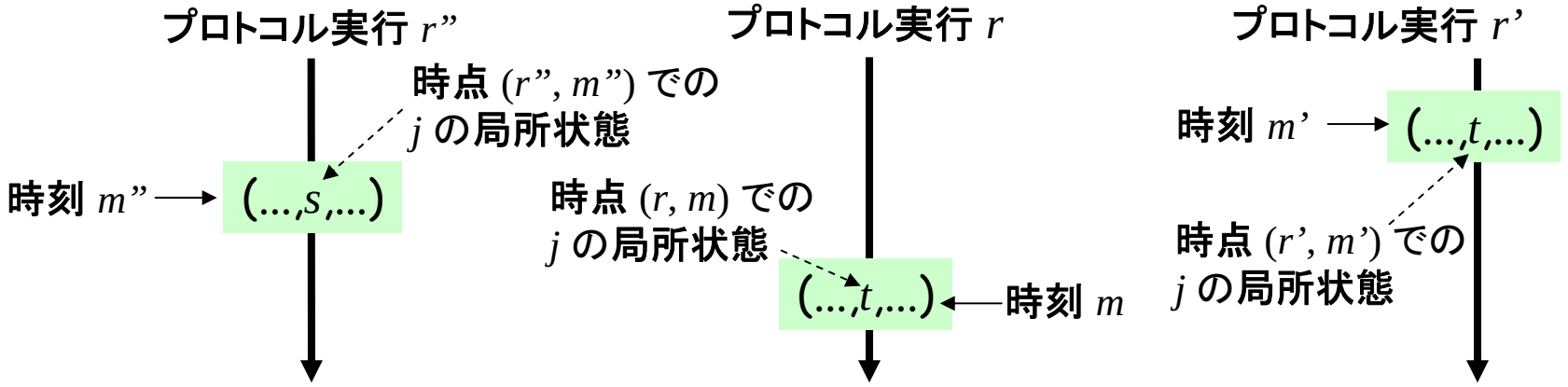
匿名性・プライバシ・顕名性・アイデンティティ（抜粋）



極大顕名性=極大アイデンティティ

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

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



(r”, m”) と (r, m) は j にとって**識別可能**

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

(r, m) と (r’, m’) は j にとって**識別不能**

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

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

(r, m) において j が φ 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 φ が成立

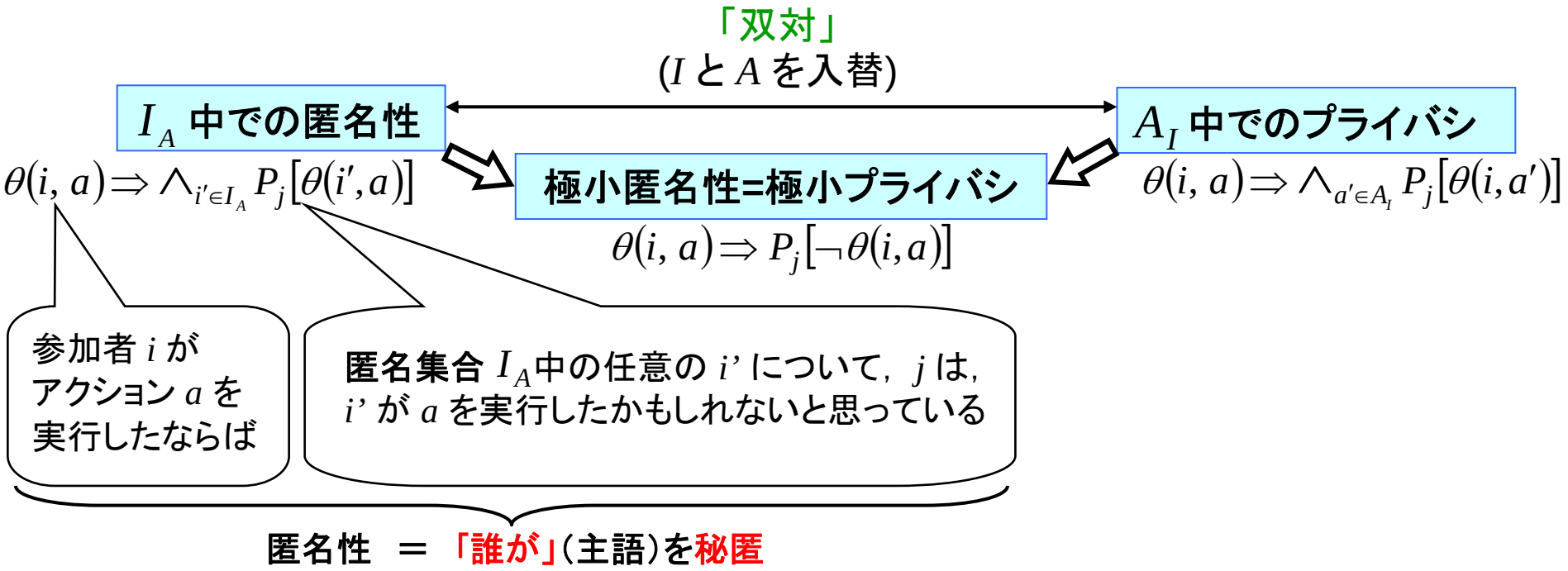
$$(r, m) \models P_j[\varphi] \Leftrightarrow \exists r' \exists m' ((r, m) \sim_j (r', m') \wedge (r', m') \models \varphi)$$

(r, m) において j が φ **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 φ が成立

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

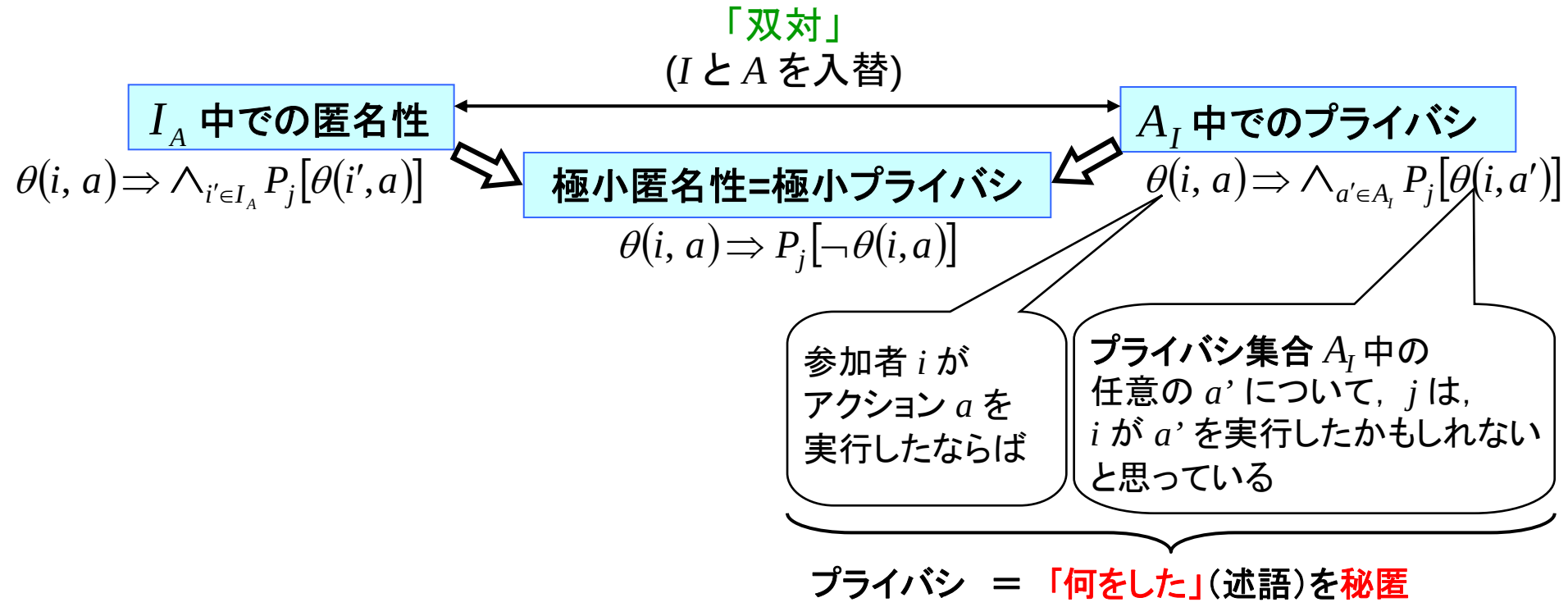
匿名性・プライバシ・顕名性・アイデンティティ（抜粋）



極大顕名性=極大ｱｲﾃﾞﾝﾃｨﾃｨ

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

匿名性・プライバシ・顕名性・アイデンティティ（抜粋）



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

A_I 中でのプライバシ
$\theta(i, a) \Rightarrow \wedge_{a' \in A_I} P_j[\theta(i, a')]$

極小匿名性=極小プライバシ
$\theta(i, a) \Rightarrow P_j[\neg\theta(i, a)]$

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)

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

= 送信者匿名性 + メッセージプライバシ

"電子投票の匿名性／プライバシ" (真野ら 2010)

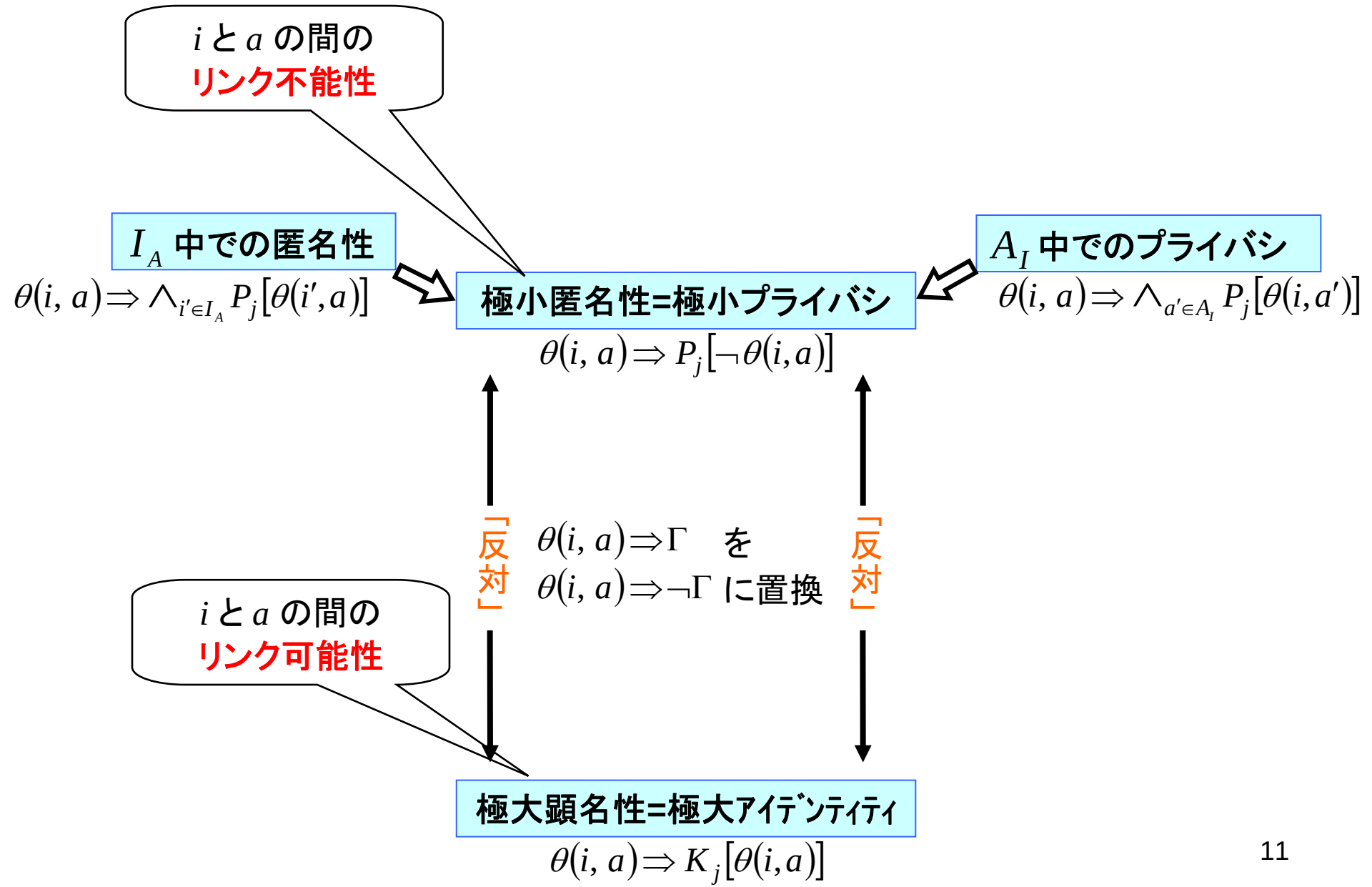
$\theta(i, vote(k)) \Rightarrow \wedge_{i' \in \{i' | i' \text{は投票権を獲得}\}} P_j[\theta(i', vote(k))] \wedge$

$\theta(i, vote(k)) \Rightarrow \wedge_{a' \in \{vote(k') | k' \text{は1票以上得票}\}} P_j[\theta(i, a')]$

= 投票者匿名性 + 投票プライバシ

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・顕名性・アイデンティティ（抜粋）



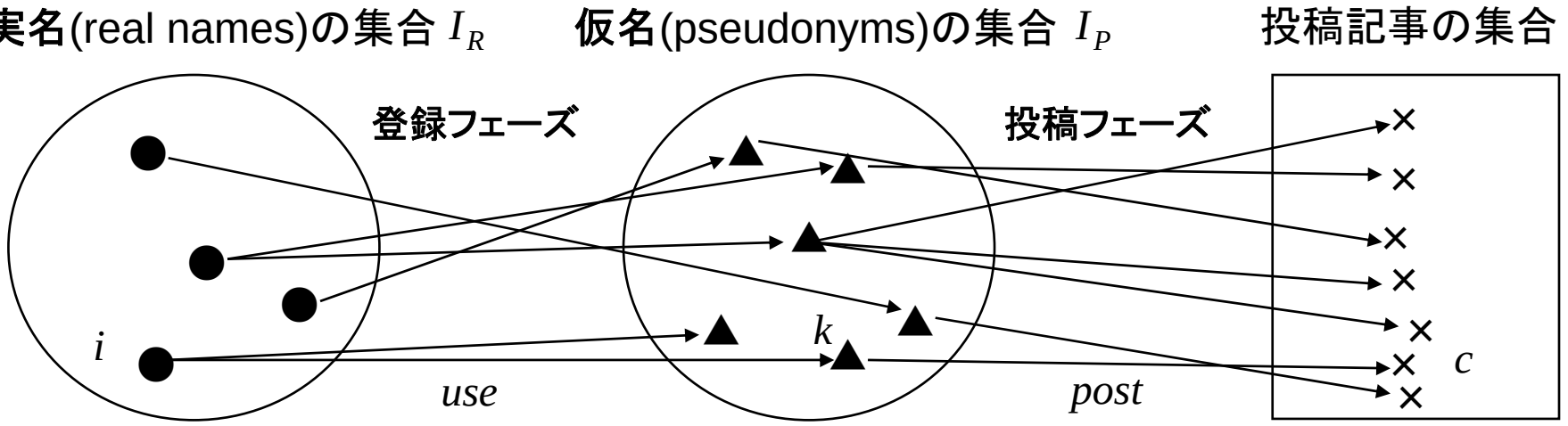
ここまでの話

【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、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

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

会員制匿名掲示板モデルの一般性

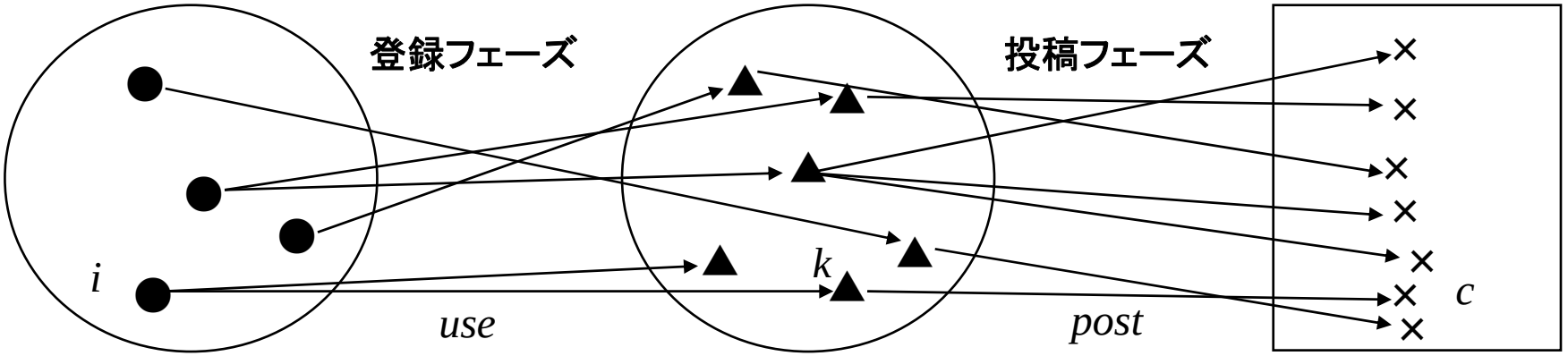
【再解釈その1】i: 投票者, k: 投票ID, c: 投票内容 ⇒ **電子投票**

【再解釈その2】*use*: 1段目 mix サーバ, *post*: 2段目 mix サーバ ⇒ **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

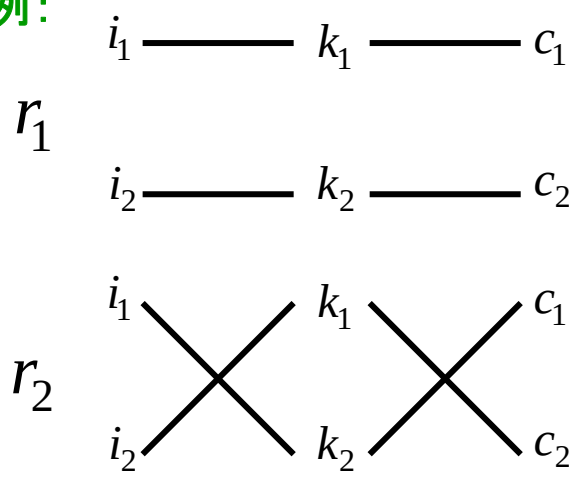
実名(real names)の集合 I_R　　仮名(pseudonyms)の集合 I_P　　投稿記事の集合 C



use に関する**匿名性**	＋	*post* に関する**プライバシ**
$\theta(i, use(k)) \Rightarrow \wedge_{i' \in I_R} P_j[\theta(i', use(k))]$		$\theta(k, post(c)) \Rightarrow \wedge_{c' \in C} P_j[\theta(k, post(c'))]$

submit に関する**匿名性** or **プライバシ**？？？　⇒成り立たない！

反例:



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は相反しない

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

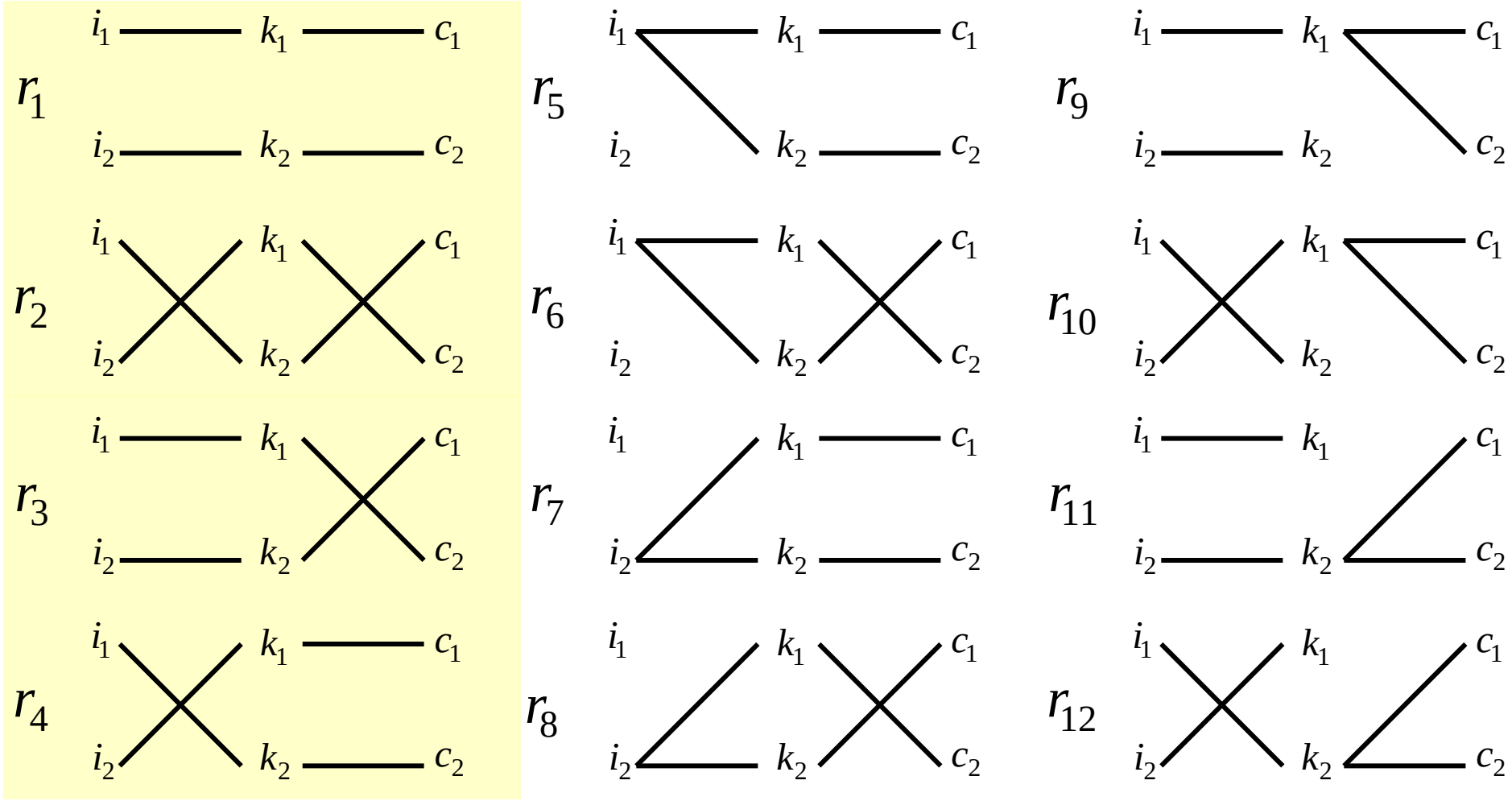
観察：*use* と *post* が「独立」ならば合成可能か？

独立性条件

$P_j[\,\theta\,(i, use(k))] \wedge P_j[\,\theta\,(k', post(c))]$
$\Downarrow$
$P_j[\,\theta\,(i, use(k)) \wedge \theta\,(k', post(c))]$

$\fallingdotseq$

$\Pr(A) * \Pr(B)$
$\|$
$\Pr(A \cap B)$



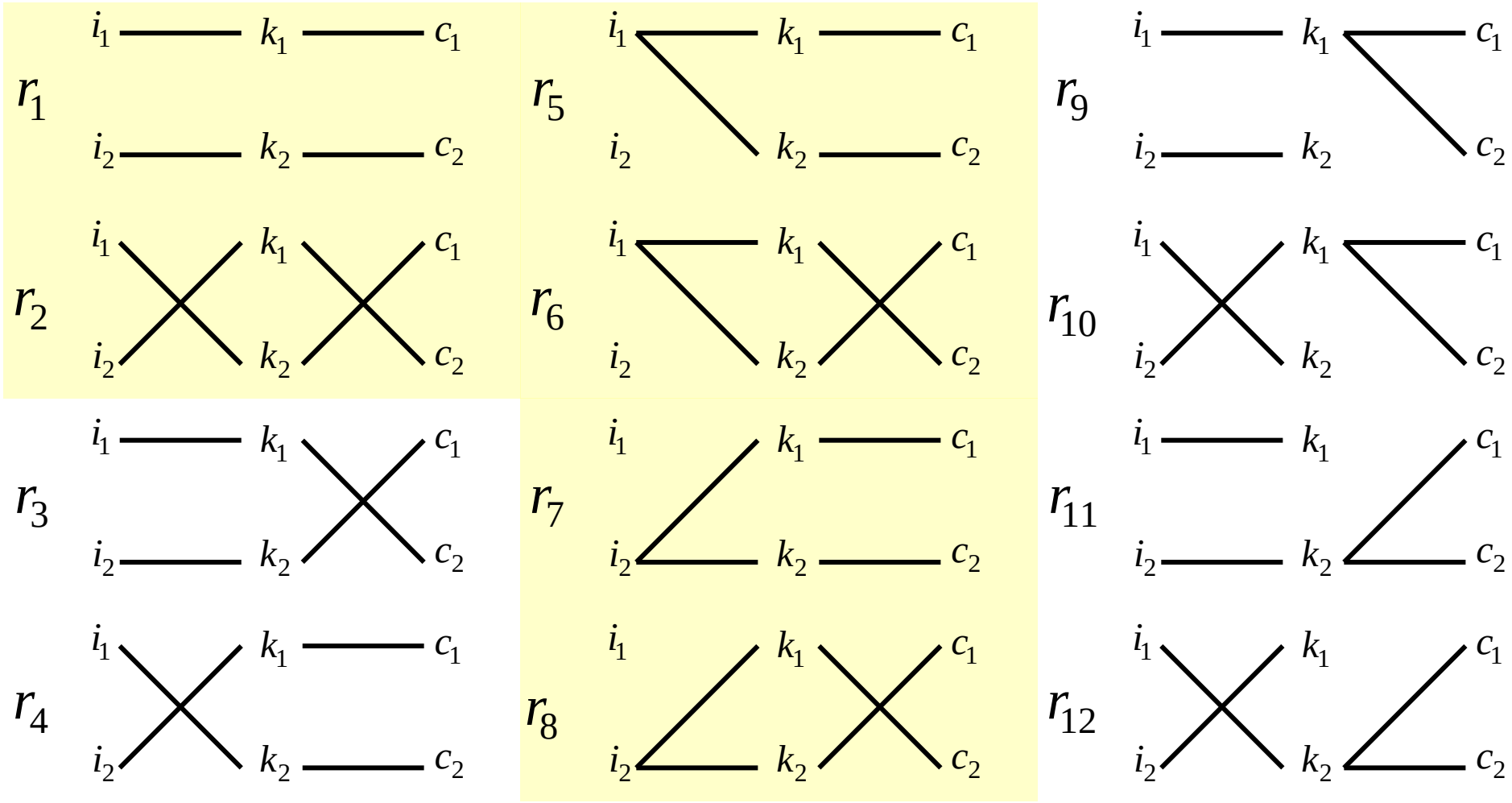
独立性条件自体が「メタレベル」のある種の匿名性・プライバシ

独立性条件

$P_j[\,\theta\,(i, use(k))] \wedge P_j[\,\theta\,(k', post(c))]$
$\Downarrow$
$P_j[\,\theta\,(i, use(k)) \wedge \theta\,(k', post(c))]$

$\fallingdotseq$

$\Pr(A) * \Pr(B)$
$\|$
$\Pr(A \cap B)$



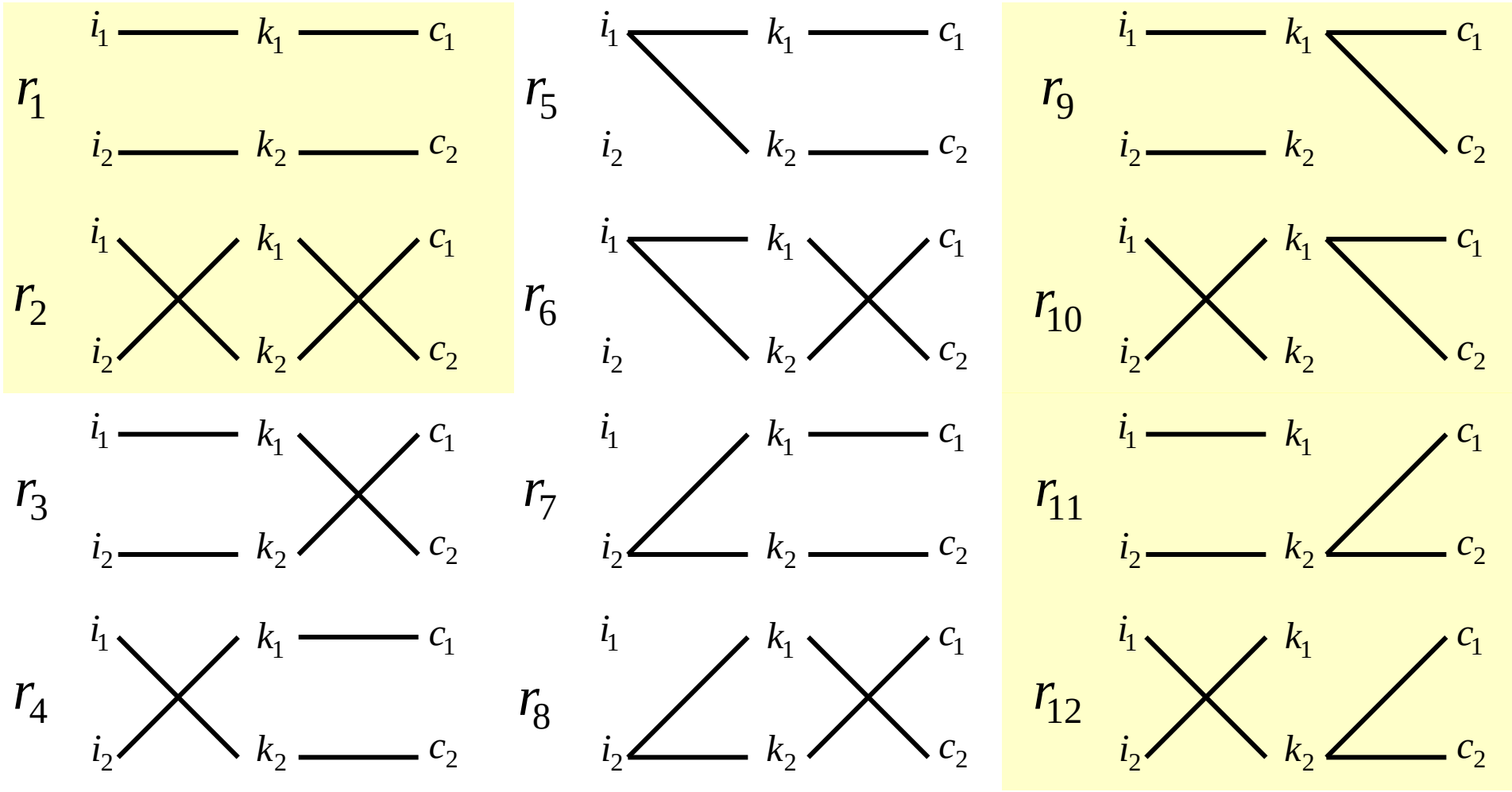
独立性条件自体が「メタレベル」のある種の匿名性・プライバシ

独立性条件

$P_j[\,\theta\,(i, use(k))] \wedge P_j[\,\theta\,(k', post(c))]$
$\Downarrow$
$P_j[\,\theta\,(i, use(k)) \wedge \theta\,(k', post(c))]$

$\fallingdotseq$

$\Pr(A) * \Pr(B)$
$\|$
$\Pr(A \cap B)$



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

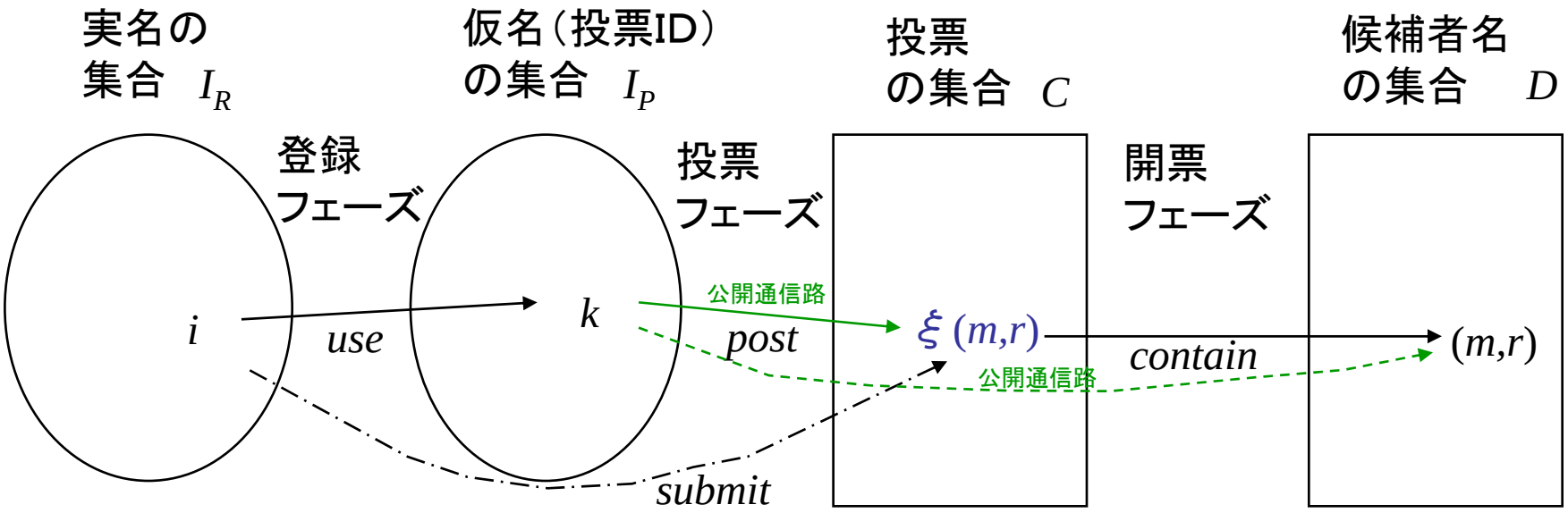
匿名性・プライバシが合成可能となるための十分条件

ケース	仮定	登録フェーズ(*use*)	投稿フェーズ(*post*)	全体(*submit*)
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 ⇒ 独立

①匿名＋プライバシ ≦ 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

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

	前提	登録フェーズ(*use*)	投票フェーズ(*post*)	開票フェーズ(*contain*)	全体(*vote*)
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・プライバシの合成不可能性
・独立性条件
・匿名性・プライバシ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