秘密計算の semi-honest安全性について

縫田 光司（NUIDA, Koji）

九州大学マス・フォア・インダストリ研究所
／産業技術総合研究所

SCIS2024＠長崎　2A3-5　　2024年1月24日

本研究の概要

- 2者間semi-honest秘密計算の標準的な安全性定義を再考
- この安全性定義がワンタイムパッドの安全性と整合的でない（ように見える）具体例を提示
- 上記の問題を解消する安全性定義の変更案を提案
  - 関連研究について（後述）
- その定義の性質と問題を考察

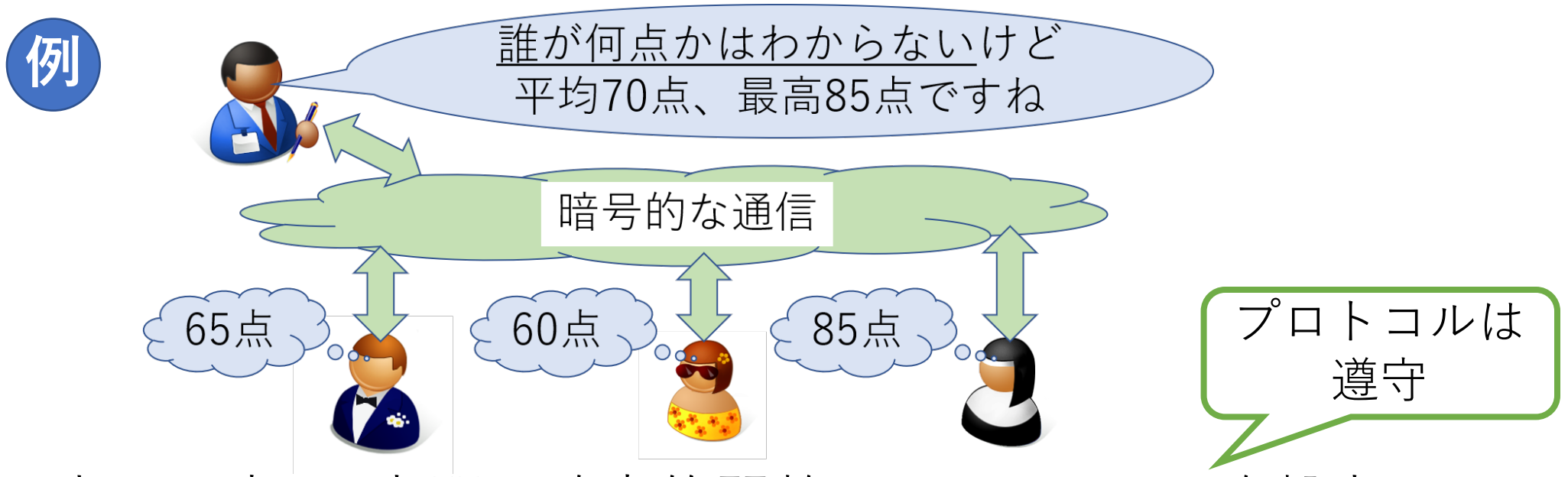
目次

- 研究の背景と問題意識
- 成果：安全性定義の再考と変更案
- 成果：提案する安全性定義の性質

目次

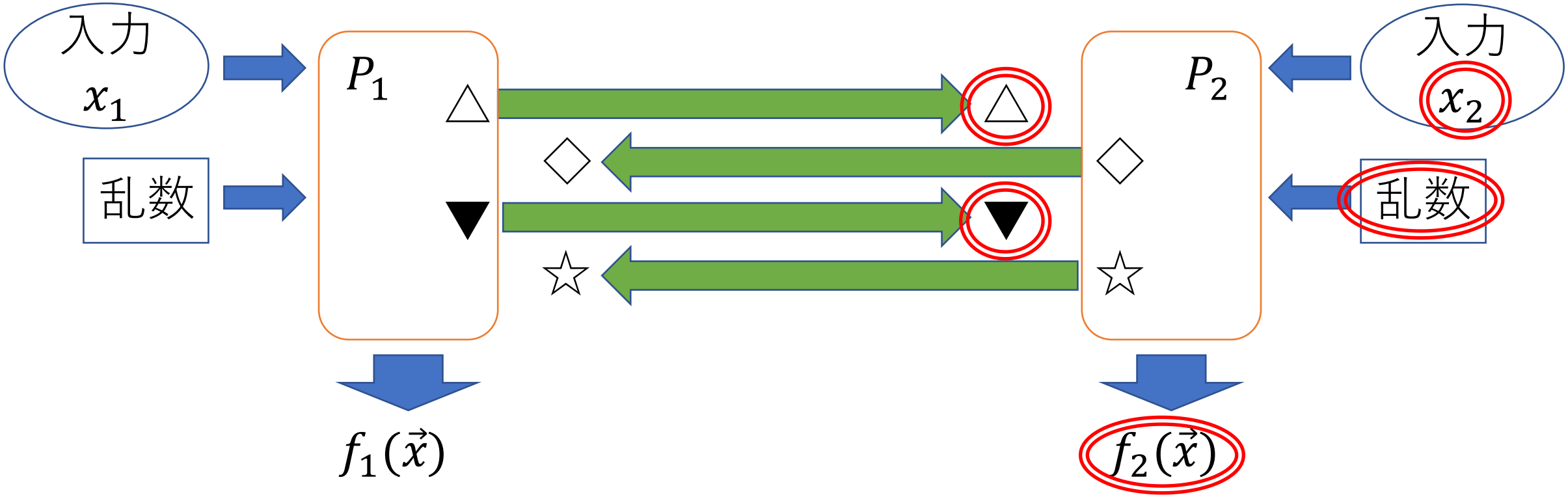
秘密計算とは

- 互いの入力を隠しつつ、欲しい計算結果だけを得る



- 本研究の設定：2者間、確率的関数、semi-honest攻撃者
  - プロトコルの正当性は常に前提

秘密計算の安全性定義（概要）



攻撃者（例：P_2）の入出力x_2と$f_2(\vec{x})$から◎の分布を模倣可能

- 「P_2はプロトコル中に入出力を超えた情報を得ない」

安全性定義の細部

- [Goldreich, FoC 7.2.2.1節]の定義（「元々の定義」）：

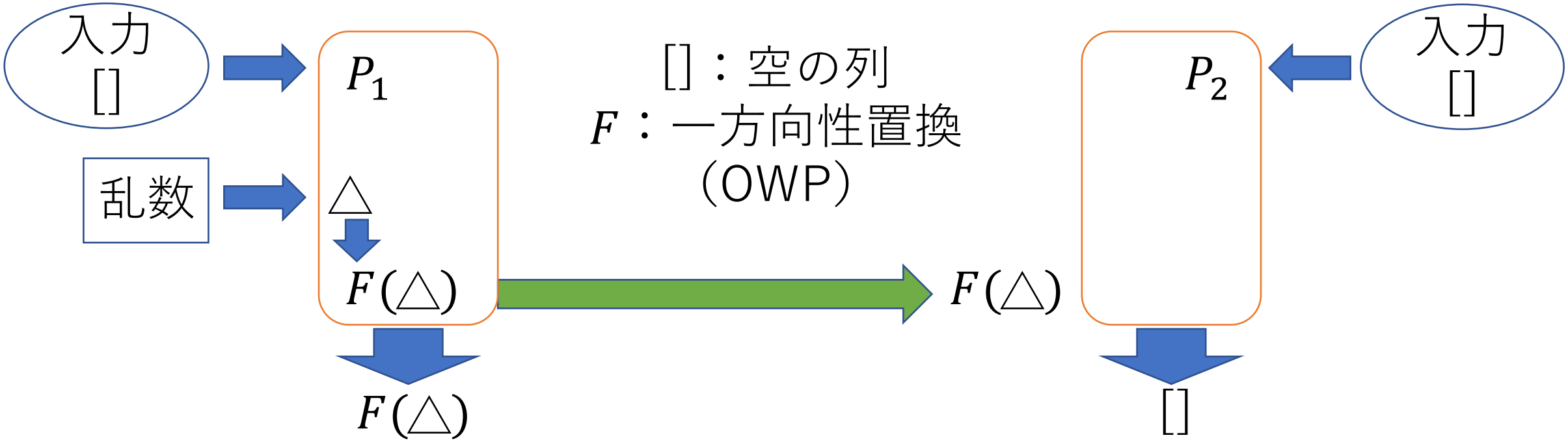
$$\{(S_2(y, f_2(x, y)), f(x, y))\}_{x,y} \overset{c}{\equiv} \{(\mathrm{VIEW}_2^{\Pi}(x, y), \mathrm{OUTPUT}^{\Pi}(x, y))\}_{x,y} \quad (7.10)$$

前ページの◎部

識別者は
関数/プロトコルの出力も得ている

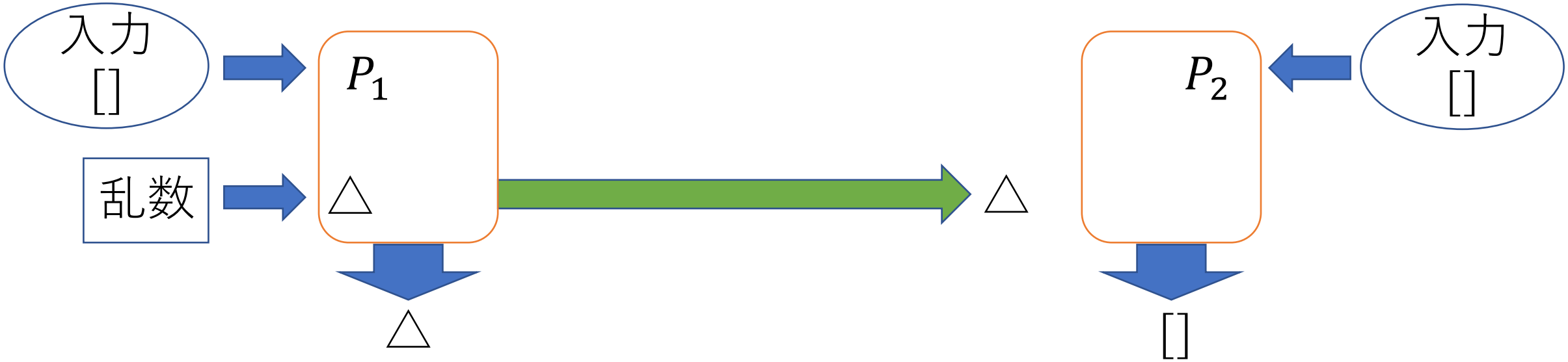
- 注：関数が非確率的ならviewの項だけで考えても同値（「簡略版定義」）

Goldreichによる説明（プロトコル2）



- P_1に対し、元々の定義では安全でなく、簡略版定義では安全
  - P_1は出力値のOWPによる逆像を得るので、安全でないかもしれない
  - 簡略版よりも慎重な定義

Goldreichによる説明（プロトコル1）

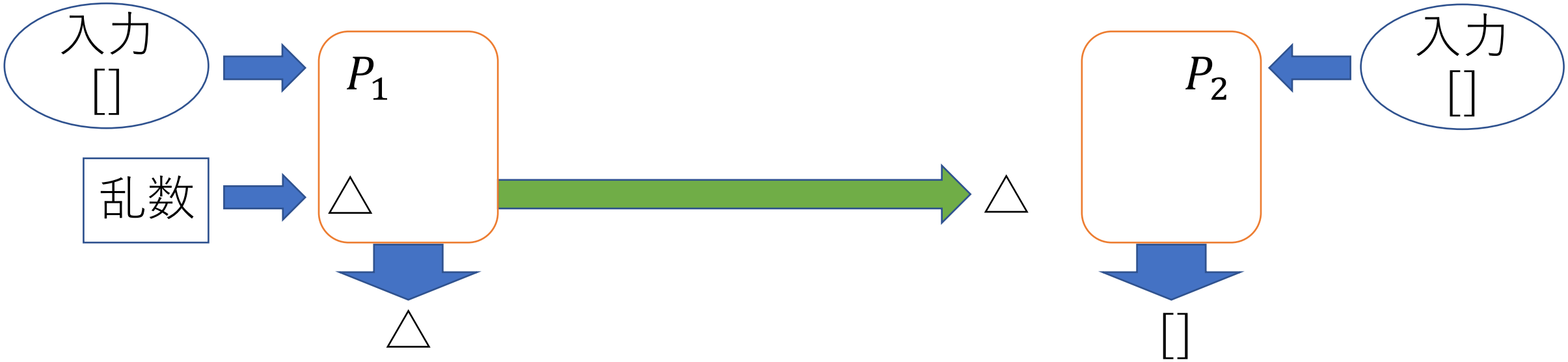


- P_2に対し、元々の定義では安全でなく、簡略版定義では安全
- Goldreichの説明：P_2はプロトコル中にP_1の**出力**を得ているのでプロトコルは安全と解釈されるべきではない
- **本研究の動機：本当にそうか？（入力ではなく出力なのに？）**

目次

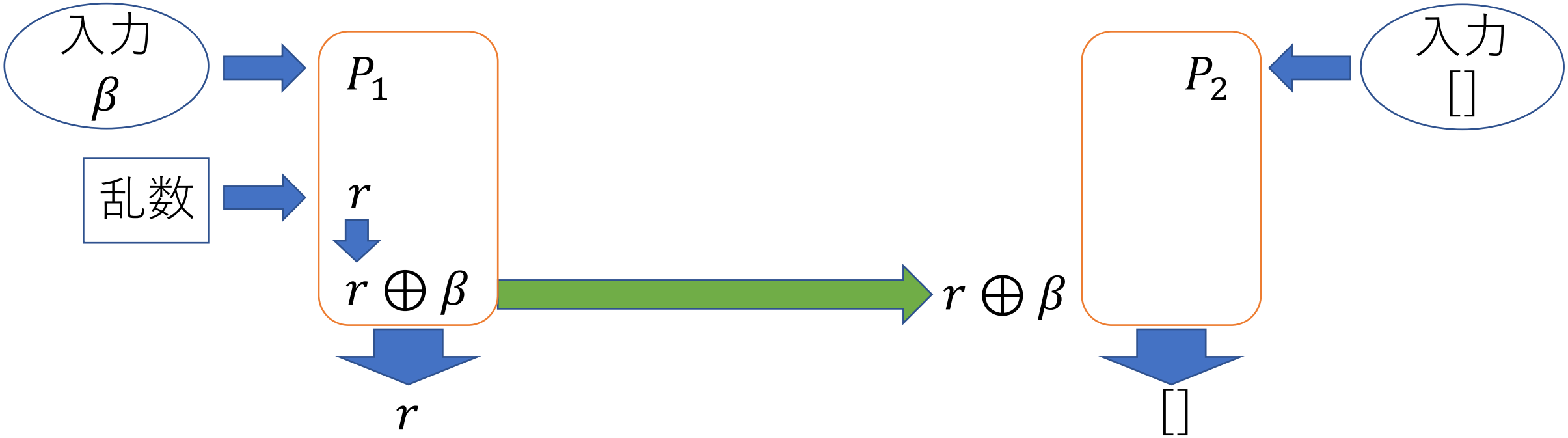
- 研究の背景と問題意識
- **成果：安全性定義の再考と変更案**
- 成果：提案する安全性定義の性質

プロトコル1について



- P_2に対し、元々の定義では安全でない
- だが、**P_2はP_1の入力（空の列！）の情報は得ていないのでは？**
  - プロトコル2とは異なり、△は計算困難な値でもない

本研究で考えた別の例（プロトコル3）



- P_2に対し、元々の定義では安全でない
- だが、$r \oplus \beta$はワンタイムパッドの暗号文なのだから、
  P_1の入力βの情報は何も漏れないはずでは？

安全性定義の再考

- [Goldreich, FoC 7.2.2.1節]の安全性定義：

$$\{(S_2(y, f_2(x, y)), f(x, y))\}_{x,y} \stackrel{c}{\equiv} \{(\text{VIEW}_2^{\Pi}(x, y), \text{OUTPUT}^{\Pi}(x, y))\}_{x,y} \quad (7.10)$$

- よく見ると、識別者は攻撃者P_2自身の出力だけでなく、**相手側P_1の出力も用いている**
- 「P_2の立場で」情報が得られない、よりも強い主張なのでは？
- **安全性定義の変更案**（「今回の定義」）：識別者に攻撃者P_2の出力を与えるが、**相手側P_1の出力は与えない**
  - ideal-realパラダイムでも同値な定義が可能
  - 暗号学的疑似乱数による安全性喪失 [N., PKC 2021] にも影響なし
- 注：実は同様の定義が（別の動機で）言及されていた（後述）

目次

- 研究の背景と問題意識
- 成果：安全性定義の再考と変更案
- **成果：提案する安全性定義の性質**

安全性の強さの比較

「強安全」　「弱安全」

- 元々の定義で安全 ⇒ 今回の定義で安全 ⇒ 簡略版定義で安全
  - 左に進むほど識別者の入力が増える（条件が厳しくなる）ので
- したがって、
  - 元々安全だったプロトコルの安全性証明を付け直す必要はない
  - 関数が非確率的であれば三つの定義はすべて同値

プロトコルの例	元々	**今回**	簡略版	（直感）
1（出力を送る）	No	**Yes**	Yes	Yes
2（一方向性置換）	No	**No**	Yes	No?
3（ワンタイムパッド）	No	**Yes**	Yes	Yes

安全性定義間の関係

- **<u>定義</u>**　P_{3_i}の出力が再現可能とは：あるPPTなTについて

$$\left(view_i(\vec{x}), out_i(\vec{x}), T\left(\vec{x}, out_i(\vec{x})\right)\right)$$
$$\approx \left(view_i(\vec{x}), out_i(\vec{x}), out_{3\_i}(\vec{x})\right)$$

- **<u>定理</u>**　**(*) P_iに対して弱安全＋(**) P_{3_i}の出力が再現可能**
  ⇒ P_iに対して強安全

- **<u>証明</u>**（概略）$\left(view_i(\vec{x}), out_i(\vec{x}), out_{3\_i}(\vec{x})\right)$

$$\approx_{(**)} \left(view_i(\vec{x}), out_i(\vec{x}), T\left(\vec{x}, out_i(\vec{x})\right)\right)$$
$$\approx_{(*)} \left(S(out_i(\vec{x})), out_i(\vec{x}), T\left(\vec{x}, out_i(\vec{x})\right)\right)$$
$$\approx_{(**)} \left(S(out_i(\vec{x})), out_i(\vec{x}), out_{3\_i}(\vec{x})\right)$$

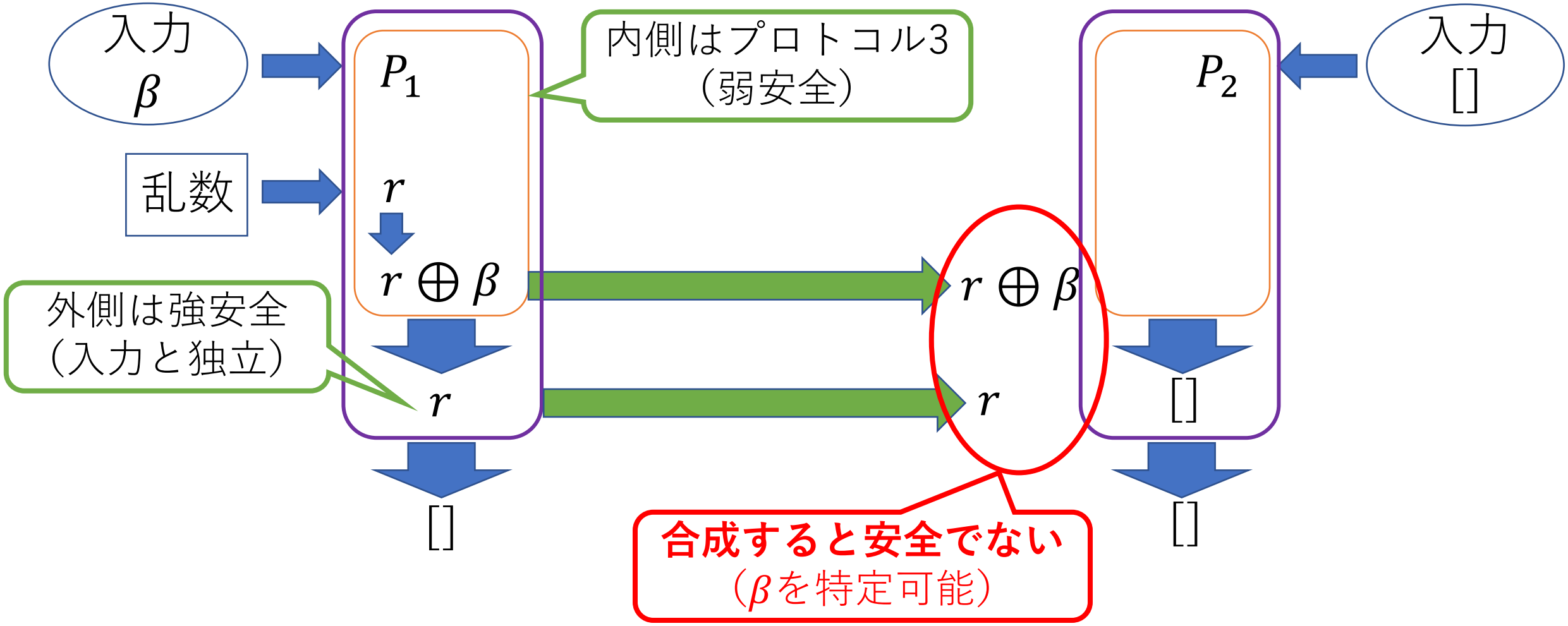
既存研究[吉田ら, SCIS 2023, 6.3節]との関係

- 吉田, 定兼, 戸澤: 秘密計算基数ソートの通信量の削減, SCIS'23
  - 正当性＋（本研究の用語で）弱安全性＋「攻撃者の入出力を固定した条件下で、攻撃者のviewと相手方の出力が独立」から強安全性を導出
- 上記論文では、提案プロトコルの強安全性を証明するための中間ステップとして弱安全性に言及
  - 「安全性定義の妥当性」には着目していない
- 上記論文の条件「　」は本研究での条件(**)とは単純比較不能
  - $\vec{x}$と$out_i(\vec{x})$から$out_{3-i}(\vec{x})$が効率的に模倣可能とは限らないため

合成定理について

- $\Pi^{(g)}$：関数gの理想機能を用いて関数fを計算するプロトコル
- Π'：関数gを計算するプロトコル
- **合成定理**[Goldreich] $\Pi^{(g)}$とΠ'がともに**強**安全であれば、$\Pi^{(g)}$の中でΠ'を用いるプロトコル$\Pi^{\Pi'}$も**強**安全
- 「$\Pi^{(g)}$が**強**安全＋Π'が弱安全 ⇒ $\Pi^{\Pi'}$は弱安全」は**不成立**（次頁）
- 「$\Pi^{(g)}$が弱安全＋Π'が**強**安全 ⇒ $\Pi^{\Pi'}$は弱安全」は**成立**
  - 証明は元々の合成定理とほぼ同様

弱安全版合成定理の反例（P_2が攻撃者）



まとめ

- 2者間semi-honest秘密計算の従来の安全性定義の問題を指摘
- 変更案の提案：識別者に攻撃者以外の参加者の出力を与えない
  - 従来の安全性定義より一般に弱い安全性
- 従来の安全性との関係を考察
- 問題点：合成定理が一般には不成立
  - 合成定理を成り立たせる便利な充分条件は今後の研究課題